MOODPRINTS LLC
Privacy Policy

Version 1.0
Last Updated: July 22, 2025

1. INTRODUCTION

1.1 Purpose. This Privacy Policy ("**Policy**") describes the manner in which MoodPrints LLC, an Oregon benefit company ("**MoodPrints**," "**we**," "**our**," or "**us**"), collects, uses, discloses, and safeguards personal data that is not protected health information ("**PHI**") under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). This Policy is a unilateral privacy notice provided for transparency; it is not a contract and does not create rights or obligations beyond those that already exist under applicable privacy law.

1.2 Relationship to Other Documents. All creation, use, and disclosure of PHI are governed exclusively by: (i) the HIPAA Notice of Privacy Practices ("**NOPP**"); (ii) the Client Terms & Telehealth Consent ("**CTTC**") for Clients; and (iii) the Platform Services Agreement together with any Business Associate Agreement ("**PSA/BAA**") for Clinicians. To the extent any provision of this Policy conflicts with the NOPP, CTTC, or PSA/BAA, the relevant HIPAA-governing document shall control for PHI, and this Policy shall control only for non-PHI personal data.

1.3 Key Terms (non-PHI only).

- **"Personal Data"** – Information that identifies or can reasonably be linked to an individual but is not PHI (e.g., name, email, IP address).
- **"Processing"** – Any operation performed on Personal Data (collecting, storing, analysing, etc.).
- **"Services"** – Moodprints.app, associated sub-domains, marketing emails/SMS, and the MoodPrints apps in their non-clinical capacities.

2. SCOPE AND APPLICABILITY

2.1 Platforms Covered. This Policy applies to Personal Data collected through:

- (a) The public website (**www.moodprints.app**) and any sub-domains;
- (b) The MoodPrints iOS and Android applications (only for non-clinical telemetry);
- (c) Email, SMS, surveys, and customer-support channels.

2.2 Users Covered. Visitors, registered Clients, Clinicians, newsletter subscribers, job applicants, and any other individuals who interact with the public portions of our Services.

2.3 Out-of-Scope Data. This Policy does not apply to: (a) PHI exchanged in secure Client–Clinician workflows (see NOPP), (b) information collected on third-party sites you reach via outbound links, and (c) offline interactions (e.g., conference meetings, postal mail).

3. CATEGORIES OF PERSONAL DATA WE COLLECT

3.1 Information You Provide Directly.

- (i) Account and profile details (name, email, phone, state/ZIP, avatar);
- (ii) Marketing preferences, survey responses, customer-support messages.

3.2 Information Collected Automatically. When you access the Services, our servers and first-party analytics scripts may automatically record:

- (i) Device identifiers, IP address, browser/OS type, crash logs;
- (ii) Usage analytics (page views, button clicks, session duration).

3.3 Information from Third Parties. We may receive limited purchase, subscription, or security-related metadata from:

- (i) App-store purchase receipts and subscription status;
- (ii) Identity-verification or anti-fraud signals, if applicable.

We do not intentionally collect sensitive data categories such as government-issued identification numbers, precise geolocation, or biometric information outside of the scope of our responsibilities as a Business Associate under HIPAA.

4. PURPOSES AND LEGAL BASES FOR PROCESSING

4.1 Service Operation and Security. We process Personal Data as necessary to register accounts, authenticate logins, maintain audit logs, prevent fraud or abuse, and otherwise perform the contract between you and MoodPrints for the provision of the Services.

4.2 Product Improvement. Usage analytics and crash diagnostics enable MoodPrints to diagnose defects, evaluate feature performance, and develop new or improved functionality. Such processing is carried out in furtherance of our legitimate interest in continually enhancing user experience.

4.3 Communications. MoodPrints uses contact information to send transactional messages, including password resets, account alerts, and policy updates, pursuant to contract performance. Marketing communications are sent only with your prior consent, which you may withdraw at any time.

4.4 Legal and Regulatory Compliance. We retain and, where required, disclose certain Personal Data to comply with applicable accounting rules, tax obligations, lawful requests, court orders, and other legal mandates.

4.5 Benefit-Company Reporting. Consistent with our status under ORS 60.750 et seq., MoodPrints may use de-identified and aggregated metrics regarding platform usage for the limited purpose of preparing an annual public-benefit report; no individual identities are revealed in such reporting.

5. DATA SHARING AND DISCLOSURE

5.1 Service Providers ("Processors"). MoodPrints engages a limited number of third-party service providers ("Service Providers") to perform narrowly defined tasks on our behalf. Each Service Provider is bound by a written agreement that: (i) requires the implementation of appropriate technical and organizational safeguards; (ii) permits the processing of Personal Data – and, where applicable, PHI – solely in accordance with MoodPrints' documented instructions; and (iii) prohibits the use of such data for the Service Provider's own marketing or other unauthorised purposes. As of the date the last Party electronically executes this Policy (the "**Effective Date**"), our principal Service Providers are:

- (a) **Amazon Web Services, Inc.:** Cloud-hosting infrastructure, database storage, virtual networking, encryption-key management, and backup services;
- (b) **Google Cloud Platform (Google LLC)**: Supplemental cloud infrastructure and, where enabled, Firebase telemetry for crash diagnostics;
- (c) **MongoDB Atlas (MongoDB, Inc.)**: Encrypted, managed database clusters;
- (d) **Mailgun Technologies, Inc.**: Transactional email delivery, including account verification, password-reset messages, notifications, and policy updates;
- (e) **Sakari, LLC**: U.S. A2P 10DLC SMS routing for marketing communications, multi-factor authentication, and account alerts;
- (f) **IPQualityScore LLC**: Device- and IP-based fraud-screening APIs that mitigate bot activity and fraudulent registrations; and
- (g) **Typeform S.L.**: Optional onboarding questionnaires and in-app surveys.

MoodPrints reviews the security posture of each Service Provider at least annually and amends this list when material changes occur. Should we retain a new Service Provider that will process Personal Data in a materially different manner, MoodPrints will update this Policy and, where required by applicable law, provide advance notice or obtain additional consent.

5.2 Affiliates and Corporate Transactions. We may disclose Personal Data to our corporate affiliates (if any) for activities consistent with this Policy. In the event MoodPrints undergoes a merger, acquisition, reorganization, sale of assets, or bankruptcy, Personal Data may be transferred as part of the transaction, subject to any successor entity's obligation to honor the promises in effect at the time the data was collected or to notify you of material changes.

5.3 Legal, Safety, and Enforcement. MoodPrints may disclose Personal Data when we believe in good faith that such disclosure is reasonably necessary to (a) comply with applicable law, regulation, subpoena,

or court order; (b) enforce our Terms of Service or other agreements; (c) protect the rights, property, or safety of MoodPrints, our users, or the public; or (d) detect, prevent, or otherwise address fraud, security, or technical issues.

5.4 Disclosures at Your Direction. We will disclose Personal Data to third parties at your express request or with your explicit consent – for example, if you instruct us to forward a support transcript to another service provider.

5.5 Aggregated and De-Identified Information. We may use and share information that has been aggregated or de-identified such that it can no longer reasonably be linked to an identified or identifiable individual. Aggregated analytics may be used for product improvement, research, or public-benefit reporting consistent with our benefit-company status.

5.6 No Sale of Personal Data. MoodPrints does not sell or rent Personal Data for monetary consideration, and we do not permit third parties to collect Personal Data across unaffiliated sites for targeted advertising purposes. You may disable non-essential cookies via browser settings and may opt out of marketing emails or texts by following the instructions in those messages. Core platform cookies necessary for security and log-in cannot be disabled.

6. COOKIES, SDKs, AND SIMILAR TECHNOLOGIES

6.1 Overview. We use a limited set of cookies, software development kits ("SDKs"), and similar tracking technologies to operate and secure the Services, remember user preferences, and gather non-identifying usage analytics. MoodPrints does not deploy third-party advertising networks or cross-site behavioral tracking cookies.

6.2 Types of Technologies.

- **(a) Strictly Necessary (Essential).** Session cookies and security tokens used to authenticate logins, maintain your session state, and prevent fraudulent activity. These are required for core functionality and cannot be disabled within the Service.
- **(b) Performance and Diagnostics.** First-party analytics or SDK telemetry (for example, crash reporting, load-time metrics, and feature interaction counts) that help us improve stability and usability. Data collected is linked to device or session identifiers rather than clinical content.

6.3 Preference Management. Most web browsers allow you to refuse or delete non-essential cookies through settings controls. Because our essential cookies are required to maintain authentication and platform security, disabling them may impair or prevent use of the Services. Mobile app users can manage telemetry permissions through in-app settings or the device's operating-system privacy controls where available.

6.4 "Do Not Track" Signals. Industry standards for responding to web browser *"Do Not Track"* (DNT) signals are not yet uniform. At this time, MoodPrints does not respond to DNT signals. We will reassess if

consensus standards emerge.

7. PHONE NUMBERS, SMS MESSAGING, AND 10DLC COMPLIANCE

7.1 Collection and Use of Telephone Numbers. If you supply a mobile telephone number, MoodPrints may use that number to send transaction-related or service-related messages, including multi-factor authentication codes, account alerts, subscription confirmations, and – if you have separately opted in – non-essential reminders or product notices.

7.2 Consent and Opt-In. Enrollment in any recurring SMS program requires an affirmative opt-in through an in-app control, web form, or other recorded method. By opting in, you authorize MoodPrints to deliver messages using an automated system; message frequency varies by account activity. Consent to receive SMS messages is not a condition of using the core Services unless SMS is required for security verification.

7.3 Opt-Out Instructions. You may revoke SMS consent at any time by replying *"STOP"* to any MoodPrints message. You may request assistance by replying *"HELP"* or by contacting **support@moodprints.app**. Opt-out requests are honored promptly; thereafter, you will receive only messages necessary to complete ongoing security transactions.

7.4 10DLC and Carrier Compliance. MoodPrints registers required campaign information with U.S. carrier 10-digit long code (10DLC) programs and agrees to carrier rules prohibiting the sale, rental, or unauthorized disclosure of mobile numbers, SMS opt-in status, or message content for marketing by third parties. Mobile information will not be shared with or sold to unaffiliated entities for promotional purposes.

7.5 Fees and Availability. Message and data rates may apply depending on your mobile plan. SMS delivery is provided on an "as available" basis and may be delayed or blocked by carrier conditions outside MoodPrints' control. MoodPrints is not liable for delayed or undelivered messages.

8. DATA RETENTION AND DISPOSAL

8.1 Standard Retention Schedules. MoodPrints keeps Personal Data only for as long as is reasonably necessary for the purposes set out in this Policy, unless law requires or permits a longer period. In most cases:

I. Authentication and server logs are stored for seven (7) years.

II. Marketing-consent records are retained while you remain opted-in and for five (5) years to demonstrate compliance with regulatory requirements.

III. Customer-support correspondence is preserved for at least five (5) years after a ticket is resolved

to facilitate quality-assurance and dispute resolution.

8.2 Extended Retention. Certain records may be held for longer than the periods above when necessary to enforce our agreements, defend legal claims, comply with audit or tax obligations, respond to law-enforcement requests, or honour a valid litigation hold. Backup archives that contain Personal Data in encrypted form may persist until they reach the end of their technical lifecycle and are then permanently destroyed.

8.3 Deletion and Anonymisation. When retention periods expire, or when a verified deletion request is granted, MoodPrints securely deletes Personal Data or irreversibly anonymises it using commercially reasonable and industry-standard techniques, ensuring that the data can no longer be associated with any identified or identifiable individual.

9. DATA SECURITY

9.1 Safeguards Implemented. MoodPrints will maintain administrative, technical, and physical safeguards consistent with NIST SP 800-53 (moderate baseline), including: (i) transport encryption via TLS 1.3 (or successor), (ii) AES-256 encryption of all stored Client and Clinician data, (iii) logically-isolated databases in AWS, MongoDB, and Google Cloud, (iv) multi-factor authentication for privileged workforce accounts, (v) quarterly penetration testing, (vi) immutable, tamper-evident audit logging retained for at least seven (7) years, and (vii) disaster-recovery measures achieving a Recovery-Point Objective of twenty-four (24) hours and a Recovery-Time Objective of forty-eight (48) hours.

9.2 Personnel and Vendor Controls. Employees and contractors with access to Personal Data are required to execute confidentiality agreements and complete annual security training. Third-party service providers are vetted for security posture and contractually bound to implement appropriate safeguards and breach-notification procedures.

9.3 Incident Response. MoodPrints maintains a written incident-response plan that defines escalation paths, containment and eradication steps, and user-notification obligations. In the event of a confirmed compromise of Personal Data (non-PHI) likely to result in risk to individuals, MoodPrints will notify affected users and, where applicable, regulators without undue delay and, in any event, within the time frames required under governing law; breach procedures for PHI are addressed in the NOPP and related HIPAA documents.

10. YOUR PRIVACY CHOICES AND REGIONAL RIGHTS

10.1 Global Rights. Subject to applicable law, you may (a) request access to the Personal Data we hold about you; (b) request correction of inaccurate or incomplete data; (c) request deletion of data no longer necessary for the purposes collected; (d) object to or restrict our Processing; and (e) withdraw consent for marketing communications at any time.

10.2 Exercising Rights. To exercise any right, submit a request by email to **privacy@moodprints.app** with your full name, registered email, and the specific right you wish to exercise. MoodPrints will verify your identity and respond within the timelines prescribed by applicable law.

10.3 California Residents (CCPA/CPRA). In addition to the global rights above, California residents may request disclosure of categories and specific pieces of Personal Data collected, opt out of any "sale" or "sharing" (as defined by CPRA), and limit use of "sensitive personal information." MoodPrints does not engage in activities constituting sale or sharing under CPRA.

10.4 Virginia Residents (VCDPA). Virginia consumers may opt out of Processing for targeted advertising, sale, or profiling; request portability of their Personal Data; and appeal denials of rights requests by emailing **privacy@moodprints.app** with the subject line "VCDPA Appeal."

10.6 Verification and Denial. If MoodPrints is unable to verify your identity or determine that statutory exceptions apply, we may deny the request in whole or in part, in which case we will provide the reason for denial and information on how to appeal or escalate.

10.7 No Discrimination. MoodPrints will not discriminate against you for exercising any privacy right, such as by denying services, charging different prices, or providing a different level of quality, except to the extent permitted by law – for example, if requested deletion renders the Services inoperable.

11. CHILDREN'S PRIVACY

11.1 Under-13 Prohibition. MoodPrints does not knowingly collect Personal Data from children under thirteen (13) years of age. If we discover that we have inadvertently obtained Personal Data from a child under 13, we will promptly delete it.

11.2 Users Aged 13–17. Individuals between thirteen (13) and seventeen (17) years of age may register for a MoodPrints account only after a parent or legal guardian executes all necessary Agreements on the minor's behalf. Any Personal Data collected from such minors is limited to that necessary for account creation, authentication, and non-clinical telemetry, and is processed strictly in accordance with this Policy.

11.3 Parental Requests. A parent or legal guardian who believes that MoodPrints has collected Personal Data from a child in violation of this Section may contact **privacy@moodprints.app**; upon proper verification we will honour requests to review, delete, or prohibit further collection of the child's Personal Data.

12. THIRD-PARTY SITES AND SOCIAL FEATURES

12.1 External Links. The Services may contain links to external websites, applications, or resources that are not operated by MoodPrints. We provide these links solely for convenience; their inclusion does not

signify endorsement. MoodPrints has no control over, and assumes no responsibility for, the content, privacy policies, or practices of any third-party site or service.

12.2 Social Media Widgets. The Services may include social-media plug-ins or sharing widgets. Your interactions with these features are governed by the privacy policies of the companies providing them, not by MoodPrints.

12.3 User Responsibility. You should review the privacy statements of every third-party site you visit. Access to any third-party site is at your own risk, and MoodPrints disclaims all liability arising from use of third-party resources.

13. CHANGES TO THIS PRIVACY POLICY

13.1 Right to Amend. MoodPrints may revise this Privacy Policy with at least thirty (30) days' notice for material changes; the latest version will always be available in-app and at **www.moodprints.app/privacy-policy**.

13.2 Continued Use Constitutes Acceptance. Your continued access to or use of the Services after the thirty-day notice of a revised Policy signifies your acceptance of the changed terms. If you do not agree to the amended Policy, you must discontinue use of the Services before the new terms become operative.

13.3 Archival Copies. Prior versions of this Privacy Policy will be preserved in an online archive accessible from the legal page for reference at **www.moodprints.app/archives**.

14. CONTACT INFORMATION

14.1 General and Privacy Inquiries. Questions about this Privacy Policy or our data-handling practices should be directed to **privacy@moodprints.app**.

14.2 Mailing Address.

MoodPrints LLC
8775 NE Wilkins St, Apt 312
Hillsboro, OR 97006
United States

14.3 Data Protection Officer. MoodPrints' Data Protection Officer ("DPO") may be contacted at the email and postal addresses above. The DPO is responsible for monitoring MoodPrints' compliance with applicable privacy laws and for acting as the primary point of contact for supervisory authorities.

15. YOUR CONSENT. By accessing or using the public portions of the MoodPrints Services after the

Effective Date defined above, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy with respect to all Personal Data processed outside the scope of HIPAA. If you do not agree, you must refrain from using the Services.