

AdGo Process Documentation

This document summarizes all 40 processes implemented in the AdGo platform, grouped by sprint wave. Each process includes its definition, protection type, acceptance criteria, and risks with mitigations.

Wave 1: Core Engine & SME Campaigns

1. Context Signals

- **Definition:** Ingests and processes real-time context data (location, time, device, user state) for ad targeting.
- **Protection Type:** Patent (algorithmic context processing)
- **Acceptance Criteria:** Context data is reliably ingested, normalized, and available for targeting logic.
- **Risks & Mitigations:** Data privacy risk; mitigate with encryption and user consent.

2. Frequency/Fatigue Management

- **Definition:** Controls ad exposure frequency to prevent user fatigue.
- **Protection Type:** Patent
- **Acceptance Criteria:** No user receives more than X ads per Y time window.
- **Risks & Mitigations:** Over-throttling; mitigate with adaptive thresholds.

3. Ranking Engine

- **Definition:** Ranks eligible ads for delivery based on context, bid, and relevance.
- **Protection Type:** Patent
- **Acceptance Criteria:** Top-ranked ad is always contextually relevant and highest value.
- **Risks & Mitigations:** Bias in ranking; mitigate with regular audits.

4. Quiet/Geofencing

- **Definition:** Suppresses ads in sensitive locations or times (e.g., hospitals, night hours).
- **Protection Type:** Copyright (geofence database)
- **Acceptance Criteria:** No ads delivered in geofenced zones/times.
- **Risks & Mitigations:** False positives; mitigate with user override and manual review.

5. Latency/Fallback

- **Definition:** Ensures ad delivery is robust to network latency, with fallback logic.
- **Protection Type:** Patent
- **Acceptance Criteria:** Ad delivery never fails due to network issues; fallback is seamless.
- **Risks & Mitigations:** Increased infra cost; mitigate with caching and edge logic.

6. Failover/Redundancy

- **Definition:** Provides failover for ad delivery and reporting systems.
- **Protection Type:** Patent
- **Acceptance Criteria:** No single point of failure; system auto-recovers.
- **Risks & Mitigations:** Complexity; mitigate with automated failover testing.

7. Campaign Targeting

- **Definition:** Enables targeting by campaign parameters (demographics, interests, etc.).
- **Protection Type:** Trademark (targeting schema)
- **Acceptance Criteria:** Campaigns reach only defined audience segments.
- **Risks & Mitigations:** Targeting leakage; mitigate with strict validation.

8. Multi-Location Support

- **Definition:** Allows campaigns to run across multiple locations and regions.
- **Protection Type:** Copyright
- **Acceptance Criteria:** Campaigns can be configured for any supported region.
- **Risks & Mitigations:** Location mismatch; mitigate with geo-validation.

9. A/B Testing

- **Definition:** Supports split testing of creatives and campaign parameters.
 - **Protection Type:** Patent
 - **Acceptance Criteria:** A/B test results are statistically valid and actionable.
 - **Risks & Mitigations:** Sample bias; mitigate with randomization.
-

Wave 2: Advanced Incentives & Security

10. Offline Redemption

- **Definition:** Allows users to redeem offers without network connectivity.
- **Protection Type:** Patent
- **Acceptance Criteria:** Redemption is logged and synced when online.
- **Risks & Mitigations:** Fraud risk; mitigate with device attestation.

11. Cross-Platform Deduplication

- **Definition:** Prevents duplicate redemptions across devices/platforms.
- **Protection Type:** Patent
- **Acceptance Criteria:** No duplicate redemptions detected in logs.
- **Risks & Mitigations:** Missed duplicates; mitigate with hash-based matching.

12. Merchant Collusion Detection

- **Definition:** Detects and flags collusion between merchants for fraudulent redemptions.
- **Protection Type:** Patent
- **Acceptance Criteria:** Collusion events are flagged and reviewed.
- **Risks & Mitigations:** False positives; mitigate with manual review.

13. Immutable Ledger

- **Definition:** Stores all transactions in an immutable, auditable ledger.
- **Protection Type:** Patent
- **Acceptance Criteria:** Ledger entries cannot be altered or deleted.
- **Risks & Mitigations:** Ledger bloat; mitigate with archiving.

14. Payout Simulations

- **Definition:** Simulates payout scenarios for advertisers and drivers.
- **Protection Type:** Copyright
- **Acceptance Criteria:** Simulations match real payout logic.

- **Risks & Mitigations:** Simulation drift; mitigate with regular sync.

15. Driver Gamification

- **Definition:** Adds gamification elements to driver experience (badges, leaderboards).
- **Protection Type:** Trademark
- **Acceptance Criteria:** Drivers see gamification features and respond positively.
- **Risks & Mitigations:** Over-gamification; mitigate with feedback loops.

16. Category-Weighted Incentives

- **Definition:** Incentives weighted by ad category for drivers and advertisers.
 - **Protection Type:** Patent
 - **Acceptance Criteria:** Incentives are correctly calculated and distributed.
 - **Risks & Mitigations:** Miscalculation; mitigate with automated tests.
-

Wave 3: Compliance, SDK, Expansion

17. Consent Receipts & Audit Logs

- **Definition:** Generates consent receipts and audit logs for all user actions.
- **Protection Type:** Copyright
- **Acceptance Criteria:** All actions are logged and receipts are available for audit.
- **Risks & Mitigations:** Log tampering; mitigate with hash chaining.

18. SDK Attestation & Obfuscation

- **Definition:** SDK provides attestation and code obfuscation for security.
- **Protection Type:** Patent
- **Acceptance Criteria:** SDK passes attestation checks and is obfuscated.
- **Risks & Mitigations:** Obfuscation breakage; mitigate with regular updates.

19. Key Management & Telemetry Watermarking

- **Definition:** Manages encryption keys and embeds telemetry watermarks in data.
- **Protection Type:** Patent
- **Acceptance Criteria:** Keys are rotated and watermarks are present in telemetry.
- **Risks & Mitigations:** Key leakage; mitigate with HSM and audit.

20. Multi-App Aggregation

- **Definition:** Aggregates data and events across multiple apps/platforms.
- **Protection Type:** Copyright
- **Acceptance Criteria:** Data is unified and accessible from all apps.
- **Risks & Mitigations:** Data siloing; mitigate with schema normalization.

21. Cross-Vertical Hooks

- **Definition:** Integrates with external verticals (delivery, aviation, logistics) for event/data exchange.
- **Protection Type:** Patent
- **Acceptance Criteria:** Hooks are triggered and data is exchanged reliably.
- **Risks & Mitigations:** API drift; mitigate with contract tests.

22. Regulator Portal

- **Definition:** Provides API endpoints and logic for regulator access, audit, and compliance review.
 - **Protection Type:** Copyright
 - **Acceptance Criteria:** Regulator actions (view, audit, export) are supported and logged.
 - **Risks & Mitigations:** Unauthorized access; mitigate with RBAC and audit.
-

Remaining Processes (Wave 1-3, Legacy & Expansion)

23-40. See AGENT_GUIDE.md for legacy, expansion, and auxiliary processes.

- Each process follows the same documentation format: definition, protection, acceptance, risks/mitigations.
 - For full details, refer to AGENT_GUIDE.md and process-specific READMEs.
-

Appendix

- **IP/Trademark/Patent/Copyright:** See legal folder for registration details.
 - **Acceptance Criteria:** All processes validated by CI, test coverage, and manual review.
 - **Risks & Mitigations:** See risk register in docs/risk-register.md.
-