Privacy and Personal Information Management Policy

Version 1.0 · Last updated 2026-10-20 · Owner: Privacy Officer

Privacy and Personal Information Management Policy

> **Unified-set note.** This internal policy governs how Silkline handles personal information (PII) and responds to data-subject rights requests, supporting SOC 2 (Privacy category) and FedRAMP privacy expectations. The **public website Privacy Notice** (silkline.ai) and **Terms of Use** are separate customer-facing legal documents maintained by Legal and are not part of this internal security policy set. Production-data protection (encryption, segmentation, access) is governed by the Data Classification Policy, Encryption and Cryptographic Module Policy, and Access Management Policy.

1. Purpose

Establish standardized processes for (1) handling and responding to data-subject requests to exercise rights concerning personal information, and (2) notifying appropriate stakeholders when PII is disclosed to third parties — ensuring transparency, accountability, and regulatory compliance.

2. Scope

All employees, contractors, and third-party vendors who handle personal information within the organization, and all PII collected or processed by Silkline under applicable agreements.

3. Handling Data Subject Rights Requests

- **Identification and documentation** — any request (access, correction, deletion, portability) is promptly identified and documented.
- **Acknowledgement** — within 1 business day of receipt, with the estimated response timeframe.
- **Verification** — authenticate the requestor's identity (or a representative's authorization) before acting.
- **Assessment** — categorize the request and identify the data processing activities and systems involved.
- **Locate and retrieve** — search all applicable systems and repositories (customer databases, supplier collaboration platforms, archives); document the search.
- **Respond** — within regulatory/contractual timeframes, typically **within 30 days** (extensions communicated if legally permitted). Deliver data securely (encrypted email or secure portal); for deletion/de-identification, document the steps taken; if a request cannot be fulfilled, provide the reason.

Request-type procedures: Access — provide PII in a readable format. Deletion — assess validity against legal obligations and retention requirements. Correction — verify and accurately update. Portability — securely transfer PII in a commonly used, machine-readable format.

Stakeholders involved: Privacy Officer; Legal/Outside Counsel; relevant Department Heads; IT Security (if technical action is required).

4. Notification of Disclosures to Third Parties

- Any disclosure of PII to a third party is promptly identified and documented.
- Stakeholders are notified **within 24 hours** of identifying the disclosure: Security Officer, Privacy Officer, Legal/Outside Counsel, affected individuals, and relevant Department Heads.
- Notification is made via email and followed by a formal letter if required.

5. Retention and Records

Records of all requests, responses, and actions are maintained for **at least three years** or as required by applicable contracts, consistent with the Data Retention and Disposal Policy.

6. Audit and Review

The processes for handling data-subject requests and notifying stakeholders of PII disclosures are **audited quarterly** for compliance and effectiveness.

7. Compliance

Failure to comply may result in disciplinary action up to and including termination, per the Code of Conduct.

8. Policy Maintenance

Reviewed annually or upon material legal/regulatory change; approved by the Privacy Officer; maintained in the policy repository with pull-request-based review.