Privacy Policy — FindMyRave

Effective date: **2026-05-05**
Last updated: **2026-05-05**
Version: **1.0**

This Privacy Policy describes how Since 1993 BV ("Since 1993", "we", "us", "our") processes personal data in connection with the FindMyRave mobile app (iOS, Android) and the website at findmyrave.com (together, the "Service"). It is written for the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") and the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.

We have written this policy in plain English wherever we could, and tightened the language where the law requires precision. If you read only one section, read Section 4 — What we collect, why, and how long we keep it.

CONTENTS

1. Who is the data controller

The controller of your personal data is:

Since 1993 BV
A Belgian limited liability company (besloten vennootschap / société à responsabilité limitée)
VAT: BE1009154643
Registered office: Pijphoekstraat 1, 9041 Oostakker, Belgium
Country: Belgium
Email: the contact form

Since 1993 BV operates the FindMyRave service. We have not appointed a Data Protection Officer (DPO) because we are not legally required to under Article 37 GDPR. For all privacy

questions, complaints, and requests, please write to the contact form.

2. How to contact us about your data

For any question about this policy, to exercise your rights, or to report a security issue, contact the contact form. We respond within 30 calendar days, in line with Article 12(3) GDPR. If your request is complex or you have submitted multiple requests, we may extend that period by up to two further months and will tell you within the first month if we need the extension.

3. Scope of this policy

This policy applies to personal data we process when you:

- install, open, or use the FindMyRave mobile app (iOS or Android);
- create or sign in to a FindMyRave account;
- connect your Spotify or SoundCloud account to FindMyRave;
- submit content (events, flyer images, descriptions) to the community;
- create or join a Nearby post, including its group chat, expenses, and ride sharing;
- use the calendar subscription feature;
- browse the public website at findmyrave.com.

It does not apply to third-party services we link out to (for example, ticket providers, venue websites, Spotify, SoundCloud, Instagram, or Facebook). Once you leave our app to one of those services, their privacy policy applies.

4. What we collect, why, and how long we keep it

For each category below we tell you:

- the exact data points we store;
- where we store them;

- the legal basis under Article 6(1) GDPR;
- how long we keep them.

All personal data is stored in our Supabase project hosted in the EU (AWS Ireland, `eu-west-1`) unless explicitly noted otherwise.

4.1 Account data

FindMyRave currently uses passwordless authentication via Supabase Auth. Depending on the active sign-in method, we store one of the following identifiers in the `auth.users` table:

- **Email address** (current default sign-in method, V1)
- **Phone number in E.164 format** (planned phone-OTP method, V2; not active for general users at the effective date)

We also store: a Supabase-generated user UUID, account creation timestamp, last sign-in timestamp, and the one-time codes we send to verify your email or phone number. One-time codes expire within minutes.

Legal basis: Article 6(1)(b) GDPR — performance of the contract between you and us (giving you an account).
Retention: for the lifetime of your account. If you delete your account, we delete the row in `auth.users` and cascade-delete the data that is keyed on your user ID. Some content you have published (for example, events you submitted that have been approved into the public catalogue) may be retained in anonymised form — see Section 4.6.

> We do not currently collect a date of birth at sign-up. The minimum-age check described in Section 7 is enforced by your declaration when you create an account, by Apple App Store / Google Play age ratings, and by content moderation. We may add explicit DOB capture in a future release; this policy will be updated before that change.

4.2 Profile data

Stored in the `user_profiles` table:

- display name (no `@username` handle is used);
- profile photo / avatar (uploaded to the `avatars` Supabase Storage bucket);

- bio (free text, optional);
- home city (free text, optional);
- a flag indicating whether you have connected Spotify;
- profile creation timestamp.

Legal basis: Article 6(1)(b) GDPR — to operate the social and discovery features you signed up for.
Retention: until you change or delete the field, or delete your account.

4.3 Location data

The Service uses location data in three distinct ways. Each runs only with your explicit OS-level permission and only while the app is in the foreground.

4.3.1 Precise GPS — used in memory only

When you grant location permission and use the Nearby tab or the home location toggle, we read your precise GPS coordinates via the device's location services (`geolocator` Flutter plugin). We use the coordinates to:

- resolve your nearest city via the `nearest_city` Supabase RPC, so we can show you the right local events;
- compute the distance between your home city and your current location to decide whether to switch the app into "Nearby" mode;
- centre the Nearby map on your position.

Your raw GPS coordinates are **never written to our database** outside the cases listed below. They live in app memory only for the duration of the session.

4.3.2 Nearby posts — exact and fuzzy coordinates

If you create a Nearby post (for example, an afterparty, a meetup, a ride share), we write to the `nearby_posts` table:

- `latitude`, `longitude` — the exact GPS coordinates you posted from. These are visible only to participants who join your post and to the post author.
- `fuzzy_latitude`, `fuzzy_longitude` — the same coordinates rounded to roughly 110-metre precision. These are what we display to anyone browsing the public Nearby map. The

fuzzy radius is large enough to obscure your exact address while still being useful for "in this area" matching.

- category, emoji, title, description, optional linked event/venue, who-can-join scope (everyone / girls only / invite only), expiry timestamp.

4.3.3 Area presence — city-level only

For the "ravers nearby" social-proof counter, we record at most one row per user in the `user_area_presence` table containing only your **city ID** and a `last_seen_at` timestamp. No coordinates. Counts shown in the app ignore rows older than 30 days.

4.3.4 Trips

If you create a trip, we store the cities and date ranges you entered. Trips do not include GPS coordinates; trip filtering matches event venue cities/countries against the trip's stops client-side.

Legal basis: Article 6(1)(a) GDPR — your consent, expressed by granting OS-level location permission and by deciding to publish a Nearby post. You can revoke this at any time in your device settings; you can also delete any Nearby post you have created.
Retention: Nearby posts are deleted automatically after their `expires_at` timestamp (1 day after expiry, typically 24 hours after the event window). Area-presence rows are overwritten when you change city and ignored for display after 30 days; we run a periodic garbage-collection pass to physically delete rows older than 90 days.

4.4 Social graph and privacy settings

Stored across the `friendships`, `user_followers`, `follows`, `friend_groups`, and `privacy_settings` tables:

- friend requests, accepted friendships, declined friendships;
- one-way follower / following relationships, including pending approval state;
- follows of venues, artists, and organisations;
- your friend groups (group name, group privacy level, member list);
- blocks (where applicable);
- your privacy preferences: who can see the events you attend, your activity feed, your upcoming events, and your hearted events; whether other users can request to follow you;

whether you appear in search; whether you are visible to friends of friends.

Legal basis: Article 6(1)(b) GDPR — performance of the contract (the social graph is a core feature you signed up for).
Retention: for the lifetime of the relationship. When you remove a friend, the `friendships` row is deleted. When you delete your account, all rows referencing your user ID are cascade-deleted.

4.5 Activity, hearts, going, watching, bookmarks

Stored in the `hearted_events`, `activity_log` tables and in client-side state for ephemeral signals:

- **Hearts** (commitment to attend) — written to `hearted_events` with your user ID, the event ID, and a timestamp. Hearts are public to your mutual friends in line with your `shareHeartedScope` setting (default: friends only).
- **Going** — same storage as hearts; signals stronger commitment.
- **Watching** — a soft "swiped right" tier kept only in app memory; not persisted to the server.
- **Bookmarks** — written to a community-content bookmarks table (`user_id`, `content_type`, `content_id`). Bookmarks are **private** to you only; nobody else, including mutual friends, can see them.
- **Activity log** — a feed of your own actions (e.g. "you hearted X event"), used to power the Friends Feed. Visibility follows your privacy settings.

Legal basis: Article 6(1)(b) GDPR — performance of the contract; Article 6(1)(f) GDPR — our legitimate interest in operating recommendations and a social feed (you can object to the latter by tightening your privacy settings to friends-only or by removing yourself from the feed).
Retention: until you remove the action or delete your account.

4.6 Community submissions and flyer images

When you submit an event:

- We store the event details you entered (title, dates, times, venue, lineup, organiser, description, ticket URLs, social URLs) in the `events` table, with `submitted_by` set to your user ID and `moderation_status` initially set to `pending`.

- We upload the flyer image you provided to the `event-images` Supabase Storage bucket under a path of the form `community/<your-user-id>/<timestamp>.jpg`.
- If you opt in to OCR auto-fill, we send the image (or a Supabase Storage URL pointing at it) to the `extract-event` Supabase Edge Function, which forwards it to **OpenAI's GPT-4 Vision API** in the United States to extract structured event data from the flyer. We do not send your account identifier to OpenAI alongside the image. See Section 5 for the international-transfer safeguards.

Legal basis: Article 6(1)(b) GDPR — operating the submission feature you used; Article 6(1)(f) GDPR — our legitimate interest in maintaining a curated events catalogue (this includes keeping approved events visible after you delete your account, anonymised by removing the link to your user ID, because the events themselves are factual public information about real-world parties).
Retention: rejected submissions are deleted within 30 days. Approved events remain in the catalogue indefinitely; if you delete your account, the `submitted_by` reference is cleared so the event becomes anonymous.

4.7 Nearby posts, group chat, expense splitting, ride sharing

In addition to the location data described in Section 4.3, when you participate in a Nearby post we store:

- your participation in `post_participants` (post ID, user ID, joined-at timestamp);
- chat messages you send in the post group chat in `chat_messages` (post ID, sender user ID, sender display name and avatar URL snapshot, message text, sent-at timestamp);
- expense entries in `group_expenses` (post ID, who paid, amount, description, splits between participants);
- ride-share offers in `group_rides` and seat assignments in `group_ride_seats` (driver user ID, route, seat count, passenger user IDs).

Chat messages are stored as plaintext on our server. They are not end-to-end encrypted. Other participants of the post can read them. Treat the group chat the same way you would treat a public WhatsApp group.

Legal basis: Article 6(1)(b) GDPR — performance of the contract.
Retention: chat messages, expenses, and ride seats are deleted together with the parent post

when it expires or is deleted. We also keep an operational backup of the database for 7 days (Supabase's default point-in-time recovery window).

4.8 Spotify connection

Spotify connection is optional. If you connect, we initiate a PKCE OAuth flow with Spotify and request the following scopes:

- `user-top-read` — read your top artists;
- `user-follow-read` — read the artists you follow on Spotify.

The following data is stored on your device only, in the OS keychain (iOS Keychain, Android Keystore) via `flutter_secure_storage`:

- Spotify access token, refresh token, and expiry timestamp;
- Spotify username (the one returned by Spotify's `/me` endpoint);
- Spotify last-sync timestamp;
- OAuth PKCE code verifier (transient).

The following data is stored in `SharedPreferences` on your device:

- your imported Spotify artist list with tier (`fire`, `liked`, `spotify`) — used to personalise event recommendations and to auto-follow matching artists already present in our public artist catalogue.

We **do not store** your Spotify access token, refresh token, listening history, or top-artist list on our servers. Matching against the public artist catalogue happens on your device, and the only thing written to our database as a result is a row in the `follows` table for each matched artist.

Legal basis: Article 6(1)(a) GDPR — your consent, expressed by completing the Spotify OAuth flow.
Retention: tokens and the imported artist list remain on your device until you disconnect Spotify in the app, uninstall the app, clear app data, or revoke our access from your Spotify account settings. Spotify-related rows in our `follows` table behave like any other follow.

4.9 SoundCloud connection

SoundCloud connection is optional and uses a different mechanism than Spotify. SoundCloud has not granted us OAuth access, so we use the public `client_id` flow only:

- You enter your public SoundCloud handle. We resolve it to a public SoundCloud user ID via the `soundcloud-proxy` Supabase Edge Function, which calls SoundCloud's public API on our server side using a rotating `client_id` extracted from SoundCloud's frontend bundle.
- We then read your public followings and likes (only data SoundCloud already shows publicly on your profile) to match artists against our catalogue.

We do not receive any private SoundCloud credentials, do not store SoundCloud tokens (none are issued in this flow), and only see what any visitor to your public SoundCloud profile would see. The matched artists are stored as follows in the same `follows` table.

Legal basis: Article 6(1)(a) GDPR — your consent, expressed by entering your handle and pressing "Connect".
Retention: the SoundCloud handle is stored on your device only and removed when you disconnect.

4.10 Calendar subscription token

You can subscribe your calendar app (Apple Calendar, Google Calendar, Outlook) to a personal iCal feed of your hearted events. To make this work, we generate a per-user secret token via the `get_calendar_token` Supabase RPC and embed it in a URL of the form `https://<our-host>/calendar/<your-token>.ics`.

The token is a secret — anyone who has the URL can read your hearted events without logging in. Treat it like a password. You can rotate it at any time via the `reset_calendar_token` RPC, which immediately invalidates the previous URL.

Legal basis: Article 6(1)(b) GDPR — performance of the contract (a feature you actively enabled).
Retention: until you reset the token or delete your account.

4.11 Notes (encrypted)

The Notes feature is designed for sensitive personal content (set lists, after-party addresses, group plans). It uses a strict client-side encryption model:

- An **AES-256-GCM** encryption key is generated on first launch and stored only in your device's secure enclave (iOS Keychain via `flutter_secure_storage`; Android Keystore-backed equivalent).
- Note titles, body text, and checklist items are encrypted on your device *before* any network call. Each blob uses a fresh 12-byte IV and the GCM authentication tag is appended automatically.
- The ciphertext is then synced to the `notes` table in Supabase. Our database never sees plaintext, and we do not have your encryption key.
- Local notes are stored on your device in a SQLite database (managed by `NotesLocalDatasource`).

Practical consequences: if you uninstall the app or wipe the device's secure storage without first signing in elsewhere, your notes become unrecoverable, even to us. We consider this a feature, not a bug. On the web build, secure storage is not available; encryption is therefore disabled and Notes persistence is also disabled on web.

Legal basis: Article 6(1)(b) GDPR — performance of the contract.
Retention: until you delete the note or your account. Encrypted blobs are removed within 7 days of deletion.

4.12 Technical data

We do not run a third-party analytics SDK, a third-party crash reporter, an advertising SDK, or a tracking pixel. Specifically, the FindMyRave app does **not** include Firebase Analytics, Firebase Crashlytics, Sentry, Amplitude, Mixpanel, PostHog, the Meta SDK, the Google Ads SDK, or any equivalent.

Technical data we do see, by virtue of you connecting to our servers, is limited to what Supabase logs automatically:

- your IP address (used for routing and to enforce rate limits; visible in Supabase access logs);
- the time of the request and the API endpoint called;
- HTTP user-agent string sent by the device.

The `get-country-from-ip` Supabase Edge Function uses your IP address to guess your country at first launch, only to pick a sensible default city. The IP itself is not stored long-term

outside of standard infrastructure logs.

Legal basis: Article 6(1)(f) GDPR — our legitimate interest in keeping the Service secure, operational, and abuse-resistant.
Retention: Supabase access logs are retained for the period set by Supabase (typically 7 days for query logs and up to 30 days for audit logs); we do not extract or copy them into a separate analytics warehouse.

5. Sub-processors and international transfers

We use a small number of carefully chosen sub-processors. Each is bound by a Data Processing Agreement (DPA) that includes the European Commission's Standard Contractual Clauses (SCCs, Module 2 controller-to-processor) where required. We list every active sub-processor below.

Supabase Inc.	
PostgreSQL hosting, authentication, file storage, edge functions	
All server-side personal data described in Section 4 (except Notes plaintext, which we never have)	
AWS Ireland (`eu-west-1`) — within the EU	
Supabase is a US company; intra-group transfers from its EU infrastructure to its US parent, where they happen, are covered by SCCs in our DPA with Supabase.	
OpenAI, L.L.C.	
Optional: GPT-4 Vision OCR of event flyers you upload (Edge Function `extract-event`)	
The flyer image you uploaded (or a temporary URL pointing at it). No account identifier, no email, no phone number.	
United States	
SCCs (Module 2). OpenAI's API tier is contractually configured not to use submitted content to train its models. You can opt out of OCR by manually entering event details instead.	
Spotify AB	
Optional: OAuth authentication and read access to your top/followed artists when you connect Spotify	
OAuth handshake metadata; we initiate the call from your device. Spotify sees the fact that you authorised our client.	
Sweden / EU; Spotify operates globally.	

			Adequacy decision (EU/EEA) for Sweden; Spotify is itself the controller of the data on its side.
SoundCloud Limited	Optional: read your public profile (followings, likes) when you enter your SoundCloud handle	The public handle / user ID. We do not authenticate; we only read what is already public.	Germany / United States	Adequacy decision (Germany / EU); for any onward US transfer, SCCs apply via SoundCloud's own terms.
Apple Inc. (App Store)	Distribution of the iOS app, in-app review submissions, push notification routing if/when enabled	Apple identifiers tied to your Apple ID. We receive only aggregated, anonymised App Store reports.	Ireland (Apple Distribution International) and United States	SCCs / Apple's standard terms; Apple is itself the controller for App Store data.
Google LLC (Google Play)	Distribution of the Android app, in-store reviews	Google Play identifiers tied to your Google account. We receive only aggregated, anonymised Play Console reports.	Ireland (Google Ireland Ltd) and United States	SCCs / Google's standard terms; Google is itself the controller for Play Store data.

We will update this list before adding a new sub-processor that touches personal data. The current list is canonical; if a service is not listed here, we do not send your data to it.

6. Security

The technical and organisational measures we have in place include:

- **Passwordless authentication** — sign-in is via email magic link or one-time code (or, in V2, phone OTP). There are no user-chosen passwords to leak.
- **Row Level Security (RLS)** — every Postgres table that holds personal data has RLS policies enforced at the database level. The Supabase anon key embedded in the app cannot bypass these policies.

- **Client-side encryption for Notes** — AES-256-GCM with the key held only in your device's secure enclave, as described in Section 4.11. We cannot read your notes.
- **TLS in transit** — all traffic between the app and our backend uses HTTPS / TLS 1.2+.
- **Secret handling** — third-party API keys (OpenAI, SoundCloud) live only in Supabase Edge Function environment variables; they are never shipped in the mobile app binary.
- **Calendar token rotation** — you can invalidate a leaked iCal subscription URL on demand.
- **Least privilege** — only the developer of Since 1993 BV has administrative access to the Supabase project.

No system is impenetrable. If we discover a personal-data breach that is likely to result in a risk to your rights and freedoms, we will notify the Belgian Data Protection Authority within 72 hours as required by Article 33 GDPR, and notify you directly when Article 34 GDPR applies.

7. Children and minimum age

The FindMyRave Service is intended for people aged **18 and over**. The Service centres on adult electronic music events, many of which serve alcohol, take place at night, and involve travel to unknown venues — including the Nearby stranger-meeting feature. We consider 18 the appropriate floor.

We do not knowingly process the personal data of anyone under 18. If we become aware that we have collected personal data from someone under 18, we will delete the account and the associated data without undue delay. If you believe a minor has created an account, please report it to the contact form.

8. Your rights

Under the GDPR you have, in respect of your personal data, the right to:

- **Access** (Article 15) — obtain confirmation of whether we process your data and a copy of it.
- **Rectification** (Article 16) — correct inaccurate or incomplete data. You can edit your display name, bio, home city, and avatar in the app.

- **Erasure** (Article 17, "right to be forgotten") — request deletion of your data. Deleting your account from the app triggers cascade deletion across the tables described above. You can also request deletion by writing to the contact form.
- **Restriction of processing** (Article 18).
- **Data portability** (Article 20) — receive the data you provided in a structured, commonly used, machine-readable format. We will provide a JSON export on request.
- **Objection** (Article 21) — object to processing based on Article 6(1)(f). In practice this affects the social feed and recommendations; tightening your privacy settings to friends-only is the in-app way to exercise this.
- **Withdraw consent** (Article 7(3)) — for any processing based on Article 6(1)(a), at any time. Disconnect Spotify or SoundCloud in the app, or revoke OS-level location permission. Withdrawal does not affect the lawfulness of processing before withdrawal.
- **Lodge a complaint** with a supervisory authority (Article 77) — see Section 12.

We will not charge you for exercising these rights unless your request is manifestly unfounded or excessive (Article 12(5) GDPR), in which case we will tell you why before charging or refusing.

9. Cookies and similar technologies

The mobile app uses no advertising or analytics cookies. It uses local device storage (`SharedPreferences`, `SQLite`, `flutter_secure_storage`) to remember your settings, your encryption key, your Spotify session, and your offline notes — these are not cookies in the web sense and are described in the relevant rows of Section 4.

The website at findmyrave.com uses only strictly necessary cookies and, where applicable, a small number of opt-in cookies. The full list, purposes, and retention periods are documented separately in our Cookie Notice.

10. Automated decision-making and profiling

We use a multi-tier scoring algorithm to rank events in the "Featured" carousel based on signals such as artists you follow, friends going, your Spotify taste, and genre overlap. This is profiling within the meaning of Article 4(4) GDPR.

It is **not** a decision with legal or similarly significant effects under Article 22 GDPR — the only outcome is which events appear higher in your list, and you can always browse the full catalogue. You can reduce the input to this ranking by tightening your privacy settings, disconnecting Spotify, or unfollowing artists/venues.

11. Changes to this policy

We will revise this policy when we add features, change sub-processors, or change the way we handle data. The "Last updated" date at the top of the page reflects the latest revision. For material changes we will notify you in-app before the change takes effect; minor clarifications may be made silently.

12. Complaints to a supervisory authority

If you believe our processing of your personal data infringes the GDPR, you have the right to lodge a complaint with a supervisory authority, in particular in the EU/EEA Member State of your habitual residence, place of work, or place of the alleged infringement. Our lead supervisory authority is:

Gegevensbeschermingsautoriteit / Autorité de protection des données
(Belgian Data Protection Authority)
Rue de la Presse 35 / Drukpersstraat 35
1000 Brussels, Belgium
Tel: +32 (0)2 274 48 00
Email: contact@apd-gba.be
Website: www.gegevensbeschermingsautoriteit.be

We would prefer the chance to address your concern first — please write to the contact form.

© Since 1993 BV. This policy was last updated on 2026-05-05.

FIND MY RAVE

The map for electronic music. Made by Since 1993 BV. Ghent, Belgium.

PRODUCT

How it works

Screenshots

Get early access

COMPANY

About

Contact

LEGAL

Privacy policy

Terms of service

Cookies

Since 1993 BV · Ghent, Belgium · VAT BE1009154643

© 2026 Since 1993 BV. All rights reserved.