US Privacy Policy

Updated: April 24th, 2026

1. Introduction

This Privacy Policy explains how Fan Token Management, Inc. (“Socios”, “we”, “us”, or “our”) collects, uses, discloses and protects personal information about users of our websites, mobile applications and online services (together, the “Services”). It also describes your privacy rights and how to exercise them. If you do not agree with this Policy, please do not use the Services.

This Policy is intended for individuals in the United States. If we provide region-specific notices required by state law, they appear in the “State Privacy Rights” section or an accompanying addendum.

2. Contents of this Privacy Policy

1. Introduction
2. Contents of this Privacy Policy
3. Scope
4. Key definitions
5. Notice at collection
6. Sources of personal information
7. How we use personal information
8. Cookies and similar technologies
9. Disclosures of personal information
10. Sale, sharing and targeted advertising
11. Your privacy rights
12. How to exercise your rights
13. Your privacy choices
14. Financial incentives (if applicable)
15. Security
16. Data retention
17. International transfers
18. Links to third-party sources
19. Minors
20. Direct marketing
21. Updates
22. Fan Token Management Inc.– company details
23. State privacy rights addendum

3. Applicable Laws

This Policy applies to personal information we collect:

- Directly from you when you use the Services, create an account, contact support, participate in promotions, or otherwise interact with us.
- Automatically, including through cookies, SDKs, pixels and similar technologies.
- From third parties, such as identity verification providers, analytics partners, payment and fraud-prevention providers, marketing partners, and social media platforms, as permitted by law.

This Policy does not cover information subject to sector-specific rules (for example, certain financial information governed by the Gramm-Leach-Bliley Act) or publicly available information as defined by applicable law.

4. What is personal data?

- "Personal information" means information that identifies, relates to, describes, or can reasonably be linked with a particular consumer or household.
- "Sensitive personal information" includes, for example, government identifiers, precise geolocation, financial account credentials, and information about a consumer's racial or ethnic origin or criminal history, as defined by applicable law.
- "Sale," "share" and "targeted advertising" have the meanings given to them under applicable state privacy laws.

5. Personal data we collect about you

We collect the following categories of personal information. The examples are illustrative and may vary depending on how you interact with us.

- Identifiers: name, username, email address, postal address, phone number, device identifiers, IP address.
- Government identifiers: passport number, national ID or driver's licence number (for identity verification and legal compliance).
- Account and commercial information: account credentials, order history, in-app transactions, preferences.
- Internet or network activity: browsing history, app usage, referral URLs, interactions with our emails and adverts.
- Geolocation data: approximate location from IP; where you enable location services, more precise location for in-app features.
- Payment and financial information processed by our payment processors (transaction ID, payment method, amount, date).
- User content and communications: support tickets, survey responses, in-app or social interactions with our official channels.
- Inferences: profiles reflecting interests or preferences derived from other information.
- Sensitive personal information: government IDs, precise geolocation (if enabled), and any other elements you actively provide that qualify as sensitive under applicable law. We do not collect biometric templates.

Purposes for collection include: providing and improving the Services; account creation and maintenance; processing transactions; customer support; security and fraud prevention; analytics and service performance; personalisation; marketing and advertising; compliance with law; and business operations (including debugging, auditing, and quality assurance).

Retention: We retain personal information for as long as necessary to provide the Services, comply with our legal obligations, resolve disputes, protect our rights, and pursue legitimate business purposes. Retention periods vary by category and context; when no longer needed, information is deleted or anonymised in accordance with our data-retention schedule.

5.1 Personal data we collect – summary table (US states)

Category of personal information	Examples we collect	Sources	Purposes of use	Disclosure to service providers/partners	Sell/Share/ Targeted ads	Sensitive PI use	Typical retention
Identifiers	Name, email, username, postal address, phone, IP, device IDs	You; automatic collection; identity verification providers	Account creation, support, security, fraud prevention, marketing, analytics, legitimate purpose (for example, defense of claims)	Cloud hosting; support tools; security; analytics; marketing partners	Share/Targeted Ads: [Confirm Yes/No]; Sale for money: No	Not sensitive	5 Years from last use; more in case of fraud prevention as per dedicated regulations
Government identifiers (SPI)	Passport/ID/driver's licence (for KYC/verification)	You; identity verification providers	Fraud prevention, security	Identity verification vendors; security tools	No sale/share/targeted ads	Limited to permitted purposes (provide services, securit	Same as above

						y, compliance)	
Commercial information	Orders, in-app transactions, preferences	You; payment processors; automatic collection	Provide and improve services; fulfilment; analytics	Payment processors; fulfilment; analytics	Share/Targeted Ads: Yes; Sale: No	Not sensitive	Same as above
Internet/network activity	App/web usage, referral URLs, interactions with emails/ads	Automatic collection; analytics/advertising partners	Service operation, debugging, analytics, advertising/measurement	Analytics and ad-tech partners; security tools	Share/Targeted Ads: Yes; Sale: No	Not sensitive	Same as above
Geolocation	Approximate IP-based; precise when you enable	Automatic collection; device settings	Feature enablement, fraud prevention, analytics	Security/anti-fraud; analytics	Share/Targeted Ads: Yes for ad cookies/SDKs; Sale: No	Precise location treated as SPI; limited to permitted purposes where applicable	Same as above
Payment and financial information	Transaction information	You; payment processors	Payments, fraud prevention, compliance	Payment processors; anti-fraud	No sale/share/targeted ads	May include SPI elements under some laws; limited to permitted purposes	Same as above

User content/communications	Support tickets, survey responses, in-app interactions	You	Support, service improvement, dispute handling	Support platforms; CRM	No sale; Share for ads: No	Not sensitive	Specific period of each purpose
Inferences	Profiles about interests or preferences	Derived from other data	Personalisation, analytics, marketing	Analytics/marketing partners	Share/Targeted Ads: Yes; Sale: No	Not sensitive	5 years

Notes: “Sell,” “share,” and “targeted advertising” have state-law meanings. Where required, we honour eligible browser- or device-based opt-out signals (for example, GPC) and provide footer links to “Your Privacy Choices/Do Not Sell or Share”. If you participate in a loyalty, rewards, or referrals programme, see “Financial incentives” for additional disclosures required by law.

6. How and why we collect personal data

We collect personal information:

- Directly from you (for example, when you register, verify identity, make purchases, or engage with support).
- Automatically through cookies and similar technologies on our Sites and Apps.
- From service providers and partners (for example, cloud hosting, identity verification, analytics, advertising, payment processing, customer-support tools, and anti-fraud services).
- From publicly available sources and social media platforms, where permitted.

7. What we use your personal data for (purpose of processing)

We use personal information to:

- Provide, operate and secure the Services, including account registration, identity verification, fraud monitoring and incident response.
- Process transactions, payments and fulfilment; manage relationships and provide customer support.
- Personalise content and features; conduct analytics, measurement and research to develop and improve products and Services.
- Send administrative messages and, where permitted, marketing communications; manage preferences and subscriptions.
- Conduct advertising and audience measurement, including cross-device and cross-service operations, and frequency capping.
- Comply with law, legal process and law-enforcement requests; enforce our terms; and protect our users, our company and others.

- Support corporate transactions (for example, merger, acquisition or asset transfer), consistent with this Policy and applicable law.

8. Cookies

We and our partners use cookies, SDKs, pixels and similar technologies to operate the Services, measure engagement, understand usage, improve performance, and deliver or measure adverts. You can control cookies through your browser or device settings; essential cookies are required for the Services to function. Where required by law, we obtain your consent before using certain cookies.

9. Authorized disclosures

We disclose personal information to:

- Service providers and processors that perform services on our behalf (for example, hosting, security, analytics, payment processing, customer support, marketing and advertising).
- Business partners you choose to interact with through the Services (for example, official partners whose goods or experiences you access). For transparency, examples include: ticketing/experience fulfilment partners, event/venue operators, and retail/merchandise partners you select. Categories of data shared are limited to what is necessary to provide the requested experience (e.g., identifiers, order details) and are subject to contractual restrictions. Your information will not be used by such partners for their own marketing unless you authorise it.
- Affiliates within our corporate group for purposes consistent with this Policy.
- Law enforcement, regulators, government entities, courts and others where required by law or to protect rights, safety and security.
- Relevant parties in connection with a corporate transaction.
- Other third parties with your direction or consent.

We implement contractual and technical safeguards with recipients, as required by law.

10. Sharing of personal data with other categories of recipients

- We do not sell personal information for money.
- We may “share” personal information or process it for “targeted advertising” as those terms are defined under some state laws, for example when we use third-party advertising cookies or analytics that help deliver ads based on your activity across non-affiliated sites or apps. You can opt out of sharing/targeted advertising as described in “Your privacy choices”, or by using the “Do Not Sell or Share My Personal Information” / “Your Privacy Choices” link in the Site/App footer. Where required, we also honour recognised browser-based opt-out signals, such as GPC.

Where required by law, we process opt-out preference signals, including Global Privacy Control (GPC). If our practices change materially, we will update this Policy and the methods to exercise your choices.

11. Your rights under the data protection laws

Depending on your state of residence, you may have the right to:

- Access/know the categories and specific pieces of personal information we have collected about you, and details about our collection, use and disclosures.
- Correct inaccuracies in your personal information.
- Delete personal information.
- Receive your personal information in a portable format.
- Opt out of: (i) sale of personal information; (ii) sharing or processing for targeted advertising; and (iii) certain profiling/automated decision-making that produces legal or similarly significant effects.
- Limit the use and disclosure of sensitive personal information to certain permitted purposes (where applicable law provides this right).
- Appeal our decision if we decline to act on your request (available to residents of states that provide an appeal right).

We will not discriminate against you for exercising your privacy rights.

12. How to exercise your rights

- Submit a request by emailing dataprotection@socios.com with the subject line “Privacy Request” or by writing to the postal address in “Contact us”.
- If available, you may also use in-app privacy settings or a web form linked in your account settings.
- We will verify your identity using information we already hold, and may ask for additional information as needed. You may designate an authorised agent where your state law permits, subject to verification of both you and your agent.

Appeals: If we deny your request (for example, because we cannot verify it), you may submit an appeal using the same contact methods. We will explain the result of the appeal and any further options. We will respond to requests and appeals within the timeframes required by applicable law (generally within 30 days, which may be extended by a further 30 days where reasonably necessary).

13. Your privacy choices

- Marketing: You can unsubscribe from marketing emails via the link in the message. We may still send service or transactional messages.
- Cookies/advertising: Use your browser or device controls to block or delete cookies. To opt out of “sharing” or targeted advertising, use our “Do Not Sell or Share” / “Your Privacy Choices” control in the Site/App footer or settings. Where required by law, we

recognise certain browser- or device-based opt-out signals, including Global Privacy Control (GPC), and apply them to the browser or device that sends the signal.
- Location permissions: You can disable location services via your device settings; some features may not function without them.
- Sensitive personal information: Where available, use in-app settings or contact us to request limitation of sensitive personal information to permitted uses.

14. Financial incentives (if applicable)

If you participate in a rewards, referrals or loyalty programme that offers benefits (for example, discounts, bonus credits or early access) in exchange for personal information, we will provide a programme-specific notice describing the material terms, including: categories of personal information involved (typically identifiers and commercial information), how to opt in, how to withdraw, a reasonably related value of the data and the method used to calculate it, and how to exercise your rights without being penalised. Participation is voluntary and you may withdraw at any time via the programme settings or by contacting us.

Nevada residents: You may submit a request to opt out of sale under Nevada law by contacting us as described above with “Nevada Opt-Out” in the subject line.

15. Security measures

We implement administrative, technical and physical safeguards designed to protect personal information against unauthorised access, misuse, disclosure, alteration and destruction. No method of transmission or storage is completely secure; we maintain and improve our safeguards over time.

16. Retention periods

We retain personal information in line with the purposes described above and our records-management schedule, which considers the nature and sensitivity of the information, potential risk of harm from unauthorised use or disclosure, the purposes for which we process it and whether we can achieve those purposes through other means, and applicable legal, tax, accounting and regulatory requirements. When retention periods expire, we delete or anonymise the information.

17. Transfers to third countries

We generally store and process personal information in the United States. If we transfer information to other countries, we will do so in accordance with applicable law and with appropriate safeguards (for example, with the Standard Contract Clauses in force).

18. Links to third-party sources

The Services may link to third-party websites, services and features. Their privacy practices are governed by their own policies; we are not responsible for their content or practices

19. Minors

Our Site, App and services are not intended to be used by any person under the age of eighteen (18) and therefore We will never intentionally collect any Personal Data from such persons. If You are under the age of consent, please consult and get Your parent's or legal guardian's permission to use the site, App and any of Our other services.

We shall consider that any Personal Data of any persons under the age of eighteen (18) received by Us, shall be sent with the proper authority from the holder of parental responsibility over the child and that the sender can demonstrate such authority at any time, upon Our request.

20. Direct marketing

Where required, we obtain your consent before sending marketing by electronic means. You may withdraw consent or opt out at any time as described in "Your privacy choices".

21. Updates

We may update this Policy from time to time. Changes will be posted here with a new "Updated" date. Material changes will be highlighted by reasonable means. Your continued use of the Services after an update signifies your acceptance of the revised Policy.

22. Fan Token Management, Inc.– company details

Fan Token Management, Inc., with registered office in the State of Delaware, at 838 Walker Rd., Suite 21-2, Dover, Delaware, 19904, USA. Email: dataprotection@socios.com Subject line: "PRIVACY REQUEST"

---

23. State privacy rights addendum

This addendum supplements the Policy for residents of California, Colorado, Delaware and Nevada. It uses terms defined by those laws.

California

- Applicable to California residents. You have rights to know/access, correct, delete, and receive your information in portable format; to opt out of "sale" and "sharing" and of processing for targeted advertising; and to limit the use/disclosure of sensitive personal information to permitted purposes. We honour recognised browser-based opt-out signals (for example, Global Privacy Control) where required..

Nevada

- Applicable to Nevada residents. You may direct us not to sell your covered information as defined by Nevada law by contacting us with “Nevada Opt-Out” in the subject line, as described in How to exercise your rights. We do not otherwise offer a financial incentive for sale.

Colorado

- Applicable to Colorado residents. You have rights to access, correct, delete, data portability, and to opt out of sales, targeted advertising, and certain profiling. An appeal mechanism is available if we decline to act on a request. We honour recognised universal opt-out mechanisms where required by Colorado law.

Delaware

- Applicable to Delaware residents. You have rights to access, correct, delete, data portability, and to opt out of sales, targeted advertising, and certain profiling. An appeal mechanism is available if we decline to act on a request. We honour recognised universal opt-out mechanisms where required by Delaware law.