Privacy Policy

Global privacy notice for the Platform and all Game Modes

Effective: August 10, 2026 Last updated: August 10, 2026
Version: 1.0 Operator: NyFTee Original LLC
Address: 11 E. Orange Grove Rd., Tucson, Arizona 85704, United States

This Policy explains what personal data NyFTee Original LLC collects, why it is used, how it is shared and retained, and the choices and rights available to players worldwide.

1. Scope and Controller

Pink Slip Arcade is one connected interactive platform. Its website, account system, economy, marketplace, applications, digital assets, events, and all current or future games are collectively the Platform. Street Heat, Passive Lanes, Street Story, and every other playable experience are Game Modes of that Platform, not separate services.

NyFTee Original LLC is the controller or business responsible for personal data covered by this Policy. Our address is 11 E. Orange Grove Rd., Tucson, Arizona 85704, United States. Contact privacy@psrgame.com for privacy matters.

This Policy applies to the Platform, Game Modes, accounts, purchases, support, events, marketplace functions, wallet connections, official communities we control, and related websites. Third parties process data under their own notices when they act independently.

2. Data We Collect

Depending on how you use the Platform, we collect:

- Account and identity data: name or display name, email, age confirmation, country or region, authentication records, and account identifiers.
- Wallet and blockchain data: public wallet addresses, signatures used for authentication, token balances relevant to Platform functions, public transaction history, and smart-contract interactions. We do not request or store private keys or seed phrases.
- Gameplay and economy data: Game Mode activity, controls, results, progression, inventory, rewards, matchmaking, achievements, marketplace actions, fraud indicators, and anti-cheat telemetry.
- Purchase and transaction data: items, amounts, currency, timestamps, receipts, payment status, tax location, chargebacks, and limited payment metadata. Payment processors generally receive full card or funding details directly.
- Device, network, and usage data: IP address, device and browser type, operating system, language, identifiers, log events, crash data, approximate location derived from IP, referral source, and cookie or similar-technology data.
- Communications and content: support requests, reports, appeals, survey responses, feedback, public posts, usernames, uploads, chat or moderation records where available, and correspondence.
- Verification and compliance data: identity, age, location, sanctions, tax, or eligibility information when required for prizes, withdrawals, regulated features, fraud prevention, or law.
- Inferences: risk, fraud, moderation, skill, matchmaking, and preference inferences derived from the categories above.

3. Sources of Data

We obtain data:

- Directly from you when you register, play, connect a wallet, purchase, communicate, enter an event, or exercise rights.
- Automatically from devices, software, cookies, logs, and gameplay systems.
- From public blockchains and blockchain indexing services.
- From payment, identity, fraud, sanctions, analytics, hosting, marketplace, social-login, and customer-support providers.
- From other users, moderators, rights holders, event partners, and lawful public sources.

4. Why We Use Data and Legal Bases

We do not use a wallet signature to obtain ownership of assets or permission to move assets unless the transaction request clearly and separately discloses that result.

We use personal data for the following purposes and legal bases:

- Contract: create and secure accounts; authenticate users and wallets; operate Game Modes; deliver purchases; maintain inventory; process rewards; provide support; and administer competitions.
- Legitimate interests: prevent fraud, cheating, abuse, and security incidents; maintain service reliability; analyze performance; improve gameplay; protect users and rights; moderate content; and establish or defend legal claims.
- Consent: use non-essential cookies or targeted advertising where applicable; send optional marketing; process data for a purpose that law requires you to approve; and obtain any permission required for immediate digital delivery.
- Legal obligations: maintain financial and tax records; respond to lawful process; perform required sanctions, age, identity, prize, and compliance checks; and meet consumer, privacy, and safety duties.
- Vital or public interests: address an imminent threat to a person, the Platform, or the public where law recognizes that basis.

5. How We Disclose Data

We disclose data only as reasonably necessary to:

- Service providers processing hosting, content delivery, databases, authentication, security, analytics, support, email, payments, tax, identity, sanctions, fraud, and moderation under contractual restrictions.
- Independent services such as payment processors, wallets, Base, marketplaces, social platforms, and app stores when you direct or use the integration.
- Other players and the public for usernames, profiles, leaderboards, match results, public posts, creator content, marketplace listings, and public blockchain activity.
- Professional advisers, auditors, insurers, investors, and transaction counterparties under confidentiality and due-diligence safeguards.
- Authorities, rights holders, affected parties, or courts when reasonably necessary to comply with law, enforce rights, prevent harm, investigate misconduct, or protect security.
- A buyer, successor, or reorganized entity in a merger, financing, asset sale, insolvency, or similar transaction, subject to applicable notice and privacy requirements.

6. Public Blockchains

Public blockchain records are visible worldwide and may permanently associate a wallet address with transactions, assets, and other public data. Company does not control Base validators, explorers, indexers, wallets, or independent copies of the ledger and generally cannot edit or delete confirmed blockchain data.

A privacy request can apply to Company-controlled profiles, links, indexes, and off-chain records, but it cannot require Company to alter a public decentralized ledger it does not control. Consider using a wallet address that does not reveal unnecessary personal information.

7. Sale, Sharing, and Targeted Advertising

We do not sell personal data for money. We do not knowingly sell or share personal data of anyone under 18 because minors may not use the Platform.

If we use advertising or analytics technology that qualifies as a sale, sharing, or targeted advertising under applicable law, we will provide a clear opt-out control and honor legally recognized browser-based opt-out preference signals, including Global Privacy Control, where required. We will not use sensitive personal data to infer characteristics beyond permitted purposes.

8. Retention

We keep personal data only as long as reasonably necessary for the purposes described, including account operation, security, disputes, tax, fraud prevention, and legal obligations. We may retain de-identified or aggregated information that cannot reasonably identify you. Public blockchain data is retained by the network, not according to Company's deletion schedule. Typical target periods are:

- Active account and core gameplay records: for the account's life, then generally up to 3 years after closure unless a longer period is needed for ownership, fraud, disputes, or law.
- Purchase, payout, tax, and financial records: generally 7 years or the period required by applicable law.
- Security, sanctions, anti-cheat, and fraud records: generally up to 5 years after the relevant event, longer for an active investigation or repeat-abuse defense.
- Support, moderation, and appeal records: generally 3 years after closure of the matter.
- Raw technical and analytics logs: generally up to 12 months, then deleted or aggregated unless needed for security or debugging.
- Consent and legal-acceptance records: for the relationship plus the applicable limitation period.
- Backups: removed or overwritten on a rolling schedule, generally within 90 days after source deletion, subject to disaster-recovery integrity.

9. Security

We use administrative, technical, and organizational safeguards designed for the nature of the data and risks. These may include access controls, encryption in transit, credential protection, logging, testing, vendor review, least-privilege access, and incident response. No system, wallet, or blockchain is completely secure. Protect your devices and credentials and report suspected compromise to legal@psrgame.com.

10. International Data Transfers

Company is based in the United States and processes data there and in other countries where providers operate. These countries may have different privacy laws. Where required, we use recognized safeguards such as adequacy decisions, standard contractual clauses, the UK International Data Transfer Addendum or Agreement, or another lawful transfer mechanism. You may request information about applicable safeguards.

11. Your Privacy Rights

Subject to identity verification, legal exceptions, and regional applicability, you may request access, confirmation, correction, deletion, portability, restriction, objection, withdrawal of consent, or a list of categories and recipients. You may opt out of sale, sharing, targeted advertising, or certain profiling where law provides that right.

Submit requests to privacy@psrgame.com or through https://psrgame.com/legal/privacy-request. We will not discriminate against you for exercising a right. An authorized agent may act where permitted, but we will verify authority and identity. If we deny a request, you may appeal by replying with "Privacy Appeal" or emailing privacy@psrgame.com. You may also complain to your local privacy regulator.

12. EEA, Switzerland, and United Kingdom

Where the GDPR, UK GDPR, or comparable law applies, you have the rights described above and the right to lodge a complaint with a supervisory authority. Contract and legitimate-interest processing is limited to what is necessary and proportionate. You may object to legitimate-interest processing, and we will stop unless compelling lawful grounds or legal claims justify continuation.

Company will identify any legally required representative or data protection officer on the live Privacy page if and when that appointment becomes required. Mandatory local rights are not limited by this Policy.

13. U.S. State Privacy Notices

Residents of states with comprehensive privacy laws may have rights to know, access, correct, delete, port, opt out of sale or sharing, opt out of targeted advertising or qualifying profiling, limit certain sensitive-data uses, and appeal. We extend the core request process in Section 11 to users worldwide when reasonably feasible, even if a statute does not require it.

Categories collected and disclosed are listed in Sections 2 and 5; purposes are in Section 4; retention is in Section 8. We do not offer financial incentives in exchange for personal data unless we first provide a legally required notice explaining material terms.

14. Automated Decisions and Anti-Fraud

We use automated systems to support matchmaking, recommendations, fraud detection, anti-cheat, sanctions screening, moderation, and security. These systems may flag or temporarily limit activity. Where law provides a right regarding a decision with legal or similarly significant effects, you may request information and human review through the appeal process.

15. Minors

The Platform is for adults 18 and older. We do not knowingly collect personal data from minors. If we learn that a minor created an account, we will restrict it and delete or retain data as required for safety, fraud prevention, and law. Report suspected minor use to privacy@psrgame.com.

16. Cookies and Communications

The Cookie Policy explains browser storage and choices. You may unsubscribe from promotional email through the message control. We may still send transactional, security, legal, or service communications. Browser Do Not Track signals are not standardized; we honor legally recognized opt-out preference signals as described above.

17. Changes to This Policy

We may update this Policy as the Platform, vendors, or law changes. The updated date will appear at the top. We will provide additional notice and obtain consent where required for a material new use. Earlier versions will remain available through the Legal Center.

18. Contact

Privacy: privacy@psrgame.com. Legal: legal@psrgame.com. Mail: NyFTee Original LLC, Attn: Privacy, 11 E. Orange Grove Rd., Tucson, Arizona 85704, United States. Website: https://psrgame.com/legal/privacy.

© 2026 NyFTee Original LLC. Pink Slip Arcade. All rights reserved.