

Virema Privacy Policy

Effective date: 16 September 2026 Last updated: 16 September 2026

Virema is operated by Valentyna Fomina, acting as a Belgian sole proprietor (registered natural person), enterprise number 1009.416.048, with a business establishment at Avenue Limbourg 55, 1070 Anderlecht, Belgium ("Virema", "we", "us" or "our"). Valentyna Fomina is the data controller for the processing described in this Policy unless a separate notice identifies another controller. This Privacy Policy explains how we collect, use, disclose, store and protect personal information when you use the Virema mobile application, website and related services (the "Service").

Contact: support@virema.app Voice support: **+1 570 359 4100** (English-language voicemail; carrier and international calling charges may apply)

1. Scope and important regional notice

This Policy applies to the international Virema Service. Local mandatory privacy and consumer laws continue to apply and may give you additional rights.

Mainland China status

The Service is not currently presented as a dedicated mainland China release. A Chinese translation is provided for Chinese-speaking users of the international Service. It does not represent that Virema has completed mainland China-specific app filing, licensing, cybersecurity, data-localisation, cross-border-transfer review or other regulatory approvals. Availability from, or use while located in, mainland China does not by itself mean that a mainland China-specific version has launched. Virema is evaluating a separate compliance framework and may introduce additional mainland China notices, consents, storage arrangements and terms before such a launch. Nothing in this notice excludes mandatory law that applies to a user or to Virema.

2. Information we collect

We collect only information reasonably needed to operate, secure and improve the Service.

A. Account and authentication information

- phone number, email address, country or calling code and verification status, depending on the sign-in method you choose;
- information returned by Google Sign-In or Sign in with Apple, such as provider account identifier, email address, name or profile information within the permissions you approve; Apple may provide a private relay email address;
- account identifier, identity provider, authentication tokens and session/device information;
- whether you mark a device as personal or temporary;
- account creation, login, logout and account-closure information.

One-time verification codes are delivered through our authentication and messaging providers. Google and Apple process sign-in information under their own terms and privacy notices. Do not share a verification code with anyone.

B. Profile and relationship-discovery information

Depending on what you choose to provide, this may include:

- display name, full name where required for a feature, date of birth or age, gender, city, country, relationship or marital status, relationship goal and profile story;

- profile photos and other photos you upload;
- mother tongue, matching languages and interests;
- education, occupation, height, weight, eye colour and body type;
- smoking, alcohol, pets, lifestyle pace, children plans, family goals and similar preferences;
- your answers, questions and basic or advanced search preferences;
- field-visibility choices.

Some profile fields, preferences, answers or content may reveal sensitive aspects of your life and, depending on their meaning, may reveal special-category information such as sexual orientation, health information, religious or philosophical beliefs. You should provide only information you are comfortable using in a relationship-discovery service. Where applicable law requires explicit consent for optional special-category information, Virema must obtain that consent separately or must not process the information for that purpose.

Stage 5 of Make Right Choice includes optional shared written answers concerning health, spiritual or cultural beliefs, and future marital intimacy. Virema stores the text of those three answers only after both Match participants give separate explicit consent for that Match. Either participant may instead use private-discussion mode, in which Virema stores only each participant's confirmation that the topic was discussed and does not store the sensitive answer text. These answers are not used for advertising or general matching. They are available to the two Match participants and may be processed by Virema and its contracted infrastructure provider Supabase acting only on Virema's instructions.

C. Identity-verification and trust information

If you choose to use an available identity-verification feature, we may process:

- an image of your identity document and a selfie showing you with that document;
- the document and selfie storage paths and technical upload information;
- a snapshot of your profile name, date of birth, gender, country and profile photo at the time of submission;
- your verification declaration and submission time;
- verification status, reviewer assignment, review notes, rejection reason, decision time and an audit trail of review actions.

Submitted cases are currently reviewed manually by authorised Virema administrators. Virema does not currently represent that an automated or AI identity-verification decision is performed. Identity verification may reduce some forms of impersonation, but it is not a criminal-background check and does not guarantee that a user is safe, truthful or compatible.

D. Matching, invitations and activity information

We process interactions needed for Match Profile, basic and advanced search, New Arrivals, Waves, responses, matches, chats, meetings and gradual relationship stages. This may include selected age and location ranges, selected preferences, compatibility or progression status, refresh usage, Wave usage, confirmations and feature history.

If you use an invitation or referral feature, we may process an invitation or referral identifier, the sharing action, link visits, inviter/invitee relationship, registration attribution and eligibility or benefit status. A recipient decides whether to open the link or register.

If you hide a field from other users, it should not be displayed on your public profile or cards. Where the app expressly explains that a hidden completed field remains usable by the matching system, we may use it only to evaluate relevant matching criteria and not to display it to another user. You can change or remove profile information and matching preferences in the app.

E. Communications, stage materials and user content

We process content you choose to create or send, including:

- text messages and edited message text;
- photos, audio messages and videos;
- questions, answers, stage notes, meeting records, proposal or wedding-planning materials and any proof image or PDF you choose to upload for a stage;
- reports, blocking actions and communications with support.
- when you call our published support number: the calling number, call time and

duration, technical call records, and any voicemail you choose to leave. The greeting tells you that a message may be recorded; automated transcription is disabled.

Virema does **not** claim that chats are end-to-end encrypted. Access is restricted using account controls, private storage and time-limited media links, but no online service can guarantee absolute security.

F. Purchase and supporter information

For Apple App Store and Google Play purchases, we receive product identifiers, transaction or purchase tokens, purchase state, environment, expiry or renewal information and backend-verification results. We do not receive your complete payment-card number. Apple or Google processes the payment under its own terms and privacy policy.

G. Device, technical and security information

This may include app version, operating system, device type, language, time zone, network and diagnostic information, IP address, security events, request identifiers, crash or error details, abuse indicators and permission status. We do not receive your Face ID, Touch ID, fingerprint or other biometric template when you enable the optional app lock; the operating system returns only an authentication result.

H. Permissions and location

With your permission, the Service may access:

- camera and photo library for profile photos, chat media, QR scanning, stage materials and optional identity-verification uploads;
- microphone for audio messages and camera audio;
- approximate or precise location when needed for a location feature.

You can change permissions in device settings. Refusing an optional permission may limit only the feature that needs it.

When you request automatic country/city detection during onboarding, the app obtains the device's current or last-known coordinates and asks the operating system's geocoding service to derive a place label. In the current flow Virema stores the resulting country and city, not the latitude and longitude. The operating-system or platform geocoding provider may process the coordinates under its own privacy terms.

The production mobile build reviewed on 15 September 2026 does not include a third-party advertising SDK, cross-app advertising tracker, third-party product-analytics SDK, third-party crash-reporting SDK or remote push-notification SDK. The notification screen currently displays product events created within the app. If this changes, we will update this Policy and the relevant Apple App Privacy and Google Play Data Safety disclosures before enabling the additional processing in a released build.

3. How we use information

We use personal information to:

- create, authenticate and protect accounts;
- support phone, email, Google and Apple sign-in and account recovery;
- provide profiles, search, matching, New Arrivals, Waves, chat, meetings and stages;
- operate invitations and registration attribution;
- show information according to your visibility choices;
- deliver media and synchronise data across authorised sessions;
- receive and manually review optional identity-verification submissions and display the resulting trust status;
- verify Apple and Google purchases and grant backend-confirmed supporter benefits;
- record acceptance of legal documents, age confirmation and profile-truth confirmation;
- provide on-device translation where supported;
- respond to support and privacy requests;
- detect, investigate and prevent fraud, spam, harassment, exploitation, unsafe behaviour and technical abuse;
- enforce our Terms and Community Guidelines;
- maintain, debug and improve reliability, accessibility and performance;
- meet legal, accounting, tax, payment, security and regulatory obligations.

4. Legal bases

Where law requires a legal basis, we rely as appropriate on:

- **contract**: processing necessary to create your account and provide the features you request;
- **consent**: optional permissions and other processing where consent is required; explicit consent is required where Article 9 GDPR or another applicable law requires it for special-category information; you may withdraw consent prospectively without affecting earlier lawful processing;
- **legitimate interests**: securing the Service, preventing abuse, maintaining reliability and improving features, balanced against your rights;
- **legal obligations and legal claims**: records or disclosures required by law, taxation, payment, safety, disputes or enforcement;
- **vital interests** in a genuine emergency where permitted by law.

Providing profile details beyond the minimum account information is generally optional, although a specific matching feature cannot work without the criteria it needs.

5. Matching, ranking and profiling

Virema uses rules and preferences to select or rank potentially relevant profiles and to operate relationship-progression features. Inputs may include age range, chosen search locations, languages, interests, advanced preferences, availability, safety restrictions and interaction history.

These processes help organise suggestions; they do not determine your legal rights, guarantee compatibility, verify identity or decide whether a relationship is safe. Virema does not use this matching to make a decision producing legal or similarly significant effects about you. You can change preferences, use basic rather than advanced criteria where available, or stop using the matching feature.

6. Local cache, media, location and translation

To make chats and profiles load more quickly, the app may keep a limited local copy of recent messages, profile images, translations and media on your device. The current chat cache retains up to 200 recent message records per chat. The shared image/file cache is configured to treat files as stale after up to 30 days, and the operating system may remove cached files earlier. Cached translations are tied to the user, chat and message. Signing out clears the current user's Virema chat and translation records on that device and clears shared image-cache entries available to the app. Deleting the app normally removes its local data; operating-system backup behaviour is controlled by the platform and your settings.

Chat attachments are stored in protected remote storage. The app obtains short-lived access links when it needs to display them and does not intentionally store those signed links as permanent message data.

Where supported, translation is performed on the device using Apple Translation or Google ML Kit. Text selected for translation is not intentionally sent to a Virema cloud translation service. Apple or Google may deliver language models or process technical platform information under their own policies.

7. How we disclose information

We do not sell personal information. We disclose it only as follows:

- **other users**, according to your profile visibility, matching and communication choices;
- **service providers**, including Supabase for authentication, database, storage and server functions; Twilio or the configured communications provider for phone verification, incoming support calls and voicemail storage; Apple and Google for sign-in, distribution, purchases, device translation, geocoding and other platform services; and website, security or infrastructure providers such as Cloudflare where used;
- **authorised Virema reviewers**, who may access the profile snapshot, document, selfie and case information necessary to decide an optional identity-verification submission, subject to role and country access controls;
- **professional advisers and authorities**, where reasonably necessary for legal advice, compliance, tax, audit, payment disputes, safety or lawful requests;
- **business changes**, if the Service or operator is reorganised, financed, merged or transferred, subject to appropriate confidentiality and legal safeguards;
- **with your direction or consent**.

Providers may process information only for contracted services and must be subject to appropriate legal and security obligations.

8. International transfers

Virema is an international Service operated from Belgium and uses providers that may process data in other countries. Your information may therefore be accessed or stored outside your country, where privacy laws may differ.

The primary region configured for Virema's current Supabase production project is Northeast Asia (Tokyo, `ap-northeast-1`). The project's primary database and Storage origin are located in that region. Storage content may be delivered through geographically distributed CDN caches, and Supabase Edge Functions may execute in a region close to the person or system invoking them. Twilio, Apple, Google, Cloudflare and their subprocessors may also process service data in other countries according to the service used.

Where required, we use an available legal transfer mechanism, contractual safeguards and risk assessment, and we limit transfers to what is reasonably necessary. EEA or UK users may contact us for information about the applicable safeguards. A dedicated mainland China launch would require a separate assessment of local collection,

storage and cross-border transfer obligations; the international Chinese translation is not a representation that this work has been completed.

9. Data retention

We keep information only for as long as reasonably needed for the purposes described above, including to provide an active account, protect users, maintain transaction and entitlement history, resolve disputes and comply with law.

Retention depends on the data and context:

- account and profile data are generally retained while the account is active;
- messages and attachments remain available while a Match is active. When a Match is archived, it disappears from both participants' active chats immediately and its ordinary message and attachment content is scheduled for deletion no later than 30 days after archival;
- an open moderation case or an expressly recorded legal hold may pause the 30-day deletion of the specific chat material reasonably needed for investigation, safety, dispute handling or legal claims;
- moderation evidence is scheduled for deletion 90 days after the related case is closed; free-text case details, internal administrative notes and routing notes are scheduled to be minimised after 12 months; the remaining moderation case record is scheduled for deletion after 24 months, unless a documented legal hold or legal obligation requires longer retention;
- original identity-verification documents and selfies are kept while manual review is pending and are scheduled for deletion 30 days after a final verified or rejected decision; unsubmitted or replaced identity uploads may be deleted after 7 days; the verification outcome, limited case metadata and access-restricted review audit may remain while the account is active where needed to maintain the trust status, handle an appeal and prevent verification fraud;
- a minimal block or pair-exclusion record, without the chat text or attachments, may remain while reasonably necessary to enforce a block, prevent the same pair from being shown again and protect users;
- purchase, tax and entitlement records may be retained for the legally required accounting, tax, refund, chargeback or dispute period;
- security logs and abuse-prevention identifiers may be retained for a proportionate period where necessary to protect users, investigate misuse and prevent repeat abuse;
- when a verified email address or phone number is used to receive a Type 1 invitation benefit, Virema keeps for 12 months a server-only keyed cryptographic marker derived from that identifier. The marker does not contain the raw email address, phone number, name or profile data and is used only to prevent the same verified identity from receiving the registration benefit again after account deletion. A repeat registration remains permitted, but no new Type 1 benefit is granted to either participant. A rejected repeat attempt does not restart or extend the 12-month period;
- support voicemail recordings are used to review and respond to the request. Virema runs a recurring deletion control so that voicemail media is removed no later than 31 days after receipt. Twilio may retain limited deleted-recording metadata for a further 40 days, and ordinary call-resource metadata may otherwise remain retrievable from Twilio for up to 13 months; Virema does not create automated voicemail transcripts;
- Virema's current Supabase production project has scheduled daily physical database backups. Point-in-time recovery (PITR) is not enabled. Deleted information may remain in backup copies until the applicable backup-retention cycle expires, unless a longer legal hold applies.

If you select account deactivation, Virema removes the active profile and personal product data and may retain a minimal recovery record containing the account identifier, real name, verified phone number and/or verified sign-in email for up to 90 days so an authorised manual restoration can be considered. If you select permanent deletion, no recovery archive is created. In both cases, files owned by the account are removed through the storage service and

the remaining purchase, moderation or safety records are deleted, de-identified or disconnected from the account where possible, subject to the exceptions described above.

"Clear for me" or a local cache action may affect only your device or your view. "Delete for everyone" is intended to remove the message from ordinary participant views, but limited copies may temporarily remain in backups, security records or legal holds. We do not retain information merely because it might be useful someday.

10. Account closure and deletion

You can choose deactivation or permanent account deletion through the app. You may also contact **support@virema.app** if you cannot use the in-app path. We will authenticate the request and delete or de-identify associated personal information unless retention is required or permitted for security, fraud prevention, payment records, disputes, legal claims or another legal obligation. Deactivation is designed to allow a limited 90-day manual recovery period; permanent deletion is not designed to be recoverable.

Removing the app, signing out or cancelling a store subscription does not by itself delete the Virema account. Account closure does not automatically cancel an Apple or Google subscription; manage the subscription in the relevant store as well.

11. Your rights and choices

Subject to applicable law, you may have the right to:

- know whether and how we process your information;
- access and receive a copy of it;
- correct inaccurate information;
- delete information or close your account;
- withdraw consent and change permissions;
- object to or restrict certain processing, including certain profiling;
- receive portable data where applicable;
- complain to a competent data-protection authority;
- not be discriminated against for exercising a statutory privacy right.

Use in-app controls where available or email **support@virema.app**. We may ask for information necessary to verify that the request concerns your account. Authorised-agent requests may require proof of authority. Some rights are subject to lawful exceptions.

You can withdraw the explicit consent used for sensitive relationship and matching information from **Settings** → **Privacy** by leaving Make Right Choice. This removes the profile from new MaRC discovery and matching while leaving existing active chats available. If you later choose to return to Make Right Choice, the app asks for explicit consent again and records the new time and consent-text version.

You can separately withdraw Stage 5 consent for one Match from Stage 5 or for all Matches from **Settings** → **Privacy**. Withdrawal deletes the three sensitive answer texts from active and archived application records without ending the Match, chat or completed progress. The topics then continue in private-discussion mode. Deleted answers are not restored if both participants later consent again. Residual copies may remain in encrypted rotating backups for up to seven days before automatic expiry, subject to any longer retention strictly required by law or security obligations.

We normally respond to a valid rights request within one month. Where permitted because a request is complex or numerous, we may extend that period and will explain the extension. You may lodge a complaint with the Belgian Data Protection Authority (Autorité de protection des données / Gegevensbeschermingsautoriteit), Rue de la Presse

35, 1000 Brussels, Belgium, contact@apd-gba.be, or with another competent supervisory authority in the place where you live or work or where an alleged infringement occurred.

12. Security and device protection

We use access controls, protected storage, encrypted transport, server-side purchase verification, short-lived media access links, role-restricted identity review, monitoring and other organisational and technical measures appropriate to the Service. We also provide optional device authentication through the operating system.

You are responsible for securing your phone number, email or provider account, device, verification codes and device unlock method; signing out on a shared device; and promptly reporting suspected unauthorised access. No system is perfectly secure. If a breach creates a legally reportable risk, we will notify affected users and authorities as required.

13. Safety, reports and moderation

Authorised human reviewers may review information reasonably necessary to assess an identity-verification submission, investigate a report, protect a person, enforce our rules or respond to law. Reports are not public to the reported user unless disclosure is required for fairness or law. We may use rule-based service restrictions, but this Policy does not represent that an automated system makes a final identity-verification or moderation decision. QR meeting confirmation, profile information, identity-verification status and progression percentages are not guarantees of safety, honesty or compatibility. In an emergency, contact local emergency services.

14. Adults only

Virema is only for people aged 18 or older. We do not knowingly permit children to create accounts. If you believe a person under 18 has provided information, contact support@virema.app so we can investigate and delete it where appropriate.

15. Changes to this Policy

We may update this Policy when the Service, providers or law changes. We will update the date and provide additional notice in the app or by another reasonable method when a change is material. We will request consent if law requires it. Continued use after an effective update is subject to rights that cannot be waived under applicable law.

16. Contact

Data controller: Valentyna Fomina Belgian sole proprietor (registered natural person) Enterprise number: **1009.416.048** Business establishment address: **Avenue Limbourg 55, 1070 Anderlecht, Belgium** Email: support@virema.app Voice support: **+1 570 359 4100** (English-language voicemail; carrier and international calling charges may apply)

No walk-in customer support is provided at this address. For the fastest response, please contact Virema by email or through the support channels made available in the Service. Do not leave passwords, one-time verification codes, payment-card details or identity-document numbers in a voicemail.