Technical & Ethical Compliance Commitments

Oríon Labs | December 2025 | Confidential

Executive Summary

Oríon Labs is committed to the highest standards of technical security, data privacy, and ethical AI practices. This document outlines our comprehensive compliance framework for the TikTok Battle Agents integration.

Part 1: Data Privacy & Protection

1.1 Regulatory Compliance

Certifications & Standards

Regulation	Status	Scope
GDPR (EU)	Compliant	All EU user data processing
CCPA (California)	Compliant	California resident data
COPPA (Children)	Compliant	Age verification, parental consent
LGPD (Brazil)	Compliant	Brazilian user data
PIPL (China)	Ready	Chinese market requirements

Data Processing Principles

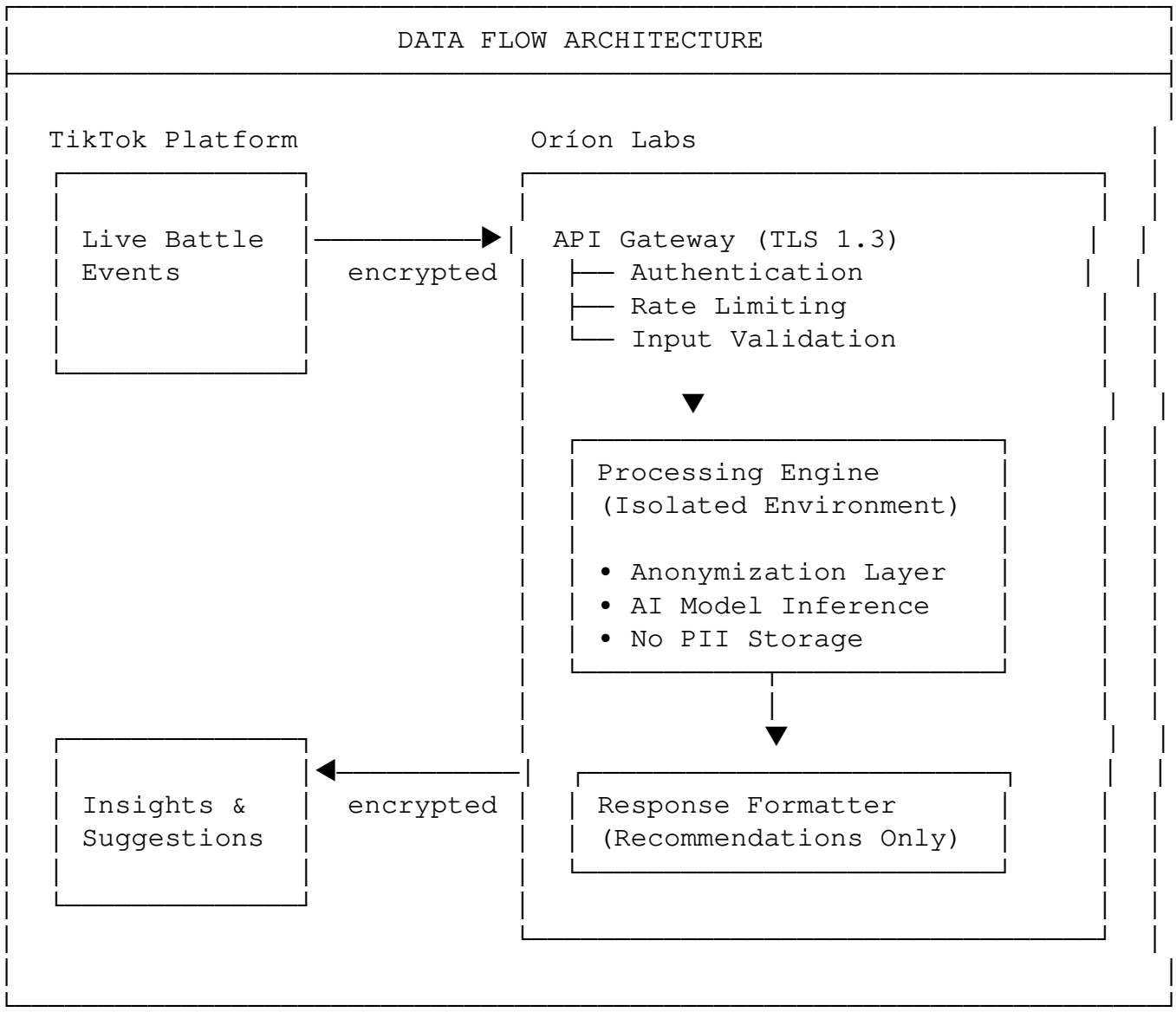
1. **Lawfulness & Transparency**
    - Clear disclosure of all data processing activities
    - User-facing privacy notices in local languages
    - Consent mechanisms where required
2. **Purpose Limitation**
    - Data used exclusively for battle optimization
    - No secondary use without explicit consent
    - No sale or transfer to third parties
3. **Data Minimization**
    - Collect only essential behavioral signals
    - No PII storage beyond session context
    - Aggregated analytics preferred over individual tracking

4. **Storage Limitation**

    - Raw event data: 90-day retention
    - Aggregated insights: 2-year retention
    - User deletion requests: 30-day fulfillment

1.2 Data Architecture

Data Flow Diagram



Data Categories

Category	Examples	Storage	Encryption
Session Data	Battle IDs, timestamps	90 days	AES-256
Behavioral Signals	Gift timing, engagement patterns	90 days	AES-256
Aggregated Metrics	Conversion rates, averages	2 years	AES-256
Model Parameters	AI weights (no user data)	Indefinite	AES-256
PII	None collected	N/A	N/A

Part 2: Technical Security

2.1 Infrastructure Security

Hosting & Isolation

- **Cloud Provider:** AWS/GCP (SOC 2 Type II certified)
- **Region Options:** US, EU, APAC (data residency compliance)
- **Environment Isolation:** Dedicated VPC per client
- **Network Security:** Private endpoints, no public exposure

Security Controls

Layer	Control	Implementation
Network	Firewall	AWS WAF, security groups
Transport	Encryption	TLS 1.3 minimum
Application	Auth	OAuth 2.0 + API keys
Data	Encryption	AES-256 at rest, TLS in transit
Access	IAM	Role-based, least privilege
Monitoring	SIEM	Real-time threat detection

2.2 Application Security

Secure Development Lifecycle

1. **Design Phase**
    - Threat modeling (STRIDE methodology)
    - Security requirements definition
    - Privacy impact assessment
2. **Development Phase**
    - Secure coding standards (OWASP Top 10)
    - Dependency vulnerability scanning
    - Code review with security focus
3. **Testing Phase**
    - Static Application Security Testing (SAST)
    - Dynamic Application Security Testing (DAST)
    - Penetration testing (annual, third-party)
4. **Deployment Phase**
    - Infrastructure as Code (auditable)
    - Immutable deployments
    - Automated rollback capability

Vulnerability Management

Severity	Response Time	Notification
Critical	24 hours	Immediate
High	7 days	Within 48 hours
Medium	30 days	Monthly report
Low	90 days	Quarterly report

2.3 API Security

Authentication & Authorization

```
API REQUEST FLOW:
═══════════════════════════════════════════════════════════════

1. TikTok Server → [OAuth Token + API Key + Request Signature]
                                    │
                                    ▼
2. Oríon Gateway → [Validate Token]
                 → [Verify Signature (HMAC-SHA256)]
                 → [Check Rate Limits]
                 → [Validate Request Schema]
                                    │
                                    ▼
3. Processing    → [Process if all checks pass]
                 → [Return signed response]
                                    │
                                    ▼
4. Audit Log     → [Log request metadata (no payload)]

═══════════════════════════════════════════════════════════════
```

Rate Limiting

Tier	Requests/sec	Burst	Use Case
Standard	100	500	Normal operations
Elevated	1,000	5,000	High-traffic events
Emergency	10,000	50,000	Platform-wide events

Part 3: Ethical AI Commitments

3.1 Responsible AI Principles

Our Ethical Framework

1. **Transparency**

- AI recommendations are explainable
- Users understand when AI is active
- No hidden manipulation

2. **Fairness**

   - No discrimination based on demographics
   - Equal opportunity for all participants
   - Regular bias audits

3. **User Autonomy**

   - Recommendations, not mandates
   - Easy opt-out mechanisms
   - User control over AI features

4. **Harm Prevention**

   - No encouragement of excessive spending
   - Spending limit support
   - Cool-down period recommendations

3.2 Anti-Exploitation Measures

Vulnerable User Protection

Protection	Implementation
Spending Limits	Optional daily/weekly caps
Cool-Down Alerts	Notification after extended sessions
Pattern Detection	Flag potentially problematic behavior
Minor Protection	Enhanced safeguards for <18 users

What We Will NEVER Do

- ✕ Use dark patterns to manipulate spending
- ✕ Target vulnerable users for increased monetization
- ✕ Exploit addiction mechanisms
- ✕ Hide the presence of AI optimization
- ✕ Sell or share user data
- ✕ Discriminate based on protected characteristics

3.3 Algorithmic Accountability

Model Governance

Aspect	Commitment
Training Data	Audited for bias, documented sources
Model Updates	Staged rollout with monitoring
Performance Metrics	Fairness metrics alongside business metrics

Human Oversight	Human-in-the-loop for edge cases

Audit Trail

- All AI decisions logged with reasoning
- Monthly algorithmic impact assessments
- Third-party annual ethics audit
- Public transparency report (anonymized)

Part 4: Contractual Commitments

4.1 Service Level Agreement (SLA)

Metric	Commitment	Measurement
Uptime	99.9%	Monthly
Latency (p95)	$<$100ms	Real-time
Error Rate	$<$0.1%	Weekly
Incident Response	$<$15 min (Critical)	Per incident

Breach Remedies

Uptime	Credit
99.0% - 99.9%	10% monthly fee
95.0% - 99.0%	25% monthly fee
$<$95.0%	50% monthly fee

4.2 Data Processing Agreement (DPA)

Key Terms

1. **Data Controller:** TikTok
2. **Data Processor:** Oríon Labs
3. **Sub-processors:** Listed and pre-approved only
4. **Data Location:** As specified by TikTok
5. **Deletion:** Within 30 days of contract termination

Audit Rights

- TikTok may audit with 30-day notice
- Annual third-party audit reports provided
- Immediate access for security incidents

4.3 Intellectual Property

Element	Ownership

TikTok user data	TikTok
Battle event data	TikTok
AI models (pre-existing)	Oríon Labs
Custom developments	Jointly negotiated
Integration code	TikTok (license)

Part 5: Incident Response

5.1 Security Incident Procedure

Classification

Level	Description	Response
P1 - Critical	Data breach, system compromise	Immediate escalation
P2 - High	Service degradation, potential breach	1-hour response
P3 - Medium	Minor security issue	24-hour response
P4 - Low	Informational, best practice	Standard process

Notification Timeline

```
INCIDENT TIMELINE:
──────────────────────────────────────────────────────────────

T+0       Incident detected
T+15min   Initial assessment complete
T+30min   TikTok security team notified (P1/P2)
T+2hr     Preliminary report delivered
T+24hr    Detailed incident report
T+72hr    Root cause analysis
T+7d      Remediation plan + implementation
T+30d     Post-incident review

──────────────────────────────────────────────────────────────
```

5.2 Business Continuity

Disaster Recovery

Scenario	RTO	RPO
Regional outage	1 hour	5 minutes
Data center failure	4 hours	15 minutes
Complete platform failure	24 hours	1 hour

Backup Strategy

- Real-time replication to secondary region
- Daily encrypted backups (30-day retention)
- Annual recovery testing

Part 6: Compliance Certifications

Current Certifications

Certification	Status	Valid Until
SOC 2 Type II	✓ Certified	Dec 2026
ISO 27001	✓ Certified	Mar 2026
ISO 27701	In Progress	Q2 2025
GDPR Compliance	✓ Verified	Ongoing
CCPA Compliance	✓ Verified	Ongoing

Planned Certifications

- ISO 27701 (Privacy) — Q2 2025
- PCI DSS (if payment processing) — Q3 2025
- FedRAMP (if US government) — Q4 2025

Signatures

Oríon Labs Commitments

We, Oríon Labs, hereby commit to all technical, security, privacy, and ethical standards outlined in this document.

Authorized Signatory:

_____
Name: [CEO Name]
Title: Chief Executive Officer
Date: _____

Technical Signatory:

_____
Name: [CTO Name]
Title: Chief Technology Officer
Date: _____

Contact for Compliance Inquiries

Data Protection Officer Email: dpo@orionlabs.ai

Security Team Email: security@orionlabs.ai Emergency: +1-XXX-XXX-XXXX (24/7)

Legal & Compliance Email: legal@orionlabs.ai

Document Version: 1.0 Last Updated: December 2025 Classification: Confidential