FREEKEEK - PRIVACY POLICY

Version 1.2
Version date: 2026-10-03
Effective date: 2026-10-03.

This Privacy Policy explains how **FREEKEEK 4E PLACES LAB LTDA.**, trade name **FREEKEEK 4E**, registered under CNPJ No. **69.122.866/0001-71**, with registered office at Rua Corticeira, 643, Hípica, Porto Alegre/RS, ZIP Code 91755-654, Brazil, processes personal data in connection with the **Freekeek** platform.

Privacy and data-subject rights: privacy@freekeek.app
Legal matters and public-authority requests: legal@freekeek.app

1. Who is the controller

FREEKEEK 4E PLACES LAB LTDA. is generally the controller of personal data processed for operation of the Freekeek platform because it determines the main purposes and means of that processing.

Providers that process data on Freekeek's behalf may act as processors. In certain integrations, a third party may process data for its own purposes and under its own responsibilities, according to its terms and applicable law.

The address **privacy@freekeek.app** is the channel for data-subject requests and privacy matters. The existence of this channel does not, by itself, constitute public appointment of a specific natural person as a data protection officer or equivalent contact unless Freekeek formally makes such a designation in a separate document.

2. Scope of this Policy

This Policy applies to personal-data processing carried out through freekeek.app, applications, Accounts, Places, Marketplace, authentication, communications, moderation, support systems and other features connected with the platform.

It does not apply to processing independently carried out by third-party websites, services or applications reached through links or integrations, although this Policy explains the main circumstances in which those providers may receive data from Freekeek.

3. Data-protection principles and commitment

Freekeek seeks to process personal data in accordance with Brazil's General Data Protection Law — **LGPD**, the Brazilian Civil Rights Framework for the Internet, Brazilian laws protecting children and adolescents and other applicable mandatory rules.

Depending on the operation, processing will be guided by principles including purpose limitation, adequacy, necessity, free access, data quality, transparency, security,

prevention, non-discrimination and accountability.

For children and adolescents, best interests, comprehensive protection and privacy by default are additional design and operating parameters.

4. How we obtain data

Freekeek may obtain data:

- directly from the user when they create an Account, complete a profile, post content, send a message, create a listing, provide location information, request Place management or contact us;
- from a Legal Guardian where linkage, authorization, supervision or verification of an Adolescent Account is involved;
- from other users when they mention, tag, invite, report or interact with the data subject;
- automatically from the device and use of the platform, including access records, IP address, session, security, browser, operating system and technical events;
- from organizations represented by the user or legitimate public sources; and
- from external mapping, location, authentication, communications, security or other integrated service providers, within applicable contractual and legal limits.

5. Categories of data processed

5.1 Registration and authentication data

May include name, username, date of birth or age range, email address, protected credentials, language, country or region and information necessary to create, recover and secure an Account.

5.2 Profile and preference data

May include profile photo, biography, description, pronouns where provided, interests, followed Places, language preferences, privacy settings and communications choices.

5.3 Content and interactions

Includes posts, images, videos, comments, reviews, reactions, tags, connections, reports and other User Content.

5.4 Communications

May include messages and metadata necessary for delivery, protection, abuse prevention and investigation of reports, subject to applicable rights and legal limits governing the content of communications.

5.5 Organization data

For Organization Accounts, we may process legal or institutional name, display name, category, website, contact information, representative information and data used to verify authority or affiliation.

5.6 Adolescent Account and Legal Guardian data

May include age range, information concerning linkage to a guardian, identifiers necessary for supervision, protection settings, authorization records and data strictly necessary for age-assurance procedures.

5.7 Pet Profile data

Information about an animal, viewed in isolation, is not necessarily personal data. However, a Pet Profile’s name, photographs, location, routines, posts and relationships may identify or support inferences concerning its responsible person or other individuals and, to that extent, will be treated as personal data associated with the responsible Account.

5.8 Marketplace data

May include listing category, description, price, images, locality, contact information made available, listing history and interactions necessary to operate and secure the Marketplace.

5.9 Technical and security data

May include IP address, date and time, device, browser, operating system, session identifiers, authentication events, logs, fraud signals, failures and technical information necessary for security and diagnostics.

5.10 Legal records, versioning and acceptance

Freekeek may record the version of the Terms of Use and Privacy Policy presented or accepted, date and time, language, Account, whether the actor was the user or a Legal Guardian, and technical references necessary to evidence availability, contractual acceptance, acknowledgment of the privacy notice and integrity of the applicable version.

These records do not turn the Privacy Policy into blanket consent. Specific consents, where legally required, will be recorded separately for the relevant purpose.

6. Sensitive personal data

Freekeek does not generally require sensitive personal data to create a standard Account.

Users may nevertheless voluntarily disclose sensitive information in posts, profiles or communications. Depending on applicable law, this may include information concerning health, racial or ethnic origin, religion, political opinions, trade-union membership, sex life, genetics or biometrics.

Voluntary disclosure by a user does not authorize Freekeek to use such data for purposes incompatible with the context of the disclosure or without an appropriate legal basis.

We recommend particular care before making sensitive information publicly accessible.

7. Location data and association with Places

Freekeek is structured around Places and certain features may therefore process geographic information.

Location may derive from a Place selected by the user, a city or region provided by the user, an address associated with a listing, an approximate location technically inferred, or device location where authorization exists and the feature requires it.

Following, posting to or interacting with a Place may reveal interests, movements, relationships or location inferences. Such information will be processed according to the selected audience, Account settings and applicable protections.

For Adolescent Accounts, geolocation sharing will receive heightened protection and may remain restricted by default, including parental-supervision controls where required.

8. Google Maps Platform and Places API

Freekeek may integrate **Google Maps Platform**, including the **Places API**, for specific functions involving search, identification, location, matching or display of places and points of interest.

When a user uses a feature that depends on this service, data necessary for the request may be transmitted to Google, such as search terms, technical identifiers, IP address and, where the feature requires it and an appropriate permission exists, approximate or precise location data. Google may process this information under its own terms, its **Privacy Policy** and the terms applicable to Google Maps Platform.

Use of Google Maps features and content through Freekeek is also subject to the applicable **Google Maps/Google Earth Additional Terms of Service**. Freekeek will preserve required attribution and notices when displaying Google-provided content.

Freekeek distinguishes Google Maps Platform content from Freekeek data and User Content. Identifiers expressly permitted to be stored, such as a **Google Place ID**, may be retained as a technical reference. Other elements may only be stored, cached, exported, combined or reused to the extent permitted by the then-current terms and documentation.

Freekeek must not use Google Maps content to create or augment a persistent listings or Place directory database where such use is prohibited by the applicable agreement. Persistent Freekeek Place data must have an independent legitimate source, such as information supplied by a user or representative, a lawfully usable public source, a licensed source or data legitimately produced by Freekeek.

Management of a Freekeek Place does not create, modify or transfer rights in any profile, listing, content or property existing in Google services. Google and its services may act as independent controllers for processing carried out under their own terms.

9. Purposes of processing

Freekeek may process personal data to:

- create, authenticate, maintain and recover Accounts;
- provide profiles, Places, feeds, search, connections and other social features;
- display User Content according to audience, preferences and selected context;
- operate Organization Accounts, verify administrators and manage permissions;
- operate Adolescent Accounts, assure age, link Legal Guardians and apply safeguards;
- create, identify, organize, correct and administer Places using Freekeek data or legitimately usable sources;
- process Place-management requests and verify relationships with organizations or establishments;
- operate Marketplace, listings and related interactions;
- enable communications between users;
- maintain security, authentication and prevention of fraud, spam and abuse;
- moderate content, receive reports, conduct reviews and enforce rules;
- protect the rights of users, third parties and Freekeek;
- comply with legal, regulatory, judicial or administrative obligations;
- respond to support, privacy and legal requests;
- record, version and evidence acceptance of Terms, acknowledgment of privacy notices and documentary changes;
- generate operational, diagnostic, availability and security metrics;
- develop, test and improve features in a manner compatible with this Policy; and
- establish, exercise or defend rights in judicial, administrative or arbitral proceedings.

10. Legal bases

The legal basis depends on the processing operation and may include:

- **performance of a contract and pre-contractual procedures**, to provide requested features and administer the user relationship;
- **compliance with a legal or regulatory obligation**, where law requires retention, disclosure, protection or another action;
- **legitimate interests**, where appropriate and after consideration of the data subject's rights, freedoms and reasonable expectations;
- **consent**, where required for a specific purpose such as certain device permissions or optional communications;
- **regular exercise of rights / establishment, exercise or defense of legal claims**, to prevent or defend claims;
- **protection of life or physical safety**, in circumstances compatible with the applicable statutory basis; and
- other legal bases provided by applicable law.

This Privacy Policy does not turn all processing into consent-based processing. Where consent is required, it will be requested specifically, prominently and separately where appropriate.

11. Children, adolescents and Adolescent Accounts

Freekeek sets a minimum age of 13 for a natural-person Account in this version of the Services.

Users aged 13 to 17 will use an **Adolescent Account**. In Brazil, Accounts belonging to children and adolescents **up to and including 16 years of age** must remain linked to the Account of a Legal Guardian. Users aged 17 remain protected as minors and may require a guardian's authorization or assistance for particular acts or features.

Freekeek will apply more protective default privacy and security settings for minors, taking account of age, progressive autonomy and the nature of the feature.

Data used for age assurance will be limited to what is necessary and may not be reused for incompatible purposes. Where an identification document is collected exclusively to confirm age and law requires immediate deletion of the image or copy after the necessary age information is extracted, Freekeek will perform that deletion.

Parental-supervision tools will be structured to enable legally required controls without using interface patterns intended to induce users to weaken safeguards.

Freekeek will not use data of children and adolescents to create behavioral profiles for commercial advertising where applicable law prohibits that practice.

12. Pet Profiles and data of the responsible person

A Pet Profile is a dependent profile linked to an adult Personal Account.

Freekeek will process information concerning the responsible person necessary to administer the Pet Profile and may associate posts, messages, Places and settings of the profile with the responsible Account.

Users should avoid publishing through a Pet Profile information that reveals residence, routines or location in a manner that could compromise their own safety or the safety of others.

13. Public content, search engines and third parties

Content configured as **Public**, public profiles, public Place pages, public organization information and public listings may be accessible without login and, where technically enabled, indexed by search engines or other external services.

Freekeek does not fully control copies made by third parties following legitimate public disclosure. Later deletion from the platform does not guarantee deletion of external copies.

Content configured as non-public will not intentionally be made available by Freekeek to public search engines in a manner inconsistent with the selected audience.

14. Cookies, sessions, measurement, and similar technologies

Freekeek uses cookies and similar technologies that are strictly necessary for authentication, sessions, security, fraud prevention, language, theme, and operation of the Services. These essential technologies do not depend on measurement consent.

The Google tag for visit and conversion measurement is optional. Consent Mode starts with optional storage denied; measurement is enabled only after an affirmative choice and may be declined or withdrawn at any time through the **Measurement** link in the footer. Declining does not prevent registration or reduce essential functionality. Ad personalization remains disabled by Freekeek.

Accounts identified as adolescent do not receive optional measurement technologies. Categories, providers, duration, processed data, and instructions for changing a choice are described in the Cookie Policy, which forms part of this notice by reference without replacing specific consent where required.

15. Recommendations, ranking and automated systems

Freekeek may use automated systems to organize feeds, rank results, suggest Places, detect spam, identify risks, assist moderation and recommend content.

Those systems may consider signals such as user relationships, followed Places, language, settings, recency and interactions, subject to restrictions applicable to minors and data-protection principles.

Where law grants a right to review a decision based solely on automated processing that affects the data subject’s interests, the user may exercise that right through the privacy channel.

16. Sharing with processors and providers

Freekeek may share strictly necessary data with service providers that assist with hosting, infrastructure, storage, security, authentication, communications delivery, maps, location, development, technical monitoring, fraud prevention and other platform-support activities.

Such providers must process data within applicable purposes and corresponding contractual or legal obligations according to their role in each operation.

Freekeek **does not sell personal data**.

If a future business model introduces a new material category of sharing, this Policy will be updated before or when required by law.

17. Public authorities, orders and protection of rights

Data may be preserved or disclosed to public authorities where there is a legal obligation, valid court order or another legally authorized basis.

Freekeek may also use or preserve data necessary to prevent fraud, protect security, investigate serious violations, defend rights or fulfill obligations relating to protection of children and adolescents.

Formal authority requests should be sent to **legal@freekeek.app**.

18. Location of primary infrastructure and international transfers

Freekeek is a Brazilian company and remains responsible, as controller, for processing operations governed by Brazilian law.

The **primary infrastructure used to host the application is located in Canada**. Personal data and technical data necessary to operate the platform may therefore be stored or processed using infrastructure located in that country.

For transparency, Freekeek identifies the relevant country but does not publicly disclose data-center addresses, IP addresses, network topology, internal architecture, credentials, server configurations or other details that are unnecessary for exercising data-subject rights and whose disclosure could increase security risks.

International transfers will be carried out for legitimate purposes compatible with this Policy and using mechanisms legally admitted under the LGPD and applicable regulations, according to the nature of each operation. Freekeek may use contractual clauses, recognized safeguards or other permitted mechanisms where necessary.

Global providers used for particular features may process data in other jurisdictions according to their services and policies. Where law requires additional specific information concerning destination country, purpose or transfer mechanism, it will be made available to the data subject through the appropriate channels.

19. Application of laws from different countries

The LGPD is Freekeek’s primary data-protection framework as a Brazilian controller and applies to operations within its territorial scope regardless of the country in which data is physically stored.

Technical processing in Canada may also be subject to mandatory Canadian rules applicable to the infrastructure or relevant provider, without removing Freekeek’s obligations toward users protected by Brazilian law.

Where territorial criteria of other data-protection regimes are met, including in relation to users in other jurisdictions, Freekeek will observe mandatory rights applicable to the relevant processing.

The mere technical availability of the platform in a country does not automatically make every law of that jurisdiction applicable.

20. Retention periods

Freekeek retains personal data for the period necessary to achieve the purposes described in this Policy and comply with applicable legal obligations, avoiding indefinite retention without a valid basis.

While an Account remains active, registration data, content and settings necessary to provide the Services may remain stored.

Application access logs will be retained for the legally applicable period, including the minimum **six-month** period where required by the Brazilian Civil Rights Framework for the Internet, without prejudice to longer preservation supported by a valid legal basis.

Records of acceptance of Terms, acknowledgment of Privacy Policy versions, publication of legal versions and other contractual evidence may be retained for the period necessary to evidence the legal relationship, comply with obligations and establish, exercise or defend legal claims, including after Account termination where supported by a valid basis.

Data related to reports, fraud, security, disputes, moderation and exercise of rights may be retained for the period necessary to investigate, comply with obligations or defend claims.

Third-party content will be retained or cached only within the limits permitted by the relevant provider's agreement and documentation. Technical identifiers whose retention is expressly permitted may be retained while necessary.

Backups may contain residual copies for a limited period until overwritten or deleted under the applicable technical cycle, without renewed use for incompatible purposes.

21. Account deletion and effects on data

When a user requests deletion of an Account, Freekeek will begin the process of deleting or anonymizing data that does not need to be retained.

Certain data may remain after termination where retention is required by law, record-preservation duties, security, fraud prevention, protection of third parties or the establishment, exercise or defense of legal claims.

Content shared with other users or incorporated into public contexts may require specific handling. Account deletion does not require Freekeek to erase third-party content merely referring to the user unless a legal basis for removal exists.

22. Data-subject rights

Under the LGPD and depending on the processing operation, the data subject may request:

- confirmation that processing exists;
- access to data;
- correction of incomplete, inaccurate or outdated data;
- anonymization, blocking or deletion of unnecessary, excessive or unlawfully processed data;
- portability, where regulated and applicable;
- deletion of data processed on the basis of consent, subject to statutory retention exceptions;
- information about sharing;
- information about the possibility and consequences of refusing consent;
- withdrawal of consent where consent is the legal basis relied on;
- objection in circumstances provided by law; and
- review of certain automated decisions, where applicable.

Requests should be sent to **privacy@freekeek.app**. Freekeek may request information reasonably necessary to confirm identity or representative authority and prevent fraud or improper disclosure.

The data subject may also petition the Brazilian National Data Protection Authority — ANPD — or another competent authority where applicable law permits.

23. Information security

Freekeek adopts technical and administrative measures proportionate to the nature and risks of processing to reduce unauthorized access, loss, alteration, destruction or improper disclosure of data.

Credentials and passwords must be protected through appropriate technical mechanisms and should not be stored in plain text.

No internet-connected service can guarantee absolute security. If a personal-data incident occurs that is subject to mandatory notification, Freekeek will take applicable legal measures, including notification to the competent authority and affected data subjects where required.

Specific details concerning internal architecture, servers, networks, keys, internal controls or defensive mechanisms may remain confidential where disclosure could compromise the security of the platform or its users.

24. Changes to this Policy and versioning

This Policy may be updated to reflect legal, regulatory, technological, provider, security or feature changes.

Each published version will have a version number, effective date and preserved content. A published version should not be silently modified; subsequent changes must produce a new version or another formally identifiable revision.

Material changes will be communicated as appropriate. Where a specific processing activity depends on consent, a change in purpose or conditions may require a new, specific consent request; this is distinct from merely updating this privacy notice.

Freekeek will maintain a history of prior versions for transparency, audit and evidence of the content applicable during each period.

25. Contact and languages

Privacy, personal data and data-subject rights: privacy@freekeek.app
Legal matters and public-authority requests: legal@freekeek.app

This Policy may be made available in Portuguese, English and Spanish. The **Brazilian Portuguese** version is the authoritative legal text. In the event of a translation inconsistency, the Portuguese version prevails, without prejudice to mandatory rights provided by applicable law.

Privacy addendum — Passkeys and cryptographic credentials

When a Passkey is registered or used, identity verification by biometrics, PIN, or device unlock takes place locally on the selected device or authenticator. **Freekeek does not receive or store a fingerprint, facial image, device PIN, or private key**, and does not use Passkeys for advertising, profiling, or biometric recognition.

To authenticate and protect the Account, Freekeek may process the credential identifier, cryptographic public key, signature counter, user-assigned name, authenticator transports and type, synchronisation or backup state, technical authenticator identifier (when supplied), creation and last-use dates, and related security events. Cryptographic challenges are temporary, bound to the operation, and intended for one-time use.

These data are processed for authentication, fraud prevention, Account protection, credential management, and incident investigation. The public credential remains linked while the Passkey is active or until it is removed, subject to security records retained as needed to comply with obligations, prevent fraud, or establish and exercise rights.

The operating system, manufacturer, password manager, or provider selected by the user — such as Apple, Google, or Microsoft — may store or synchronise the private key under its own terms. Freekeek does not control that synchronisation. Removing a Passkey from Freekeek does not necessarily remove a copy held on a device or credential manager, and the reverse is also true.

Passkey registration, use, failure, alteration, and removal may generate security logs and alerts. Those records do not contain the private key or biometric data used locally.

© 2026 FREEKEEK 4E PLACES LAB LTDA. - FREEKEEK 4E. All rights reserved.