Privacy Policy
Effective Date: March 18, 2026

1. Who we are
This Privacy Policy describes how FitX brands Inc. (referred to as “FitX,” “we,” “us,” or “our”) collects, uses, discloses, and protects personal information when you visit our website, use our apps, participate in foot-scan sessions, or purchase our products and services.

2. Personal information we collect
We collect the following categories of personal information:

2.1 Identifiers and contact information

Email address, phone number, first and last name, and account ID.

We use this information to create and manage your account, send order receipts, deliver foot-scan links, and provide customer support.

2.2 Device, network, and usage information

IP address at signup and for rate limiting; User-Agent string; device type (desktop/mobile/tablet); referrer URL; page URLs visited; and country inferred from IP address.

We use this information for security, fraud prevention, analytics, and to understand how users interact with our services.

2.3 Authentication and security information

Password hashes (we never store plaintext passwords), email verification tokens, password reset tokens, magic link tokens, phone-based one-time passcodes delivered via Twilio, OAuth provider identifiers (such as Google “Sign in with Google”), and JSON Web Tokens (JWTs) embedded in scan link URLs and QR codes.

We use this information to authenticate you, secure your account, enable password-less login, and control access to the FitX scan app.

2.4 Behavioral and survey information

Event-level data about how you use our site and apps, including button clicks, form interactions, survey steps, scroll depth, and section impressions.

Responses to optional surveys about pain points, current footwear brand, running frequency, and motivation.

2.5 Financial and transaction information

Order amount and currency, payment status, payment provider transaction ID, order type, customization details, and billing address information shared with our payment processor.

We do not store full credit card numbers; card data is handled by our payment provider (currently Square).

2.6 Biometric foot-scan data
When you use the FitX foot-scan experience, we collect biometric data as described in our Biometric Foot-Scan Data Collection Notice & Consent and Biometric Foot-Scan Data Retention & Destruction Policy, including:

3D scans or images of your feet.
Foot geometry measurements.
Gait or pressure characteristics (if applicable).

Because these measurements can uniquely identify you, they qualify as biometric data under certain privacy laws. We treat them as sensitive and apply additional protections and conditions described in Section 7 below.

2.7 Derived and profiling data

Derived metrics such as intent or propensity scores, average dwell time, scroll-depth percentage, time-to-submit, return-visit count, acquisition source/campaign, and inferences such as primary pain point or benchmark brand.

We derive these from the information described above for analytics, personalization, and marketing optimization.

3. How we use personal information
We use personal information to:

Provide, operate, and maintain our services, including account creation, order processing, scan workflows, and customer support.

Authenticate you and secure our services, including fraud prevention, abuse detection, and rate limiting.

Analyze usage and performance, including funnel completion, scroll behavior, and content engagement, to improve our website, apps, and products.

Personalize your experience, including tailoring recommendations, on-site content, and marketing messages.

Measure and improve our marketing, including sending conversion events, order values, and hashed identifiers to advertising platforms for attribution and optimization.

Comply with legal obligations, resolve disputes, and enforce our agreements.

Where required by law, we rely on your consent (for example, certain cookies/trackers or biometric collection) or on our legitimate interests (for example, security, basic analytics, and service improvement) as our legal bases for processing.

4. Cookies, and similar technologies
We use cookies and similar technologies to recognize you and to understand how you interact with our services.

We store identifiers in your browser such as cookies and similar browser storage technologies in your local storage (for example: anonymous visitor IDs, session IDs, consent preferences, survey answers, scan session state, and CCPA opt-out flags).

We may also read and set HTTP cookies, including a fallback anonymous ID cookie, to maintain sessions and support analytics and conversion tracking.

We use pixels and tags from advertising and analytics partners (such as Meta Pixel) and security tools (such as Google reCAPTCHA Enterprise) that may read or set identifiers and collect device and browsing information.

In some jurisdictions (such as the EU/UK), these technologies are treated like cookies. Where required, we present a consent banner allowing you to manage preferences for analytics and marketing storage and tracking.

You can control cookies and similar technologies through your browser settings. Some features may not function properly if you disable them.

5. Biometric data: notice, use, retention, and rights
This section summarizes and incorporates our biometric foot-scan documents.

5.1 Notice of biometric data collection
To provide accurate product sizing and personalized fit recommendations, we collect a 3D scan of your feet, which may include foot geometry measurements and gait or pressure characteristics. Because these measurements can uniquely identify you, they qualify as biometric data under certain state laws.

5.2 How we use biometric foot-scan data
We use your foot-scan data only to:

Generate fit and sizing recommendations.

Create custom-fit or personalized products.

Improve scan accuracy and system performance.

Create and use deidentified and aggregated data derived from your use of the services for analytics, product improvement, and other lawful business purposes, as described in this Privacy Policy.

We do not sell, lease, or otherwise profit from biometric data, and we do not use biometric data for advertising or marketing.

5.3 Biometric retention and destruction
Your biometric data is retained according to our Biometric Foot-Scan Data Retention & Destruction Policy:

If you create an account: retained for up to 24 months from your most recent interaction (such as a new scan, login, or purchase), unless you request deletion sooner.

If you do not create an account: retained for no longer than 90 days after your scan, unless you opt-in to extended storage; after that, it is permanently deleted.

Upon request: we delete your biometric data within 30 days of receiving a verifiable deletion request, subject to applicable law.

We permanently destroy biometric templates and 3D scan files, including removal from backups during scheduled cycles and vendor-secured destruction for third-party systems, so destroyed biometric data cannot be recovered.

5.4 Biometric security
We protect biometric data using industry-standard security measures, including encryption and access controls, consistent with applicable biometric privacy laws.

5.5 Biometric rights and consent
Where required by law, we obtain your explicit consent before collecting biometric data; you may withdraw consent at any time. Depending on your state, you may have rights to:

Request access to your biometric data.
Request deletion of biometric data.
Receive disclosures about biometric collection.
Opt out of additional uses, as permitted by law.
You can exercise these rights using the contact information in Section 11.

6. Ad platforms and “sharing” of personal information
We work with advertising platforms such as Meta, Google Ads, TikTok, Pinterest, and Reddit to measure and improve our marketing campaigns.

We may send these partners:

Conversion events (for example, purchases), associated order values, and technical identifiers used to connect your visit to the ad that brought you here.

Hashed identifiers (such as email or phone number hashed with a one-way function) to help match events to existing platform accounts.

For Meta, events can be sent both via the browser (Meta Pixel) and from our servers (Conversions API), deduplicated by event ID.

Under laws like the California Consumer Privacy Act (as amended by CPRA), this may constitute “sharing” personal information for cross-context behavioral advertising. Where required, we provide a “Do Not Sell or Share My Personal Information” mechanism to allow you to opt out. Our current browser-based opt-out uses cookies

and similar browser storage technologies in your local storage flag, which will reset if you clear browser storage; we may also offer account-level persistence.

7. Service providers and third parties
We share personal information with third-party service providers who process data on our behalf, including:

Payment processing: e.g., Square (card tokenization, payment processing).

SMS verification and messaging: e.g., Twilio (phone number, OTP codes, scan link URLs).

Email delivery: e.g., Postmark (email address, order details, QR code images and scan links).

Cloud infrastructure: e.g., Google Cloud Platform (hosting, storage, databases).

Security and bot detection: e.g., Google reCAPTCHA Enterprise (browser signals for bot/fraud prevention).

3D reconstruction: e.g., IBV for reconstructing 3D models from foot photos and sensor data.

Advertising and analytics: e.g., Meta, Google Ads, TikTok, Pinterest, Reddit for conversion tracking and marketing measurement.

These providers are authorized to process personal information only as needed to provide their services and are bound by confidentiality and security obligations.

8. Data retention and deletion
We retain personal information for as long as necessary to fulfill the purposes described in this policy, to comply with legal obligations, and to resolve disputes.

Orders, invoices, and core account data may be retained for longer where required by tax, accounting, or legal obligations.

Security and rate-limiting data (including IP or email identifiers used for abuse prevention) is stored only as long as needed and is periodically deleted or anonymized.

We maintain a deletion process that, when you request account deletion, removes your personal data across our systems (including orders, scans, events, and machine-learning features) and deletes associated scan files from storage, subject to limited legal exceptions.

Information already sent to independent third parties (such as ad platforms) may be subject to their own policies and cannot always be recalled by us; you may need to contact those providers directly to exercise your rights in their systems.

9. Your privacy rights
Depending on your location, you may have rights such as:

Accessing the personal information we hold about you.

Requesting correction of inaccurate information.

Requesting deletion of your personal information.

Objecting to or restricting certain processing, including profiling and targeted advertising.

Withdrawing consent where we rely on consent (for example, biometric data or certain cookies).

Exercising specific rights under CCPA/CPRA (such as the rights to know, delete, and opt out of “sale” or “sharing” of personal information).

You can exercise these rights by contacting us using the information below. We may need to verify your identity before responding.

10. Children’s privacy
Our services are not directed to children under 13, and we do not knowingly collect personal information from children under 13. If we learn that we have collected such information without appropriate consent, we will take steps to delete it.

11. International transfers
If you are located outside the country where our systems are hosted, your information may be transferred to, stored, and processed in other countries that may have data protection laws different from those in your jurisdiction. Where required, we use appropriate safeguards (such as Standard Contractual Clauses) for such transfers.

12. How to contact us

If you have questions about this Privacy Policy, biometric data, or would like to exercise your rights, contact us at:

Email: hello@fitxlab.com

Mailing Address: 600 N Broad Street Suite 5-912, Middletown, DE 19709

13. How to Exercise Your Privacy Rights

To exercise your privacy rights, please email us at hello@fitxlab.com with the subject line “Privacy Request.” Please include your full name, the email address associated with your account or interaction with us, the right you would like to exercise, and enough information for us to locate your records. We may need to verify your identity before processing your request, including by confirming the request through the email address associated with your account or by requesting additional information reasonably necessary to verify your identity. Authorized agents may submit requests on your behalf where permitted by law, but we may require proof of authorization and may still ask you to verify your identity directly. We will respond within the time required by applicable law. In some cases, we may deny or limit a request where permitted by law, including where we cannot verify your identity or must retain certain information for legal, security, fraud-prevention, or transaction-completion purposes.

14. Changes to this policy

We may update this Privacy Policy from time to time. If we make material changes, we will notify you by updating the “Effective Date” and, where appropriate, by additional notice (such as on our website or via email).