

## PRIVACY POLICY

This Privacy Policy explains how [Precision Project Flow], a [New York Limited Liability Company] (“**Company**,” “we,” “our,” or “us”), collects, uses, discloses, and protects information when you access or use our online marketplace platform and related services (collectively, the “**Platform**”).

This Privacy Policy applies to all users of the Platform, including Vendors, Buyers, and any individual acting on behalf of a business entity. By accessing or using the Platform, you agree to the practices described in this Privacy Policy.

The Platform is intended for business users only. We collect and process information related to businesses and their representatives in connection with the operation of a business-to-business engineering marketplace.

This Privacy Policy is designed to comply with applicable U.S. privacy standards. It does not provide rights or disclosures required under laws such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) unless expressly stated.

For purposes of this Privacy Policy, “**Personal Information**” means information that identifies, relates to, describes, or can reasonably be linked to an identified or identifiable individual. “**Vendor**,” “**Buyer**,” and “**User**” have the meanings defined in the Terms of Service.

### 1. Information We Collect

#### 1.1. **Information You Provide to Us**

1.1.1. *Account Information.* When you register for an account, we collect information such as your name, business name, job title, email address, phone number, and any other details required to create and maintain your account.

1.1.2. *Vendor Onboarding Information.* Vendors may be required to submit additional business details during manual onboarding, which may include business verification documents, tax information, regulatory or licensure materials, and any other information needed to assess eligibility.

1.1.3. *Listings and User Content.* Vendors may upload product descriptions, technical specifications, images, certifications, engineering documents, and other materials. Buyers may submit inquiries, order information, or transaction-related messages.

1.2. **Communications.** When you communicate with us or other Users through the Platform, we collect the content of those communications, including messages, attachments, and metadata.

#### 1.3. **Information We Collect Automatically**

1.3.1. *Device and Usage Data.* We collect information about the devices you use to access the Platform, including IP address, browser type, operating system, device identifiers, and language settings.

1.3.2. *Activity Data.* We collect information about your activity on the Platform, such as the pages you view, links you click, listings you browse, and actions you take.

1.3.3. *Cookies and Similar Technologies.* We use cookies, pixel tags, and similar tools to collect information about your interactions with the Platform. Cookies help us personalize content, maintain session data, and analyze performance.

## 1.4. Information We Receive from Third Parties

1.4.1. *Stripe*. When you use Stripe to process payments, we may receive information related to identity verification, payout eligibility, fraud prevention, and transaction status.

1.4.2. *Analytics Providers*. We may receive aggregated or anonymized information from analytics tools, such as Google Analytics, that helps us understand Platform performance.

1.4.3. *Public and Business Databases*. We may collect publicly available business information to verify Vendor identity or supplement account information.

## 2. How We Use Information

2.1. **To Operate and Maintain the Platform.** We use information to provide, manage, and improve the Platform, including account creation, Vendor onboarding, listing management, transaction facilitation, and general platform functionality.

2.2. **To Process Transactions.** We use information to enable payments and payouts through Stripe, verify transaction details, and comply with financial or operational requirements related to payment processing.

2.3. **To Verify Identity and Conduct Vendor Review.** We use information submitted during Vendor onboarding, along with information received from third parties, to confirm business identity, assess eligibility, and maintain the integrity of the Platform.

2.4. **To Facilitate Communication.** We use information to enable communications between Vendors and Buyers, including messaging, notifications, and responses to inquiries.

2.5. **To Provide Customer Support.** We use information to respond to User questions, resolve issues, and provide technical or administrative support.

2.6. **To Enforce Safety and Compliance.** We use information to investigate and address violations of the Terms of Service, detect fraudulent or harmful activity, enforce platform rules, and comply with legal and regulatory obligations.

2.7. **For Analytics and Improvement.** We use information to analyze Platform performance, understand usage patterns, develop new features, and improve Platform efficiency and security.

2.8. **To Send Administrative Communications.** We use information to send notices about account activity, policy updates, operational changes, and other communications relevant to the use of the Platform.

2.9. **For Legal Purposes.** We use information to comply with applicable laws, respond to legal requests, enforce contractual rights, and protect the rights, property, and safety of the Platform and its Users.

## 3. How We Share Information

### 3.1. Sharing with Other Users

3.1.1. *Vendor Information Shared with Buyers.* When a Vendor lists products or services on the Platform, certain information becomes visible to Buyers, including business name, profile information, listings, technical details, and any other information the Vendor chooses to provide.

3.1.2. *Buyer Information Shared with Vendors.* When a Buyer initiates or completes a transaction, we share the Buyer's relevant business and contact information with the Vendor so the Vendor can fulfill the order and communicate with the Buyer.

3.1.3. *Messaging and Communications.* Communications sent through the Platform may be visible to the recipient, stored on the Platform, and reviewed in accordance with this Privacy Policy and our Terms of Service.

## 3.2. **Sharing with Third-Party Service Providers**

3.2.1. *Stripe.* We share information necessary for payment processing, identity verification, fraud detection, payout eligibility, and dispute resolution with Stripe.

3.2.2. *Analytics Providers.* We may share anonymized or aggregated usage data with analytics tools, such as Google Analytics, to help evaluate Platform performance and user engagement.

3.2.3. *Hosting and Operational Providers.* We may share information with cloud hosting providers, email delivery services, and customer support tools that assist in operating and supporting the Platform.

3.3. **Legal and Regulatory Disclosures.** We may disclose information if required to do so by law or if we believe in good faith that such disclosure is necessary to:

- (a) comply with legal or regulatory obligations;
- (b) respond to lawful requests from courts, regulatory agencies, or law enforcement;
- (c) enforce the Terms of Service;
- (d) investigate and address fraud, security issues, or technical problems; or
- (e) protect the rights, property, or safety of the Platform, our Users, or the public.

3.4. **Business Transfers.** If we engage in a merger, acquisition, financing, sale of assets, or similar transaction, information may be shared with or transferred to the relevant acquiring or successor entity. We will require any successor to handle Personal Information in a manner consistent with this Privacy Policy.

## 4. **Cookies, Tracking Technologies, and App Data Collection**

We use cookies, mobile identifiers, and similar tracking technologies to operate the Platform, understand usage patterns, improve performance, and support security. If we launch a mobile application, we may also use device identifiers and software development kits (“**SDKs**”) consistent with Apple’s and Google’s developer requirements.

### 4.1. **Web-Based Tracking Technologies**

4.1.1. *Cookies.* Cookies are small text files stored on your device. We use cookies to maintain session information, remember your preferences, authenticate Users, support security features, and analyze Platform usage.

4.1.2. *Pixel Tags and Web Beacons.* These are small code snippets that help us measure the effectiveness of communications, track usage patterns, and understand how Users navigate the Platform.

4.1.3. *Log Files.* We collect log information, such as IP addresses, browser types, pages viewed, timestamps, and referring URLs, to diagnose issues and maintain system integrity.

**4.2. Mobile App Technologies (If Applicable).** If you access the Platform through a mobile application, we may use the following:

4.2.1. *Device Identifiers.* We may collect identifiers such as device ID, operating system version, hardware model, and mobile network information.

4.2.2. *Mobile Analytics SDKs.* We may integrate analytics tools that collect app usage data, crash reports, performance metrics, and user engagement information.

4.2.3. *Push Notifications.* If enabled, we may use your device token solely to send operational notifications, such as order updates or account alerts. You may disable notifications through your device settings.

4.2.4. *App Tracking Transparency (Apple).* If any feature involves tracking across other companies' apps or websites for advertising or measurement purposes, we will request permission in accordance with Apple's App Tracking Transparency framework. We do not currently engage in cross-app tracking or targeted advertising.

4.2.5. *Google Play Data Safety.* If distributed through Google Play, we will disclose all data collected, used, and shared in compliance with Google's Data Safety requirements.

**4.3. Categories of Data Collected Through Cookies and Tracking Tools.** We may collect the following categories of data:

4.3.1. *Usage data* (interactions, pages viewed, features used)

- (a) Device and browser information
- (b) Session identifiers and authentication tokens
- (c) Performance data, crash logs, and diagnostics
- (d) IP address and general location information (city/state level)
- (e) Metadata related to messages or files sent through the Platform

4.4. **Purposes of Tracking.** We use tracking technologies for the following purposes:

- (a) *Platform functionality:* account login, session management, security
- (b) *Analytics and performance:* understanding user behavior and improving features
- (c) *Operational communications:* remembering choices and preferences
- (d) *Fraud prevention:* detecting suspicious behavior or unauthorized access

4.5. **Third-Party Analytics and Service Providers.** We may use third-party tools, such as Google Analytics, to help us understand usage patterns. These providers may set their own cookies or collect information directly through their SDKs. We do not allow third-party advertisers to collect information for ad targeting.

**4.6. User Controls and Consent**

4.6.1. *Browser Controls.* You may block or delete cookies through your browser settings. Some essential cookies are required for core functionality and cannot be disabled.

4.6.2. *Mobile App Controls.* You may disable app tracking (if it was ever enabled) in your device's privacy settings. You may disable push notifications at any time through your device's system settings. You may control analytics collection if your device or operating system provides that option.

4.7. **Effect of Disabling Tracking Tools.** If you disable cookies or tracking tools, certain features of the Platform may not function as intended, including login, session persistence, or account features.

4.8. **Do Not Track Signals.** The Platform does not respond to browser-based Do Not Track signals. Industry standards are evolving, and we may update this approach if standards or regulations change.

## 5. Data Retention

5.1. **Retention of Account Information.** We retain account information, including contact details, business information, and profile data, for as long as your account is active. If you close your account, we may retain this information as required for operational, legal, tax, or compliance purposes.

5.2. **Retention of Vendor Onboarding Materials.** We retain Vendor verification documents, regulatory materials, and any onboarding information submitted during manual approval for as long as the Vendor maintains an account. After account closure, we may retain these records where necessary to comply with legal obligations, support audit requirements, or resolve disputes.

5.3. **Retention of Transaction Records.** We retain transaction data, including purchase history, payment information received from Stripe, communications, and related metadata, to comply with financial reporting, tax obligations, fraud prevention, and recordkeeping requirements.

5.4. **Retention of Listings and User Content.** We may retain copies of listings, technical specifications, engineering documents, and other User content after account closure if retention is necessary for compliance, dispute resolution, or operational integrity. We may also retain anonymized or aggregated versions for analytics and research.

5.5. **Retention of Cookies, Logs, and Analytics Data.** Cookies may remain on your device until you delete them or they expire. Server logs and analytics data are retained for varying periods, depending on their purpose, typically 12 to 36 months. Diagnostic, crash, and performance data collected through mobile SDKs may be retained in accordance with Apple and Google requirements and our internal operational needs.

5.6. **Criteria for Retention.** When determining retention periods, we consider legal and regulatory obligations; operational requirements; the nature of the data; potential for disputes or fraud; system integrity and security needs.

5.7. **Deletion Upon Request.** Users may request deletion of certain Personal Information. We will review each request and delete information where feasible, subject to legal obligations, audit and compliance requirements, our need to maintain transaction records, and fraud prevention or security considerations.

5.8. **Anonymization.** When information is no longer needed and deletion is neither required nor practical, we may anonymize the data so it cannot be linked to an identifiable individual or business.

## 6. Data Security

6.1. **Safeguards We Use.** We use administrative, technical, and physical safeguards designed to protect Personal Information from unauthorized access, disclosure, alteration, or destruction. These safeguards may include encryption, access controls, secure servers, firewalls, and regular monitoring of system activity.

6.2. **Limited Access.** We restrict access to Personal Information to personnel who need the information to operate the Platform, provide support, or fulfill legal obligations. Individuals with access must agree to maintain the confidentiality and security of the information.

6.3. **Third-Party Security.** We require third-party service providers, including Stripe, hosting providers, and analytics vendors, to use commercially reasonable measures to protect Personal Information consistent with industry standards.

6.4. **No Absolute Security Guarantee.** We take steps to protect Personal Information, but no method of transmission over the internet or method of electronic storage is completely secure. We cannot guarantee the absolute security of information transmitted to or stored on the Platform.

6.5. **User Responsibility.** Users are responsible for maintaining the security of their account credentials and for restricting access to devices used to access the Platform. If you believe your account has been compromised, you must notify us immediately.

6.6. **Security of Mobile Applications (If Applicable).** If the Platform is offered as a mobile app, we will implement mobile-specific safeguards, including encryption at rest and in transit, secure key storage, device-specific authentication tokens, and compliance with mobile operating system security guidelines. Users may enhance security by enabling biometric authentication or device-level protections.

6.7. **Incident Response.** If we discover a security breach involving Personal Information, we will take reasonable steps to contain the incident, investigate its cause, notify affected Users where required by law, and implement measures to prevent recurrence.

## 7. International Data Transfers

7.1. **Processing in the United States.** The Platform is operated from the United States. If you access the Platform from outside the United States, your information may be transferred to, stored in, and processed in the United States, where privacy laws may differ from those in your jurisdiction.

7.2. **Consent to Transfer.** By using the Platform, you consent to the transfer of your information to the United States for processing in accordance with this Privacy Policy and U.S. privacy laws and regulations.

7.3. **Vendors Located Outside the United States.** Vendors operating outside the United States acknowledge that information shared through the Platform, including communications with U.S. Buyers, may be transferred to and stored in the United States.

7.4. **Data Transfers to Third Parties.** Certain third-party service providers, including Stripe and analytics providers, may process information in the United States or other countries. We require these providers to use commercially reasonable safeguards when handling Personal Information.

7.5. **No International Privacy Frameworks.** We do not rely on international data transfer frameworks such as GDPR adequacy decisions or Privacy Shield programs. If the Platform later serves Users subject to such laws, we may update our practices to comply with applicable requirements.

## 8. Third-Party Links

8.1. **Links to External Websites.** The Platform may contain links to third-party websites, applications, or services. These linked sites are not owned, controlled, or operated by us, and we are not responsible for the content, privacy practices, or security of those third parties.

8.2. **No Endorsement.** Links to third-party sites are provided for convenience only and do not constitute an endorsement or recommendation. Users access third-party sites at their own risk.

8.3. **Review of Third-Party Policies.** We encourage Users to review the privacy policies, terms of service, and security practices of any third-party site or service they access through the Platform. Third-party practices may differ significantly from those described in this Privacy Policy.

8.4. **Third-Party Data Collection.** Third-party sites or services may independently collect information about you, including through cookies, SDKs, or other tracking technologies. We do not control and are not responsible for such collection.

## **9. Children's Privacy**

The Platform is intended for use by businesses and their authorized representatives. It is not directed to children, and we do not knowingly collect Personal Information from individuals under 18. Users must be at least 18 years old to create an account or use the Platform. If we learn that we have collected Personal Information from a minor under 18, we will delete the information as soon as reasonably possible. If you believe that a minor has provided Personal Information to us, please contact us using the information in Section 13 so we can take appropriate steps.

## **10. User Rights**

10.1. **Access to Information.** Users may access the information associated with their account by logging into the Platform. This includes profile information, business details, listings, and communication history.

10.2. **Correction of Information.** Users may update or correct certain account information at any time through their account settings. If you are unable to make a correction, you may contact us using the information in Section 13.

10.3. **Request for Deletion.** Users may request deletion of certain Personal Information. We will evaluate each request and delete information where required or permitted by law, subject to our need to retain information for legal, tax, or regulatory obligations; retention of transaction records; fraud prevention and security purposes; and operational requirements, such as account closure verification.

10.4. **Limitations on Deletion.** We may be unable to delete certain information if it is needed to complete an active or pending transaction, maintain accurate financial or tax records, comply with legal or regulatory requirements, or enforce our rights under the Terms of Service.

10.5. **Communications Preferences.** Users may opt out of certain non-essential email communications by following the instructions in those communications. Administrative and transactional communications are required to operate the Platform and cannot be opted out of.

10.6. **No Extended Rights Under Foreign Laws.** Because the Platform operates under U.S. privacy standards, Users do not have rights provided under laws such as the GDPR or CCPA unless such laws expressly apply to the User and the Platform's operations.

## **11. Choices and Controls**

11.1. **Account Settings.** Users may update their profile information, business details, password, and communication preferences through their account settings. Keeping this information current is the User's responsibility.

11.2. **Cookie Management.** Users can manage, block, or delete cookies through browser settings. Essential cookies are required for core Platform functionality and cannot be disabled. Disabling other cookies may affect performance or functionality.

11.3. **Email Communications.** Users may opt out of marketing or informational emails by following the unsubscribe instructions included in those communications. Users cannot opt out of administrative messages, including notices related to transactions, security, or account status.

11.4. **Mobile App Controls (If Applicable).** Users may disable push notifications through their device settings. Users may disable analytics or tracking tools through their device OS settings if supported. Users may revoke tracking permissions through Apple's App Tracking Transparency framework or Google Play controls if the Platform ever uses cross-app tracking.

11.5. **Do Not Track.** The Platform does not respond to browser-based Do Not Track signals. Users may control data collection through the tools described in this Section.

11.6. **Review of This Policy.** Users may review this Privacy Policy at any time to understand how information is collected and used. Continued use of the Platform constitutes acceptance of any updates described in Section 12.

## **12. Changes to the Privacy Policy**

12.1. **Right to Update.** We may update or modify this Privacy Policy at any time. Updated versions will be posted on the Platform, and the "Last Updated" date will be revised accordingly.

12.2. **Notice of Material Changes.** If we make changes that materially affect how we collect, use, or share Personal Information, we may provide additional notice by email or through the Platform. Users are responsible for reviewing updated versions of the Privacy Policy.

12.3. **Effective Date.** Changes become effective when posted unless a later effective date is stated. Continued use of the Platform after the effective date constitutes acceptance of the updated Privacy Policy.

12.4. **Historical Versions.** We are not required to maintain or provide access to previous versions of this Privacy Policy. The most current version will remain available on the Platform.

## **13. Contact Information**

13.1. **How to Contact Us.** If you have questions about this Privacy Policy or our data practices, you may contact us at:

[Precision Project Flow LLC]  
418 Broadway Ste N, Albany, NY 12207 US  
[Precisionprojectflow@gmail.com]

**Privacy Requests.** Users may submit requests to access, correct, or delete Personal Information using the contact information above. We may require verification of identity or authority before responding to certain requests.

13.2. **Data Protection Inquiries.** If you have concerns about the handling of Personal Information, please contact us using the methods provided. We will review and respond to inquiries in a reasonable timeframe.