

Meet Over Coffee
Privacy Policy (Website & Mobile Application)

Last Updated: January 29, 2026

This Privacy Policy explains how **Meet Over Coffee, LLC**, a Wyoming limited liability company with its principal place of business at 30 N Gould Street Ste R Sheridan, Wyoming 8280, United States of America (“**MOC**,” “**we**,” “**us**,” “**our**”), collects, uses, discloses, and protects information when you use our website located at <https://meetovercoffee.com/> and <https://meetover.coffee>, our mobile application(s) (the "App"), and related services (collectively, the "Services"). For purposes of GDPR and UK GDPR, Meet Over Coffee, LLC is the data controller of your personal information.

1. Scope. This Privacy Policy applies to information we collect: through the Services; through communications with you (e.g., email, support); from third parties as described below. It does not apply to third-party websites, apps, or services that may link to or integrate with the Services.

2. Information We Collect.

2.1 Information You Provide:

a. **Account information:** name, email, phone number, username, password (stored in hashed form), profile details.

b. **Transaction information:** shipping address, billing address, order details, subscription preferences.

c. **Communications:** messages to support, survey responses, reviews, photos, and other content you submit.

d. **Brand/Business information (if applicable):** company name, contact details, business identifiers (if applicable), product listings, marketing assets, and fulfillment details.

2.2 Information Collected Automatically:

a. **Device and usage data:** IP address, device identifiers, browser type, app version, operating system, pages/screens viewed, clicks, session duration, crash logs.

b. **Approximate location:** derived from IP address; **precise location** only if you enable it and we request permission.

c. **Cookies and similar technologies:** see Section 8.

2.3 Information from Third Parties:

- a. **Payment processors:** payment status and limited payment-related data (we generally do not store full card numbers).
- b. **Vendors/partners:** order fulfillment updates, shipping status, product availability.
- c. **Analytics and advertising partners (if used):** aggregated or pseudonymous usage and campaign performance data (subject to your settings and applicable law).
- d. **Social logins (if enabled):** information you allow the provider to share.

We do not knowingly collect or process biometric identifiers or biometric information (such as fingerprints, facial recognition data, voiceprints, or retina scans), nor do we create or use sensitive inferences about individuals (such as health conditions, precise geolocation, religious beliefs, or political affiliations), unless explicitly disclosed to you with prior notice and, where required by law, your consent.

3. How We Use Information. We use information to:

- 3.1 provide, operate, and maintain the Services;
- 3.2 create and manage accounts;
- 3.3 process Transactions, subscriptions, and fulfill orders;
- 3.4 provide customer support and communicate with you;
- 3.5 personalize content, recommendations, and experiences (including AI-enabled features) using the categories of information described in Section 2, such as profile details, preferences, and communications/content (if applicable); we do not use personal information to train or improve third-party AI models or share personal information with third-party AI providers without providing prior notice and obtaining consent or establishing another lawful basis under applicable law;

Where the Services provide analytics, insights, or reporting to brands, franchise operators, or enterprise customers, such outputs are generated using aggregated, de-identified, or anonymized data unless you have expressly consented to the sharing of identifiable personal information. Enterprise customers do not receive access to individual user profiles or personal information unless required to complete a transaction you initiate or authorized by you.

- 3.6 improve the Services, including debugging, analytics, and product development; detect, prevent, and address fraud, abuse, and security issues;

- 3.7 comply with legal obligations and enforce our terms.

We do not engage in automated decision-making, including profiling, that produces legal effects or similarly significant effects concerning you within the meaning of Article 22 of the GDPR. Any AI-enabled personalization, recommendations, or insights are intended to support user experience and decision-making and are not determinative or binding.

4. How We Disclose Information. We may disclose information to:

4.1 **Service providers** (hosting, analytics, customer support tools, email/SMS providers, fraud prevention, payment processing) that process data on our behalf;

4.2 **Vendors and logistics partners** to fulfill orders and provide shipping/delivery updates;

4.3 **Brands/Businesses** when you interact with them (e.g., purchases, inquiries, event registrations), as needed to complete the interaction;

4.4 **Affiliates and successors** in connection with corporate transactions (merger, acquisition, financing, or sale of assets);

4.5 **Legal and safety disclosures** when required by law or to protect rights, safety, and security.

We do not sell your personal information for monetary consideration. However, we may disclose personal information to third parties for cross-context behavioral advertising or targeted advertising purposes, which may be considered a "sale" or "sharing" under certain U.S. state privacy laws (including California, Colorado, Connecticut, Virginia, and Utah). You have the right to opt out of such sale/sharing. You can opt out by: (a) using our cookie banner/preferences tool (where available) to disable advertising/targeting cookies and similar technologies; (b) submitting an opt-out request using the methods described in Section 13.1; or (c) using an opt-out preference signal such as Global Privacy Control (GPC) if you are a resident of a jurisdiction that recognizes such signals. We will process opt-out preference signals in a frictionless manner as required by applicable law.

5. Legal Bases for Processing (EEA/UK Where Applicable). Where GDPR/UK GDPR applies, we process personal data based on:

5.1 **performance of a contract** (providing the Services and fulfilling orders);

5.2 **legitimate interests** (improving Services, preventing fraud, securing systems);

5.3 **consent** (marketing preferences, certain cookies, precise location where enabled);

5.4 **legal obligations**.

6. Data Retention. We retain information as long as reasonably necessary for the purposes described in this Privacy Policy, including to provide the Services, comply with legal obligations, resolve disputes, and enforce agreements. Retention periods vary by data type and context, and generally follow these timeframes: (a) Account/profile data: for the life of your account, and up to 30 days after account closure or deletion request (unless we must retain it longer for legal, security, or fraud-prevention reasons). (b) Transaction records (including shipping/billing address and order details): 7 years after the transaction to comply with tax, accounting, and audit requirements. (c) Communications and user content (support messages, surveys, reviews, photos, and other content you submit): up to 2 years after your last interaction with us, or until you delete the content (if available), unless needed to resolve disputes or enforce agreements. (d) Device and usage data (including IP address, device identifiers, and crash logs): 12 to 24 months from collection for security, analytics, and service improvement. (e) Approximate location derived from IP address: up to 12 months; precise location (if enabled): retained only while the feature is enabled and up to 30 days thereafter. (f) Marketing preferences and opt-out records: until you change your preferences, and up to 5 years after your last interaction to honor your choices and comply with applicable law. We may retain certain information longer where required by law or for fraud prevention, security, or to establish, exercise, or defend legal claims.

7. Security. We use reasonable administrative, technical, and physical safeguards designed to protect information. No system is 100% secure; you use the Services at your own risk.

8. Cookies and Similar Technologies. We use cookies, pixels, SDKs, and similar technologies (each described below) to:

8.1 keep you logged in and maintain preferences (e.g., cookies and similar storage technologies; SDKs in our App);

8.2 understand usage and performance (e.g., cookies, pixels, and SDKs);

8.3 measure marketing effectiveness (if applicable) (e.g., cookies, pixels, and SDKs).

Cookies are small text files placed on your browser or device; pixels (also called web beacons) are small code snippets that help us understand whether you interacted with content; and SDKs are code libraries in our App that help us understand App usage and measure campaign performance.

You can control cookies through browser settings and, where available, our cookie banner/preferences tool. In our App, you may be able to manage certain tracking through in-app settings (if available). Mobile settings may allow you to limit ad tracking (e.g., your device's advertising controls).

9. Your Choices and Rights. Depending on your location, you may have rights to: access, correct, or delete personal information; obtain a copy of certain information (portability); opt out of certain processing (e.g., targeted advertising where applicable); withdraw consent (where processing is based on consent).

You may delete your account at any time through the account settings within the App or Website, where available. If self-service deletion is not available, you may request deletion by contacting us using the methods described in Section 14. Account deletion will permanently remove your profile and associated personal information from our active systems, subject to the retention obligations described in Section 6. Certain information may be retained in anonymized or aggregated form or as required by law, for security, fraud prevention, or dispute resolution purposes. Deleted accounts cannot be restored.

To submit a request, contact us at **[Insert Monitored Privacy Intake Email]**. We may verify your identity before fulfilling requests.

10. Marketing Communications. You can opt out of marketing emails by using the unsubscribe link. You may still receive transactional or service-related messages.

If we offer SMS/text messaging, messages will include opt-out instructions (e.g., replying STOP).

11. Children's Privacy. The Services are not directed to children under 13 (or under 16 in the EEA/UK, or the applicable age of digital consent in your jurisdiction), and we do not knowingly collect personal information from children under these ages without verifiable parental consent as required by applicable law (including COPPA in the United States and GDPR in the EEA/UK). If you believe a child under the applicable age has provided personal information to us, please contact us immediately using the methods in Section 14, and we will take steps to delete such information as required by law.

12. International Transfers. Your information may be processed in the United States and other countries where we or our service providers operate. These locations may have different data protection laws than your jurisdiction. For transfers from the EEA, UK, or Switzerland to countries not deemed adequate by the European Commission or UK/Swiss authorities, we implement appropriate safeguards such as: (a) Standard Contractual Clauses approved by the European Commission (or UK/Swiss equivalents); (b) Binding Corporate Rules (where applicable); or (c) other legally recognized transfer mechanisms. You may request a copy of the safeguards we use by contacting us using the methods in Section 14. For transfers subject to other jurisdictions' requirements, we comply with applicable cross-border transfer laws and regulations.

13. Region-Specific Disclosures.

13.1 U.S. State Privacy Rights (e.g., CA/CO/CT/VA/UT/OR/TX/MT). If you are a resident of certain U.S. states with comprehensive privacy laws, you may have the following rights: (a) Right to Know/Access: Request disclosure of the categories and specific pieces of personal information we have collected about you; (b) Right to Delete: Request deletion of your personal information, subject to certain exceptions; (c) Right to Correct: Request correction of inaccurate personal information; (d) Right to Opt Out: Opt out of the sale or sharing of personal information, targeted advertising, and certain profiling; (e) Right to Limit Use of Sensitive Personal Information (where applicable); (f) Right to Data Portability (where applicable):

Receive your personal information in a portable format; (g) Right to Non-Discrimination: We will not discriminate against you for exercising your rights. To exercise these rights, contact us using the methods in Section 14. We will respond to verifiable requests within the timeframes required by applicable law (typically 45 days, with possible extension). You may designate an authorized agent to submit requests on your behalf by providing written authorization. We may need to verify your identity before processing requests.

13.2 EEA/UK/Switzerland. If you are located in the European Economic Area, United Kingdom, or Switzerland, you have the following rights under GDPR/UK GDPR/Swiss FADP: (a) Right of Access: Obtain confirmation of whether we process your personal data and access to such data; (b) Right to Rectification: Correct inaccurate personal data; (c) Right to Erasure: Request deletion of your personal data under certain circumstances; (d) Right to Restriction of Processing: Request restriction of processing under certain circumstances; (e) Right to Data Portability: Receive your personal data in a structured, commonly used, machine-readable format; (f) Right to Object: Object to processing based on legitimate interests or for direct marketing purposes; (g) Right to Withdraw Consent: Withdraw consent at any time where processing is based on consent; (h) Right to Lodge a Complaint: Lodge a complaint with your local supervisory authority (data protection authority). To exercise these rights, contact us using the methods in Section 14. We will respond within one month, which may be extended by two additional months where necessary. For UK residents, the UK Information Commissioner's Office can be contacted at <https://ico.org.uk>. For EEA residents, a list of supervisory authorities is available at https://edpb.europa.eu/about-edpb/board/members_en.

13.3 Saudi Arabia / South Africa (Expansion). As we launch localized offerings, we may provide additional notices, consent flows, and data handling practices as required by local law.

When you download or use our App, Apple Inc. and Google LLC may collect information as required to provide their app store and operating system services. Our data collection and use practices are described in this Privacy Policy; however, additional disclosures regarding data linked to you, data used for tracking, and data not linked to you may be presented within the app store listing or in-app disclosures as required by applicable platform policies.

14. Contact.

Meet Over Coffee, LLC

30 N Gould Street Ste R Sheridan, Wyoming 8280, United States of America

Email: feedback@meetover.coffee

Website: <https://www.meetovercoffee.com> and <https://meetover.coffee>