



Potoo Privacy Policy

2026 - 2027

Document Version

Ver	Updated By	Description	Action	Date
1.0	Ean Cravenho	Version 1 Release	Publish	01/09/2026

Overview

This General Privacy Policy describes how Potoo Marketing LLC (d.b.a. Potoo Solutions) collects, uses, protects, and retains personal information across its operations. It consolidates the Company's privacy posture covering the marketplace data underlying its services and the business contact and personnel information handled in the ordinary course of business, and serves as the authoritative privacy reference for client security assessments and vendor questionnaires.

Table of Contents

1. Purpose & Scope
2. Data We Process
3. How We Use Data
4. Legal Bases
5. Sharing & Subprocessors
6. Data Retention & Destruction
7. Security Measures
8. Data Subject Rights
9. Policy Review

Approval / Authorization

Ver	Name	Title	Action	Date
1.0	Fred Dimyan	CEO	Approved	01/12/2026

1. Purpose & Scope

This policy applies to all personal information processed by Potoo Marketing LLC (d.b.a. Potoo Solutions): the marketplace seller information collected in the delivery of digital shelf monitoring and brand protection services, the business contact information of client personnel, and the personnel information of Potoo employees. The detailed scope and legal bases governing marketplace seller data are defined in the companion Potoo Data Storage Policy, which this policy incorporates by reference.

2. Data We Process

- **Marketplace seller data.** Marketplace pricing and seller offer data, and publicly listed business contact information of marketplace sellers, collected exclusively from publicly accessible marketplace pages. This contact information is the only

category within Potoo's service data scope capable of containing personal information, and only where the seller is a natural person.

- **Client contact data.** Business names, titles, business email addresses, and business phone numbers of client personnel, maintained in the Company's CRM for account management and service delivery.
- **Employee data.** Information required for employment administration, payroll, and benefits, processed through the Company's HR platform, and identity information required for IT provisioning.

We do not collect consumer data, household data, sensitive personal information, health information (HIPAA), financial account data (GLBA), or any data obtained from non-public sources.

3. How We Use Data

- Delivering digital shelf monitoring and brand protection services to clients.
- Conducting enforcement communications with marketplace sellers on behalf of clients, governed by the Mailgun Security Posture document.
- Managing client relationships, support, and service operations.
- Administering employment, payroll, and internal IT systems.

Potoo does not sell or rent personal information, and does not use personal information for advertising.

4. Legal Bases

4.1 United States

Marketplace seller information constitutes publicly available information and is excluded from the definition of "personal information" under applicable US state privacy law, including the CCPA/CPRA and analogous state statutes. The individuals concerned act in a commercial context as marketplace traders. Potoo's data practices are further governed by the fair-practice framework of the FTC Act § 5.

4.2 European Union / EEA

Where seller information relates to an identifiable natural person, Potoo processes that data as a controller under the GDPR on the lawful basis of legitimate interest (Art. 6(1)(f)): brand protection and marketplace monitoring conducted on behalf of the brand owners whose products those sellers offer. Client and employment data is processed as necessary for the performance of contracts (Art. 6(1)(b)) and to comply with legal obligations. The full EU/EEA analysis for marketplace data is set out in the Potoo Data Storage Policy.

5. Sharing & Subprocessors

Personal information is shared only with the service providers that support Company operations: AWS (infrastructure hosting), Google Workspace (identity, email, documents), Tableau Cloud (analytics delivery), Retool (internal tooling), SugarCRM (CRM), LastPass (credential management), Mailgun (transactional email), and Paylocity (HR and payroll). The Company verifies, prior to retention and at least annually thereafter, that each provider maintains appropriate security measures, per the Potoo Security Policy and Vendor Management Policy.

6. Data Retention & Destruction

Data is retained in accordance with defined retention periods per data category, documented and reviewed annually by the Data Security Coordinator. Destruction is performed in a controlled manner: cloud resources are destroyed via deletion of encrypted volumes and snapshots (cryptographic erasure), endpoint devices are wiped prior to disposal or reassignment, and confidential physical documents, where they exist, are shredded.

7. Security Measures

Personal information is protected by the technical and organizational measures defined in the Potoo Security Policy, including:

- Multi-factor authentication enforced on all Company accounts across all major systems and subprocessors.
- Encryption at rest (AWS KMS-managed keys) and in transit (TLS) for Company databases.
- Least-privilege access provisioning with annual access recertification.
- Endpoint protection and device-level vulnerability monitoring.
- AWS CloudTrail audit logging supporting incident response under the Potoo Incident Response Policy.

8. Data Subject Rights

Individuals may request access to, correction of, or deletion of their personal information. Requests are directed to Potoo's Data Security Coordinator at datateam@potoosolutions.com, are verified before action, and are answered within the timelines required by applicable law. Potoo discloses its public-source collection practices in accordance with Art. 14 GDPR and maintains established procedures for responding to data subject requests.

9. Policy Review

This policy is reviewed annually against regulatory developments in US state privacy law and EU digital regulation. Material changes are recorded in the Document Version table and republished to relevant stakeholders.