Slipstream Financial
Data Protection Policy

Document Owner: Mo Brown Effective Date: 11-24-2024
Version: 202411
Document Approver: Miles Busby

1. Purpose

Slipstream Financial ("Slipstream," "we," "our," or "us") is committed to protecting the confidentiality, integrity, and availability of all data entrusted to us. This Data Protection Policy establishes the principles, standards, and controls governing how we collect, process, store, share, and safeguard data in the course of delivering banking and payment solutions to business clients.

2. Scope

This policy applies to:

- All employees, contractors, consultants, and third parties who process data on behalf of Slipstream.
- All systems, applications, networks, and devices used to process or store data.
- All data types, including customer data, transaction data, financial records, and internal business data.

3. Definitions

- **Personal Data:** Information relating to an identified or identifiable individual.
- **Sensitive Data:** Data requiring enhanced protection (e.g., financial account details, authentication credentials).
- **Processing:** Any operation performed on data (e.g., collection, storage, use, sharing).
- **Data Subject:** An individual whose personal data is processed.

4. Guiding Principles

Slipstream adheres to the following principles:

- **Lawfulness, Fairness, Transparency:** Data is processed legally and transparently.
- **Purpose Limitation:** Data is collected for specified, legitimate purposes only.
- **Data Minimization:** Only necessary data is collected and processed.
- **Accuracy:** Data is kept accurate and up to date.
- **Storage Limitation:** Data is retained only as long as necessary.
- **Integrity and Confidentiality:** Data is protected against unauthorized access, loss, or damage.
- **Accountability:** Slipstream is responsible for demonstrating compliance.

5. Data Collection and Use

Slipstream collects and processes data to:

- Provide banking and payment services.
- Verify identity and prevent fraud.
- Comply with legal and regulatory obligations.
- Improve products and customer experience.

Data collected may include:

- Business and customer identification details.
- Financial account and transaction data.
- Usage and system interaction data.

6. Legal and Regulatory Compliance

Slipstream complies with all applicable data protection and financial regulations, including but not limited to:

- Data privacy laws in jurisdictions where we operate.
- Anti-money laundering (AML) and know-your-customer (KYC) requirements.
- Payment industry standards (e.g., PCI DSS where applicable).

7. Data Security Controls

Slipstream implements appropriate technical and organizational measures, including:

- **Access Control:** Role-based access and least-privilege principles.
- **Encryption:** Data encrypted in transit and at rest.
- **Monitoring:** Continuous monitoring for unauthorized access or anomalies.
- **Network Security:** Firewalls, intrusion detection/prevention systems.
- **Secure Development:** Security integrated into system design and development.
- **Backup and Recovery:** Regular backups and disaster recovery planning.

8. Data Sharing and Third Parties

- Data is shared only with authorized parties for legitimate business purposes.
- Third-party service providers must meet Slipstream's data protection standards.
- Data processing agreements (DPAs) are required for all vendors handling sensitive data.

9. Data Retention and Disposal

- Data is retained according to legal, regulatory, and business requirements.
- Secure disposal methods (e.g., encryption key destruction, secure deletion) are used when data is no longer needed.

10. Data Subject Rights

Where applicable, individuals have the right to:

- Access their personal data.
- Request correction or deletion.
- Restrict or object to processing.
- Request data portability.

11. Incident Response and Breach Notification

- All suspected data breaches must be reported immediately.
- Slipstream maintains an incident response plan to investigate and mitigate breaches.
- Regulatory authorities and affected parties are notified as required by law.

12. Training and Awareness

- Employees receive regular data protection and security training.
- Awareness programs ensure understanding of responsibilities and risks.

13. Governance and Accountability

- A designated Data Protection Officer (DPO) or equivalent oversees compliance.
- Regular audits and assessments are conducted.
- Non-compliance may result in disciplinary action

14. Contact Information

For questions or concerns regarding this policy or data protection practices, contact:
Email: support@slipstreamfinancial.com

Address: Slipstream Financial
911 South Main St
Forth Worth, TX 76104