PRIVACY POLICY

PHMARKET MOBILE APPLICATION

Effective from: 1 June 2026

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Czech Republic

Company ID: 04529031 | VAT ID: CZ04529031 | Data box: 234baq7

1. INTRODUCTION AND CONTROLLER CONTACT

This Privacy Policy (the "Policy") describes how PHMarket s.r.o., Company ID: 04529031, with its registered office at Hlavní třída 87/2, 737 01 Český Těšín, Czech Republic, registered in the Commercial Register maintained by the Regional Court in Ostrava, Section C, File No. 64228 ("PHMarket", the "Controller", "we" or "our"), processes the personal data of users of the PHMarket mobile application (bundle identifier cz.phmarket.app, the "App").

This Policy is an integral part of the General Terms of Service (the "Terms") and is to be interpreted in conjunction with them. Capitalized terms not defined here have the meaning set out in the Terms.

Processing takes place in accordance with Regulation (EU) 2016/679 ("GDPR"), Act No. 110/2019 Coll., on the Processing of Personal Data, Act No. 480/2004 Coll., on Certain Information Society Services, Regulation (EU) 2022/2065 (DSA) and other applicable legislation.

Controller contact details:

PHMarket s.r.o., Hlavní třída 87/2, 737 01 Český Těšín, Czech Republic

Company ID: 04529031 | VAT ID: CZ04529031 | Data box: 234baq7

Personal data protection: privacy@phmarket.cz | General support: support@phmarket.cz

Website: https://www.phmarket.cz

Given the nature and scope of the processing, the Controller is not obliged to appoint a Data Protection Officer (DPO) under Art. 37 GDPR. All communication regarding data protection takes place via the dedicated address privacy@phmarket.cz.

2. SCOPE AND KEY CONCEPTS

2.1. Geographic scope: The App is primarily intended for users from EU Member States, the United Kingdom, Norway, Iceland, Liechtenstein and Switzerland. When used from another jurisdiction, processing takes place in accordance with the GDPR.

2.2. Data subject: You, as a natural person who downloads, installs, creates an Account or otherwise uses the App, whether in "Use without Registration" mode or as a Registered user.

2.3. Key difference between the modes:

- Use without Registration: The App works without creating an Account; basic features are available (map, prices, navigation, Quality Stations, Fuel Quality in read-only). Processed data is limited to technical device identifiers (install_id, a UUID generated by the App), preference settings (language, currency) and pseudonymized analytical data. This is NOT an anonymous Supabase account; a formal user account in our database (auth.users) is created only upon registration.
- Registered Account: A full account including a name/nickname, email and other data necessary for participation in the PHM Cash Program, the PusHMe service, Community Price Reports, the creation of Community Stations, Fuel Quality ratings and Flash Offer redemption.

3. CATEGORIES OF PROCESSED PERSONAL DATA

The Controller collects and processes the following categories of personal data, always to the extent necessary for the specific purpose and in line with the data minimization principle under Art. 5(1)(c) GDPR:

3.1. Identification and contact data (Registered Account only)

- Name or nickname (a real legal name is not required; stored in user_metadata.nickname or user_metadata.first_name)
- Email address (may be a "relay" email from Apple Hide My Email if you sign in via Sign in with Apple; in that case we do not receive your real address)
- Apple ID or Google ID (only an internal identifier provided by the OAuth process, not the password to your Apple/Google account)
- Password (stored in hashed form using bcrypt with salt in Supabase Auth, never in plaintext); only if you register by email

3.2. Technical and device identification data

- install_id: A unique identifier of the App installation generated at first launch and stored locally (MMKV). It is not a system identifier (IDFA on iOS / AAID on Android); it cannot be used for cross-app tracking.
- Mobile device type and model (e.g. iPhone 15, Samsung Galaxy S24); collected via expo-device
- Device manufacturer brand (Apple, Samsung etc.)
- Operating system version (iOS 18, Android 14 etc.)
- App version (app_version from expo-application)
- IP address (anonymized; we retain only the first three octets, e.g. 192.168.1.* instead of 192.168.1.45, exclusively for coarse geographic analysis)
- Language settings and time zone (locale, timezone); from expo-localization
- Push notification token (Expo Push Token; the Expo Push Service, which routes it onward to Apple APNs or Google FCM)

3.3. Location data

The App works with your current location to display nearby Partner Stations, calculate distances, navigate, detect the country for Fuel Quality and operate the snap-to-station mechanism when reporting prices. Processing takes place as follows:

Foreground-only tracking: The App obtains your location exclusively while it is in the foreground. We do NOT track location in the background. When the app is closed or moved to the background, the GPS subscription ends (at the iOS/Android OS level). We use only the foreground permission (Location.requestForegroundPermissionsAsync in expo-location).

Location accuracy: We use a single accuracy level, Location.Accuracy.Balanced (approximately ~100 meters). We do not use the highest accuracy (High accuracy, ~5 to 20 meters), because balanced is sufficient for the app's functionality.

Continuous tracking in the foreground: After consent is granted, the OS calls watchPositionAsync with a 30-second interval and a 50-meter threshold; in our app we store a new state only if the user has moved more than 100 meters or a certain time has elapsed. The location is therefore not stored on the server or locally every 30 seconds; it is stored only for the current app session.

Location persistence: We do not permanently store your GPS coordinates on servers, except where they are part of a specific record (e.g. a refueling under the PHM Cash Program, a community price report, the creation of a Community Station). In these cases we store only the coordinates associated with the given record, not a historical movement trail.

Detected country (cache): For the Fuel Quality feature we detect the country (CZ/PL/SK/DE/AT/HU) based on the last location and store this country code locally in MMKV (fq_detected_country). It serves to automatically initialize the Fuel Quality section on next opening, not for profiling.

Snap-to-station: When reporting a fuel price (Community Report), the App calls the find_nearest_station(GPS) function, which "snaps" your location to the nearest Catalog Station within a 25 km radius. This is an ANTI-SABOTAGE measure; a price cannot be reported for an arbitrary GPS coordinate, only for an existing station. Your GPS at the time of reporting is not retained as part of the price; only the fuel_station_id is stored.

Withdrawal of location consent: You may withdraw it at any time in the iOS/Android settings. The App also works without location; it merely cannot sort stations by distance, navigate or snap prices. Instead of the current location, the "last known location" cached by the OS is used, or the user is prompted to enter a destination as text.

3.4. Vehicle and driver profile data

- Fuel type (Natural 95, Diesel, LPG, CNG, AdBlue, HVO, EV)
- Fuel consumption (l/100 km or kWh/100 km)
- Tank or battery capacity (for EVs)
- Vehicle type (passenger car, light commercial, truck, etc.)
- Preferred currency for displaying prices (CZK, EUR, PLN, HUF, USD)
- Preferred distance unit (kilometers / miles)
- Preferred navigation app (Apple Maps, Google Maps, Waze, Mapy.cz)

The vehicle profile is stored both locally (a cache in MMKV under the key vehicle_cache for the stale-while-revalidate pattern) and on the server in user_metadata for synchronization between devices.

Profile photograph (processed exclusively on the device): If you set a profile photograph, the App resizes it to 200 x 200 pixels and stores it exclusively locally in your device's storage (documentDirectory). The profile photograph is NEVER sent to the servers of the Operator or third parties and is not part of any data transmission. You remove it in the App profile or by uninstalling the App. The photo library permission is requested only at the moment of selecting the photograph and serves exclusively this purpose.

3.5. In-App activity data

- History of Partner Stations visited in the App (opening a station detail)

- Refueling history recorded under the PHM Cash Program (date, time, Partner Station, fuel type, quantity, price, GPS at the time of refueling for verification)
- Community Price Reports: price, fuel_station_id, fuel type, timestamp, source_currency, currency, fx rate
- Created Community Stations: name, address, city, GPS coordinates, creator_display (a shortened name from user_metadata.display_name or the email prefix)
- Fuel Quality ratings: fuel_station_id, is_positive (boolean), an optional comment (max. 200 characters), an optional brand_suggestion (station brand suggestion)
- Reviews and ratings of Partner Stations
- Followed Partner Stations ("favorites")
- Routes and navigation queries (retained only temporarily for calculation; the recent_destinations_v1 cache, FIFO max. 8 items, locally)
- Easter egg progress (ee_station_detail_count, ee_app_open_count, ee_radio_unlocked, radio_cooldown_sent_at): local counters for unlocking PusHMe

3.6. PHM Cash Program data

Note: The PHM Cash Program is in preparation (coming soon) as of the effective date of this Policy. The data categories below will be processed from the moment the Program is launched.

- PHM Cash Points balance and current Level
- History of earning and redeeming Points (transactions log)
- Referral identifier (if you were invited by another user)
- Bank details: IBAN and the account holder's name (only if you request the annual payout of the monetary reward; stored only at the moment of claiming the payout, not automatically)
- Contribution score (an internal reputation score typically ranging from -10 upwards), used for automated moderation (see Article 4.4 below, the shadowban and transparent moderation)

3.7. PusHMe Service data

PusHMe is a system of encrypted short messages on user-defined Frequencies (1000 to 9999). Encryption takes place on the sender's device before sending to the server. Processing details:

Cipher key: The key is derived using SHA-256 from the string 'phmarket:radio:v1:' + the Frequency (e.g. 'phmarket:radio:v1:4242'). This is not a trivial XOR with the numeric Frequency as the key, but XOR with a 256-bit hash-derived key. In normal operation, the PHMarket server cannot read the content of messages without knowing the Frequency.

PLAIN: fallback (important): If the cryptographic API (Crypto.digestStringAsync) fails on the user's device, typically on very old devices, the App has a fallback mode in which it stores the message with the prefix "PLAIN:" in plaintext. In that case the message content is readable even without knowledge of the Frequency, for the duration of the 30-minute retention period. The probability of this occurring is low in practice (approx. <0.5 % of devices), but we disclose it for full transparency.

- Message metadata (stored on the server): time of sending, anonymized sender identifier (the auth.users.id UUID, not email/name), the Frequency (numeric channel 1000 to 9999), optionally a station_id (station context)

- Encrypted message content: stored on the server for a maximum of 30 minutes (expires_at default now() + 30 min); then automatically and irreversibly deleted by a cron job
- System Channels (101 Live drops, 111 Café & food, 121 Car care, 131 Special): messages in System Channels are PLAINTEXT (is_system=true) and are broadcast by the Operator or partners authorized by it. They serve as a marketing-light channel; the sending of commercial communications in System Channels is subject to consent under Section 7 of Act No. 480/2004 Coll. (consent to push notifications in Profile, Notifications)
- The list of your favorite Frequencies (radio_listening, max. 5): stored in the profiles table on the server
- The list of blocked users on individual Frequencies: stored locally
- Message reports (the radio_reports table): if you report a message, we retain for this report the encrypted content, the sender's identifier, the report category (illegal / harassment / spam / other), the time and your reporter ID; retained for 30 days from completion of the review or 1 year for purposes of a potential dispute

3.8. Analytical and diagnostic data

PostHog (product analytics): To understand how the App is used, we use PostHog, Inc. on an EU instance (host: https://eu.i.posthog.com). We collect pseudonymized analytical events: screen views, taps, navigation actions, success/failure of operations, easter egg progress, performance metrics. The distinct_id identifier in PostHog is the install_id during Use without Registration (anonymous per-installation) and your Supabase user_id with a Registered Account. This is therefore PSEUDONYMIZATION, not full anonymization; the user is identified consistently across sessions, but the identifier cannot on its own be traced back to your person without an additional data point (email / name) from our database. On logout we call posthog.reset(); a new session receives a new identity.

Sentry (error and crash diagnostics): To detect and fix bugs we use Sentry (Functional Software, Inc.) on US infrastructure with SCCs. Sentry captures JavaScript errors, native crashes, stack traces, breadcrumbs (captured trackEvent events forwarded to Sentry), device context (model, OS) and a pseudonymized user identifier. Sentry retention is 90 days.

- Context automatically attached to analytical events: session_id, install_id, device_model, device_brand, os_version, timezone, locale, app_version, app_start_type (cold/warm), push_permission_status
- Specific events: APP_OPEN, FIRST_OPEN, SESSION_END, LOGIN_SUCCESS, LOGIN_FAILED, REGISTER_SUCCESS, LOGOUT, GDPR_ACCEPTED, GDPR_DECLINED, ONBOARDING_STARTED, ONBOARDING_COMPLETED, SCREEN_VIEW, TAB_SWITCHED, MAP_PIN_TAPPED, STATION_VIEW, STATION_NAVIGATE, URGENT_NAVIGATE, LOCATION_DENIED, PUSH_PERMISSION_UPDATED, COMMUNITY_STATION_CREATED, COMMUNITY_PRICE_SUBMITTED, FLASH_OFFER_CLAIMED, BENEFIT_VIEW, FUEL_QUALITY_*, ERROR_BOUNDARY and other technical events
- Geographic aggregation for statistics: your GPS coordinates are rounded in analytical aggregations to ~10 km blocks (lat_bucket, lng_bucket) to identify geographic trends, not to identify a specific place

3.9. Support communication data

- The content of your message sent to support (support@phmarket.cz, privacy@phmarket.cz, legal@phmarket.cz, notice@phmarket.cz, csae@phmarket.cz)
- Our replies and any further communication
- Communication metadata (time, email address, subject)

4. PROCESSING PURPOSES AND LEGAL BASES

The Controller processes your personal data only for specific, explicitly stated and legitimate purposes, on the basis of a specific legal ground under Art. 6(1) GDPR. Detailed overview:

4.1. Provision of the App's basic features (map, fuel prices, navigation, Quality Stations, Fuel Quality in read-only) to users without registration and Registered Users. Legal basis: contract performance (Art. 6(1)(b) GDPR), i.e. performance of the Terms, which constitute the contract. Data: technical device data, location data (foreground only), preference settings. Retention: for the duration of use of the App; preference settings for the duration of the Account or until uninstallation.

4.2. Management of the Registered Account, authentication, password reset. Legal basis: contract performance (Art. 6(1)(b) GDPR). Data: name/nickname, email, hashed password, Apple/Google OAuth identifier. Retention: for the duration of the Account + 90 days after deletion for backup rotation.

4.3. Participation in the PHM Cash Program (awarding Points, refueling records, payouts); active from the Program launch, currently coming soon. Legal basis: contract performance (Art. 6(1)(b) GDPR); a legal obligation under the Accounting Act and tax laws (Art. 6(1)(c) GDPR) for accounting purposes. Data: identification data, refueling data, level, points, bank details (IBAN, account holder), the IBAN only upon claiming a payout. Retention: for the duration of participation in the Program; accounting documents 10 years under Act No. 563/1991 Coll.

4.4. The PusHMe Service: sending and delivering encrypted messages between users, content moderation, abuse prevention. Legal basis: contract performance (Art. 6(1)(b) GDPR); legitimate interest (Art. 6(1)(f) GDPR) for moderation and abuse prevention. Data: message metadata, encrypted content (or PLAIN: fallback), sender identifier, blocked users, reports. Retention: encrypted/plaintext content max. 30 minutes; metadata max. 90 days; reports until review completion + 1 year.

4.5. Community Price Reports, creation of Community Stations, reviews, ratings of Partner Stations. Legal basis: contract performance (Art. 6(1)(b) GDPR); legitimate interest (Art. 6(1)(f) GDPR), operation of the App and information quality; anti-fraud audit (prices_audit). Data: user identifier, creator_display, report/station content, timestamp, GPS for snap-to-station verification (not stored long-term), anti-fraud rate_limit_block records. Retention: contributions for the duration of the Account or until deletion of the individual content; anti-fraud audit 3 years.

4.6. Fuel Quality ratings: reviews (positive / with reservations), brand suggestions. Legal basis: contract performance (Art. 6(1)(b) GDPR) and legitimate interest (Art. 6(1)(f) GDPR), informing consumers about fuel quality. Data: fuel_station_id, is_positive, an optional comment (max. 200

characters), an optional brand_suggestion, user identifier, time. Retention: for the duration of the Account or until deletion of the individual rating.

4.7. Publication of penalties imposed by the Czech Trade Inspection Authority (ČOI) in the Fuel Quality section. Legal basis: legitimate interest (Art. 6(1)(f) GDPR), informing consumers about publicly available data on fuel quality; the data originates from publicly published ČOI decisions. Data: station name, city, penalty year, reason, URL of the ČOI source document. Retention: for as long as the data is relevant (active penalty) + 3 years.

4.8. Service push notifications (Account changes, PHM Cash Points, content moderation, Statement of Reasons). Legal basis: contract performance and legitimate interest (Art. 6(1)(b) and (f) GDPR). Data: Expo Push Token, Account event data. Retention: for the duration of use of the App.

4.9. Marketing push notifications, news, Flash Offers in PusHMe (currently inactive; to be activated in future versions). Legal basis: consent (Art. 6(1)(a) GDPR), granted via the opt-in dialog in Profile, Notifications. Data: Expo Push Token, preferences (notif_nearby, notif_discount, notif_loyalty, notif_quality, notif_location). Retention: until withdrawal of consent.

4.10. Product analytics (PostHog): improving UX, preventing errors, A/B testing. Legal basis: legitimate interest (Art. 6(1)(f) GDPR). This is an important change compared to earlier versions of this Policy; analytics was originally conditioned on a separate consent in the GDPR consent screen; following review, this conditionality was assessed as incompatible with Art. 7(4) GDPR and EDPB Guidelines 5/2020 (consent bundling). Analytics now takes place on the basis of legitimate interest with pseudonymization, EU hosting and an easy opt-out in Profile, Privacy. Data: pseudonymized analytical events, install_id (before registration), Supabase user_id (after registration); device context (model, OS, locale). Retention: PostHog 12 months; aggregated anonymous statistics indefinitely.

4.11. Error and crash diagnostics (Sentry). Legal basis: legitimate interest (Art. 6(1)(f) GDPR). Data: stack trace, breadcrumbs, pseudonymized device identifier, OS/app version, device context. Retention: 90 days (Sentry retention).

4.12. Fraud prevention, prevention of abuse of the PHM Cash Program, PusHMe and Flash Offers; automated moderation including the shadowban system (transparently, per Art. 17 DSA). Legal basis: legitimate interest (Art. 6(1)(f) GDPR); a legal obligation under the DSA. Data: activity data, contribution_score, IP address (anonymized), device, prices_audit records. Retention: for the duration of the investigation + 3 years for a potential dispute.

4.13. Compliance with DSA obligations (notice-and-action, statement of reasons, internal complaints, transparency reporting). Legal basis: a legal obligation (Art. 6(1)(c) GDPR), Regulation (EU) 2022/2065. Data: data on reports, moderation decisions, appeals, transparency reports. Retention: 5 years from completion of the review.

4.14. Support communication and complaint handling. Legal basis: contract performance and legitimate interest (Art. 6(1)(b) and (f) GDPR). Data: communication content, email address, metadata. Retention: 3 years from the last contact.

4.15. Compliance with legal obligations (accounting, taxes, AML, requests of public authorities). Legal basis: a legal obligation (Art. 6(1)(c) GDPR). Data: accounting and tax data including bank details for PHM Cash payouts, data for fulfilling requests. Retention: 5 to 10 years under the Accounting Act and tax laws.

5. DATA RETENTION

5.1. General principle: We retain data only for the period strictly necessary to fulfill the relevant processing purpose and in line with data minimization. Upon expiry of the retention period, data is irreversibly deleted or anonymized.

5.2. Account deletion: Upon deletion of the Account, we initiate the following process:

- Production database: 30 days from confirmation of the request
- Backups: 90 days from confirmation of the request (backups are rotated automatically)
- Accounting documents and data for AML and tax purposes: 5 to 10 years regardless of Account deletion
- Data related to an ongoing dispute/investigation: for its duration + 3 years
- Anonymized data (aggregated statistics): may be retained indefinitely
- PostHog distinct_id: we call posthog.reset() on logout; after Account deletion a new session no longer has a link to the user_id, but historical events in PostHog tied to the user_id remain within the 12-month retention; upon an erasure request we also call the PostHog Delete API

5.3. Sign in with Apple revoke (commitment): If you signed in via Sign in with Apple and request Account deletion, the Controller calls the Apple Sign In REST API revokeToken endpoint as part of the deletion process and revokes your refresh + access tokens with Apple Inc. This commitment is mandated by Apple App Store Review Guideline 5.1.1(v); implementation details are published in the code-side change tracking document.

6. DATA RECIPIENTS AND PROCESSORS

We transfer your personal data to the following categories of recipients, always to the extent necessary for the given purpose and on the basis of data processing agreements under Art. 28 GDPR:

6.1. Processors (Data Processors)

Supabase Inc. (USA; database hosted in Frankfurt, EU) Role: hosting of the Postgres database (auth.users, profiles, stations, prices, radio_broadcasts, fuel_stations etc.), authentication, real-time features for PusHMe and community price broadcast. Legal basis: DPA + SCCs; data stored exclusively in the EU region (Frankfurt); ISO 27001/SOC 2.

PostHog, Inc. (USA; EU instance: eu.i.posthog.com) Role: pseudonymized product analytics. Legal basis: DPA; an EU instance without transfer of analytical data to the USA.

Functional Software, Inc. d/b/a Sentry (USA) Role: App error and crash diagnostics. Legal basis: DPA + SCCs; pseudonymization of identifiers; short retention (90 days).

Apple Inc. (USA / Ireland for EU operations) Role: push notification delivery (APNs); Sign in with Apple authentication; App Store distribution. Legal basis: Apple Developer Program Agreement + Apple Privacy Policy; transfer mechanisms per the EU adequacy decision / DPF.

Google LLC (USA / Ireland for the EU) Role: push notification delivery (FCM); Sign in with Google; Maps API for map tiles; Google Play distribution. Legal basis: Google API Terms + DPA; SCCs / DPF.

Expo (650 Industries, Inc., USA) Role: the Expo Push Service as a brokerage layer between the App and APNs/FCM; OTA updates infrastructure. Legal basis: Expo Privacy Policy; the Expo Push Token serves as a proxy for the APNs/FCM token; SCCs.

Resend / Mailgun or similar (transactional email provider) Role: delivery of transactional emails (registration confirmation, password reset, account deletion). Legal basis: DPA + SCCs; minimal retention.

6.2. Data Recipients

- Partner Stations: to a limited extent upon Flash Offer redemption (claim_code, time, station_code) or registration of a refueling under the PHM Cash Program (a pseudonymized identifier + refueling data). Partner Stations do not receive your name, email or Apple/Google ID.
- The Operator's bank: for the payout of the monetary reward from the PHM Cash Program (IBAN, account holder name, amount); from the launch of the Program.
- Tax administration: if a payout exceeds statutory reporting limits.
- The Operator's accounting firm: within ordinary accounting operations.
- Legal representatives, auditors: in fulfilling legal obligations.
- Law enforcement authorities, courts, supervisory authorities (ÚOOÚ, ČOI, ČTÚ, the DSCs of other EU Member States): upon a duly submitted request and in accordance with applicable law.
- The National Center for Missing & Exploited Children (NCMEC) via the Internet Watch Foundation: upon detection of CSAM/CSAE content (Art. 22 of the Terms and the CSAE Policy).
- Trusted flaggers (DSA Art. 22): based on their notices and to the extent necessary for the exercise of their authority.

7. INTERNATIONAL DATA TRANSFERS

7.1. EU localization principle: We operate our primary data infrastructure (the Supabase database, PusHMe servers) exclusively within the European Economic Area (EEA), specifically in Germany (Frankfurt). No international transfers to third countries within the meaning of the GDPR take place there.

7.2. Transfers to the USA and third countries: Some processors (Apple, Google, Expo, Sentry, Resend/ Mailgun) are headquartered in the United States. For these transfers we apply:

- Standard Contractual Clauses (SCCs) under Commission Implementing Decision (EU) 2021/914 as the legal mechanism under Art. 46(2)(c) GDPR
- Apple and Google: certified under the EU-U.S. Data Privacy Framework (DPF) where this mechanism is in effect; alternatively SCCs
- Supplementary measures: encryption in transit (TLS 1.3) and at rest (AES-256); pseudonymization of identifiers; minimization of transferred data

7.3. Transfer Impact Assessment: For each systematic transfer to a third country, we conduct a Transfer Impact Assessment (TIA) per EDPB recommendations.

8. YOUR RIGHTS AS A DATA SUBJECT

In connection with the processing of your personal data, you have the following rights under the GDPR. You may exercise them at any time at privacy@phmarket.cz or directly in the App (where the specific right enables it):

Right of access (Art. 15 GDPR) You have the right to obtain confirmation as to whether your data is being processed and, if so, the right of access to the data and to information about the processing. You may request a copy of the data, which we will provide free of charge (a reasonable fee for further copies).

Right to rectification (Art. 16 GDPR) You have the right to have inaccurate data rectified. Most data can be edited directly in Profile, Edit Profile in the App.

Right to erasure (Art. 17 GDPR) You may request the erasure of your data, preferably via the "Delete Account" feature in the App (Profile, Settings, Delete Account), via the web phmarket.cz/delete-account, or by email to support@phmarket.cz. Erasure may be limited by compliance with legal obligations (accounting, AML, DSA reporting).

Right to restriction of processing (Art. 18 GDPR) You may request restriction of processing in the cases under Art. 18(1) GDPR.

Right to data portability (Art. 20 GDPR) You have the right to receive the data you provided in a structured, commonly used and machine-readable format (JSON) and to transmit it to another controller.

Right to object (Art. 21 GDPR) You have the right to object at any time to processing based on legitimate interest (Art. 6(1)(f)). This concerns in particular: product analytics (PostHog), diagnostics (Sentry), fraud prevention, moderation, geographic aggregation. You may object in Profile, Privacy, Raise an Objection, or by email to privacy@phmarket.cz. Upon an objection we will cease the processing unless we demonstrate compelling legitimate grounds overriding your interests. FOR PostHog ANALYTICS: you may simply opt out in Profile, Privacy, Analytics (a toggle); after switching it off, PostHog is no longer called in the app (a purely client-side gate).

Right not to be subject to automated decision-making (Art. 22 GDPR) You have the right not to be subject to a decision based solely on automated processing with significant effects. Our automated moderation (rate limits, plausibility checks, the shadowban based on contribution_score) is NOT solely automated; the final decision on sanctions such as a shadowban is reviewed by a human, and in any event you have the right to a Statement of Reasons (DSA Art. 17) and to file an internal complaint (DSA Art. 20).

Right to withdraw consent (Art. 7(3) GDPR) Where processing is based on consent (marketing push notifications), you may withdraw consent at any time in the App or OS settings.

Right to lodge a complaint with a supervisory authority (Art. 77 GDPR) In the Czech Republic: the Office for Personal Data Protection (ÚOOÚ), Pplk. Sochora 27, 170 00 Prague 7, https://www.uoou.gov.cz. In other EU Member States: the supervisory authority of your country of habitual residence.

Response timeframes: We will handle requests without undue delay, at the latest within one (1) month. The period may be extended by a further two months. Handling is free of charge; for manifestly unfounded requests, a reasonable fee or refusal.

Identity verification: To protect your rights, we reserve the right to verify your identity before handling a request (typically by email from the address associated with the Account).

9. CONSENTS IN THE APP AND ONBOARDING

On the first launch of the App, we display an initial consent screen (the "GDPR consent screen"). In the current version 3 of this Policy:

- Consent to the processing of personal data (BLOCKING): This consent reflects that by accepting the Terms you use the App and agree to the processing of the personal data necessary for the performance of the contract (Art. 6(1)(b) GDPR). The App cannot be used without this consent.
- Consent to the collection of analytical data (NON-BLOCKING, opt-out at any time): Analytics (PostHog) is primarily processed on the basis of legitimate interest (Art. 6(1)(f) GDPR). The consent on the consent screen has an informational character and gives you the option of an initial opt-out. You may switch analytics off at any later time in Profile, Privacy, Analytics.

Change from previous versions of this Policy: Previous versions conditioned the use of the App on consent to analytics as a blocking checkbox. Following review, we removed this conditionality in line with Art. 7(4) GDPR and EDPB Guidelines 5/2020; consent to analytics cannot be a valid condition for using a service that does not need analytics to function.

10. COOKIES AND SIMILAR TECHNOLOGIES

10.1. In the mobile App: The App does not use standard web cookies. Instead:

- Local MMKV device storage: for preference settings, the install_id, authentication tokens (stored encrypted), feature flags, cached data
- Key classification (lib/dataLifecycle.ts): DEVICE_LEVEL_KEYS (survive logout: install_id, language, currency, push_token) vs USER_LEVEL_KEYS (deleted on logout: cache, preferences)
- The install_id generated by the App: for identifying the installation in analytics; it is NOT the system IDFA (Apple) or AAID (Google)
- The Expo Push Token: for delivering push notifications

10.2. On the phmarket.cz website: If you visit our website (e.g. phmarket.cz/delete-account), we may use necessary technical cookies per the Cookies Policy on the website.

11. PERSONAL DATA SECURITY

11.1. Technical and organizational measures:

- Encryption in transit: TLS 1.3 for all communication with servers; HSTS on the website
- Encryption at rest: AES-256 for sensitive data in the Supabase database; bcrypt for password hashing

- PusHMe encryption: XOR with a SHA-256 derived key (from phmarket:radio:v1:Frequency); the server does not see the content in normal operation, but NOTE: in the case of the PLAIN: fallback (failure of the crypto API on the device) the message is stored in plaintext for the 30-minute retention
- Pseudonymization of identifiers in analytical data
- The least privilege principle for data access; Row-Level Security (RLS) in Supabase
- Regular security updates and infrastructure patching
- Automated backups with regular recoverability testing
- Logging of security events and their monitoring (Sentry, Supabase audit logs)
- Penetration testing, code review of new code
- Information security policies and employee training
- Server-side validation of all RPC calls: rate limits, plausibility checks (±50 % of the price median), geofence (25 to 50 km), duplicate detection (50 m)

11.2. Notification of a security breach: In the event of a breach likely to result in a high risk to your rights, we will notify you without undue delay under Art. 34 GDPR. We also report serious breaches to the ÚOOÚ within 72 hours under Art. 33 GDPR.

11.3. Recommendations for you: Use a strong and unique password; protect access to your email; do not share login credentials; promptly report any suspected unauthorized access to support@phmarket.cz.

12. CHILDREN AND PROTECTION OF MINORS

12.1. Age restriction: The App is not intended for children under seventeen (17) years of age. The Mature 17+ rating on Google Play and the 18+ category on the Apple App Store (under Apple's age rating system effective from 2026, which replaced the previous 17+ category) relate to the PusHMe feature (communication with unknown persons).

12.2. User warranty: By using the App, you represent that you have reached at least 17 years of age.

12.3. CSAE / CSAM: The App maintains absolute zero tolerance for child sexual abuse material (CSAM/CSAE). Detection takes place via hash matching (PhotoDNA/Microsoft / IWF hash lists), report buttons in PusHMe and community contributions, and automated heuristics. Upon detection, the content is immediately removed, the User permanently banned, NCMEC is notified via the IWF and law enforcement authorities are informed under Regulation (EU) 2021/1232. Contact: csae@phmarket.cz.

13. CHANGES TO THIS POLICY

We may update this Policy from time to time. We will inform you of material changes with reasonable advance notice (at least 30 days before effectiveness) in the App, by push notification or by email. The current version is always available in the App and at phmarket.cz/privacy-policy.

14. PLATFORM-SPECIFIC INFORMATION FOR APPLE (iOS)

14.1. Privacy Manifests (PrivacyInfo.xcprivacy): The App contains a Privacy Manifest in accordance with the Apple App Store Privacy requirements (effective May 2024). Third-party SDKs (PostHog 3.x+, Sentry 8.x+) also contain their own Privacy Manifests.

14.2. App Tracking Transparency (ATT): The Controller does not engage in tracking within the meaning of the Apple ATT framework; no cross-app tracking or sharing with data brokers. The App therefore does not show the ATT prompt.

14.3. Sign in with Apple: When signing in via Sign in with Apple, you may use "Hide My Email" (an Apple relay email). Upon Account deletion, we call the Apple Sign In REST API revokeToken endpoint and revoke your tokens with Apple. This implementation is published in the code-side change tracking document.

14.4. Family Sharing: If you share the App via Family Sharing, each family member creates their own Account with their own data.

15. PLATFORM-SPECIFIC INFORMATION FOR GOOGLE (Android)

15.1. Data Safety form: We have completed the Data Safety form in the Google Play Console in accordance with the Google User Data Policy. It describes in detail the types of processed data, the purposes and sharing with third parties.

15.2. Account deletion web resource: In accordance with the Google Play User Data Policy, account deletion may also be initiated via phmarket.cz/delete-account, without installing the App.

15.3. Sign in with Google: We receive from Google only your name and email address from your Google profile.

15.4. Play Integrity API: For abuse prevention purposes we use (or will use) the Google Play Integrity API. The verdict contains signals about the integrity of the device and the app; we store it only in anonymized form for fraud detection (the integrity_checks table, read/written only by the service_role).

16. HOW TO CONTACT US

For any inquiries, requests or complaints regarding personal data protection:

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Czech Republic

Company ID: 04529031 | Data box: 234baq7

Personal data protection: privacy@phmarket.cz

General support: support@phmarket.cz

Legal matters / DSA contact point: legal@phmarket.cz

DSA notice-and-action: notice@phmarket.cz

Child safety (CSAE): csae@phmarket.cz

Website: https://www.phmarket.cz

Account deletion (web): https://www.phmarket.cz/delete-account

Supervisory authority CZ: Office for Personal Data Protection (ÚOOÚ), Pplk. Sochora 27, 170 00 Prague 7, Czech Republic, https://www.uoou.gov.cz, phone: +420 234 665 111

This Privacy Policy becomes effective on 1 June 2026 and supersedes all previous versions.