ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ

MOBILNÍ APLIKACE PHMARKET

Účinnost od: 1. června 2026

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Česká republika

IČO: 04529031 | DIČ: CZ04529031 | Datová schránka: 234baq7

1. ÚVOD A KONTAKT NA SPRÁVCE

Tyto Zásady ochrany osobních údajů (dále jen "Zásady") popisují, jakým způsobem obchodní společnost PHMarket s.r.o., IČO: 04529031, se sídlem Hlavní třída 87/2, 737 01 Český Těšín, Česká republika, zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě, oddíl C, vložka 64228 (dále jen "PHMarket", "Správce", "my" nebo "naše"), zpracovává osobní údaje uživatelů mobilní aplikace PHMarket (bundle identifier cz.phmarket.app, dále jen "Aplikace").

Tyto Zásady jsou nedílnou součástí Všeobecných obchodních podmínek (dále jen "Podmínky") a vykládají se s nimi v souvislosti. Termíny psané s velkým počátečním písmenem, které zde nejsou definovány, mají význam stanovený v Podmínkách.

Zpracování probíhá v souladu s Nařízením (EU) 2016/679 ("GDPR"), zákonem č. 110/2019 Sb., o zpracování osobních údajů, zákonem č. 480/2004 Sb., o některých službách informační společnosti, Nařízením (EU) 2022/2065 (DSA) a dalšími platnými předpisy.

Kontaktní údaje Správce:

PHMarket s.r.o., Hlavní třída 87/2, 737 01 Český Těšín, Česká republika

IČO: 04529031 | DIČ: CZ04529031 | Datová schránka: 234baq7

Ochrana osobních údajů: privacy@phmarket.cz

Obecná podpora: support@phmarket.cz

Webové stránky: https://www.phmarket.cz

Vzhledem k charakteru a rozsahu zpracování nemá Správce povinnost jmenovat pověřence pro ochranu osobních údajů (DPO) dle čl. 37 GDPR. Veškerá komunikace ve věcech ochrany osobních údajů probíhá prostřednictvím dedikované adresy privacy@phmarket.cz.

2. ROZSAH PŮSOBNOSTI A KLÍČOVÉ KONCEPTY

2.1. Geografická působnost: Aplikace je primárně určena uživatelům z členských států EU, Spojeného království, Norska, Islandu, Lichtenštejnska a Švýcarska. Při užívání z jiné jurisdikce probíhá zpracování v souladu s GDPR.

2.2. Subjekt údajů: Vy jako fyzická osoba, která stáhne, instaluje, vytvoří Účet nebo Aplikaci jakkoli užívá, ať v režimu "Užívání bez registrace" nebo jako Registrovaný uživatel.

2.3. Klíčový rozdíl mezi režimy:

- Užívání bez registrace: Aplikace funguje bez vytvoření Účtu, k dispozici jsou základní funkce (mapa, ceny, navigace, Quality stanice, Fuel Quality v read-only). Zpracované údaje jsou omezeny na technické identifikátory zařízení (install_id, UUID generovaný Aplikací), preferenční nastavení (jazyk, měna) a pseudonymizovaná analytická data. NENÍ to anonymní Supabase účet, formální uživatelský účet v naší databázi (auth.users) je vytvořen až při registraci.
- Registrovaný Účet: Plnohodnotný účet zahrnující jméno/přezdívku, e-mail a další údaje nezbytné pro účast v Programu PHM Cash, službu PusHMe, Komunitní hlášení cen, vytváření Komunitních stanic, hodnocení Fuel Quality a uplatnění Flash Offer.

3. KATEGORIE ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ

Správce shromažďuje a zpracovává následující kategorie osobních údajů, vždy v rozsahu nezbytném pro konkrétní účel a v souladu se zásadou minimalizace podle čl. 5 odst. 1 písm. c) GDPR:

3.1. Identifikační a kontaktní údaje (jen Registrovaný Účet)

- Jméno nebo přezdívka (skutečné občanské jméno není vyžadováno; uloženo v user_metadata.nickname nebo user_metadata.first_name)
- E-mailová adresa (může být tzv. "relay" e-mail z Apple Hide My Email, pokud se přihlašujete přes Sign in with Apple, Vaši skutečnou adresu pak nedostáváme)
- Apple ID nebo Google ID (pouze interní identifikátor poskytnutý OAuth procesem, nikoli heslo k Apple/Google účtu)
- Heslo (uložené v hashované podobě pomocí bcrypt s solí v Supabase Auth, nikdy v plaintextu), pouze pokud se registrujete e-mailem

3.2. Technické a identifikační údaje zařízení

- install_id: Unikátní identifikátor instalace Aplikace generovaný při prvním spuštění a uložený lokálně (MMKV). Není to systémový identifikátor (IDFA na iOS / AAID na Androidu), nelze ho použít k cross-app trackingu.
- Typ a model mobilního zařízení (např. iPhone 15, Samsung Galaxy S24), shromažďováno přes expo-device
- Značka výrobce zařízení (Apple, Samsung atd.)
- Verze operačního systému (iOS 18, Android 14 atd.)
- Verze Aplikace (app_version z expo-application)
- IP adresa (anonymizovaná, uchováváme pouze první tři oktety, např. 192.168.1.* místo 192.168.1.45, výhradně pro hrubou geografickou analýzu)
- Jazykové nastavení a časové pásmo (locale, timezone), z expo-localization
- Push notifikační token (Expo Push Token, služba Expo Push Service, která ho dále směruje na Apple APNs nebo Google FCM)

3.3. Lokalizační údaje

Aplikace pracuje s informací o Vaší aktuální poloze pro zobrazení blízkých Partnerských stanic, výpočet vzdálenosti, navigaci, detekci země pro Fuel Quality a snap-to-station mechanismus při hlášení cen. Zpracování probíhá takto:

Foreground-only tracking: Aplikace získává Vaši polohu výhradně, pokud je v popředí (foreground). NEsledujeme polohu na pozadí. Při zavření aplikace nebo přepnutí do pozadí GPS subscription končí (na úrovni iOS/Android OS). Pro získání polohy používáme pouze foreground permission (Location.requestForegroundPermissionsAsync v expo-location).

Přesnost polohy: Používáme jednotnou úroveň přesnosti Location.Accuracy.Balanced (přibližně ~100 metrů). Nevyužíváme nejvyšší přesnost (High accuracy ~5 až 20 metrů), protože pro funkci aplikace stačí balanced.

Kontinuální sledování v popředí: Po udělení souhlasu se OS volá watchPositionAsync se 30sekundovým intervalem a 50metrovým prahem; v naší aplikaci ukládáme nový stav jen, pokud uživatel ujel více než 100 metrů nebo uplynul určitý čas. Poloha tedy není ukládána na serveru ani lokálně každých 30 sekund, ukládá se pouze pro aktuální session aplikace.

Persistence polohy: Vaše GPS souřadnice neukládáme trvale na servery, s výjimkou případů, kdy jsou součástí konkrétního záznamu (např. tankování v Programu PHM Cash, komunitní hlášení ceny, vytvoření Komunitní stanice). V těchto případech ukládáme pouze souřadnice spojené s daným záznamem, nikoli historickou stopu pohybu.

Detekovaná země (cache): Pro funkci Fuel Quality detekujeme zemi (CZ/PL/SK/DE/AT/HU) na základě poslední polohy a tento kód země ukládáme lokálně v MMKV (fq_detected_country). Slouží k automatické inicializaci sekce Fuel Quality při dalším otevření, nikoli k profilování.

Snap-to-station: Při hlášení ceny paliva (Komunitní hlášení) Aplikace volá funkci find_nearest_station(GPS), která Vaši polohu "přichytí" k nejbližší Katalogové stanici v okruhu 25 km. To je ANTI-SABOTAGE opatření, nelze hlásit cenu pro libovolnou GPS souřadnici, pouze pro existující stanici. Vaše GPS v okamžiku hlášení pak nezůstává uložena jako součást ceny; ukládá se pouze fuel_station_id.

Odvolání souhlasu s polohou: Můžete kdykoli odvolat v nastavení iOS/Android. Aplikace funguje i bez polohy, pouze nemůže řadit stanice podle vzdálenosti, navigovat ani snap-tovat ceny. Místo aktuální polohy se použije "poslední známá poloha" cachovaná v OS, případně se uživatel vyzve k zadání cíle textově.

3.4. Údaje o vozidle a profilu řidiče

- Typ paliva (Natural 95, Diesel, LPG, CNG, AdBlue, HVO, EV)
- Spotřeba paliva (l/100 km nebo kWh/100 km)
- Kapacita nádrže nebo baterie (u EV)
- Druh vozidla (osobní, lehký užitkový, kamion atd.)
- Preferovaná měna pro zobrazení cen (CZK, EUR, PLN, HUF, USD)
- Preferovaná jednotka vzdálenosti (kilometry / míle)
- Preferovaná navigační aplikace (Apple Maps, Google Maps, Waze, Mapy.cz)

Vehicle profile je uložen jak lokálně (cache v MMKV pod klíčem vehicle_cache pro stale-while-revalidate vzor), tak na serveru v user_metadata pro synchronizaci mezi zařízeními.

Profilová fotografie (zpracování výhradně v zařízení): Pokud si nastavíte profilovou fotografii, Aplikace ji zmenší na 200 x 200 pixelů a uloží výhradně lokálně do úložiště Vašeho zařízení (documentDirectory). Profilová fotografie NIKDY není odesílána na servery Provozovatele ani třetích stran a není součástí žádného přenosu dat. Odstraníte ji v profilu Aplikace nebo odinstalováním Aplikace. Oprávnění k fotogalerii (photo library) je vyžadováno pouze v okamžiku výběru fotografie a slouží výlučně k tomuto účelu.

3.5. Údaje o aktivitě v Aplikaci

- Historie navštívených Partnerských stanic v Aplikaci (otevření detailu stanice)

- Historie tankování zaevidovaného v Programu PHM Cash (datum, čas, Partnerská stanice, typ paliva, množství, cena, GPS v okamžiku tankování pro verifikaci)
- Komunitní hlášení cen, cena, fuel_station_id, typ paliva, časová známka, source_currency, valuta, fx kurz
- Vytvořené Komunitní stanice, název, adresa, město, GPS souřadnice, creator_display (zkrácené jméno z user_metadata.display_name nebo prefix e-mailu)
- Fuel Quality hodnocení, fuel_station_id, is_positive (boolean), volitelný komentář (max 200 znaků), volitelný brand_suggestion (návrh značky stanice)
- Recenze a hodnocení Partnerských stanic
- Sledované Partnerské stanice ("oblíbené")
- Trasy a navigační dotazy (uchovávány pouze dočasně pro výpočet, recent_destinations_v1 cache FIFO max 8 položek lokálně)
- Easter egg progress (ee_station_detail_count, ee_app_open_count, ee_radio_unlocked, radio_cooldown_sent_at), lokální čítače pro odemčení PusHMe

3.6. Údaje o Programu PHM Cash

Pozn.: Program PHM Cash je k datu účinnosti těchto Zásad v přípravě (coming soon). Níže uvedené kategorie údajů budou zpracovávány od okamžiku spuštění Programu.

- Stav Bodů PHM Cash a aktuální Level
- Historie získání a směny Bodů (transactions log)
- Referral identifikátor (pokud jste byl pozván jiným uživatelem)
- Bankovní spojení, IBAN a jméno majitele účtu (pouze pokud žádáte o roční výplatu peněžní odměny; ukládáno pouze v okamžiku uplatnění výplaty, nikoli automaticky)
- Contribution score (interní reputační skóre v rozsahu typicky -10 až +∞), používané pro automatizovanou moderaci (viz článek 4.4 níže, shadowban a transparentní moderace)

3.7. Údaje ze služby PusHMe

PusHMe je systém šifrovaných krátkých zpráv na uživatelsky definovaných Frekvencích (1000 až 9999). Šifrování probíhá v zařízení odesílatele před odesláním na server. Detaily zpracování:

Klíč šifry: Klíč je odvozen funkcí SHA-256 z řetězce 'phmarket:radio:v1:' + Frekvence (např. 'phmarket:radio:v1:4242'). Není to triviální XOR s číselnou Frekvencí jako klíčem, ale XOR s 256bitovým hash-derived klíčem. Server PHMarket nemá v běžném provozu možnost přečíst obsah zpráv bez znalosti Frekvence.

PLAIN: fallback (důležité): Pokud na zařízení uživatele selže kryptografické API (Crypto.digestStringAsync), zpravidla na velmi starých zařízeních, Aplikace má bezpečnostní záchytný režim, ve kterém uloží zprávu s prefixem "PLAIN:" v plaintextu. V tomto případě je obsah zprávy čitelný i bez znalosti Frekvence, a to po dobu 30minutového retention period. Pravděpodobnost vzniku tohoto stavu je v praxi nízká (cca <0,5 % zařízení), ale zveřejňujeme ji pro úplnou transparentnost.

- Metadata zprávy (uloženo na serveru): čas odeslání, anonymizovaný identifikátor odesílatele (UUID auth.users.id, nikoli e-mail/jméno), Frekvence (číselný kanál 1000 až 9999), volitelně station_id (kontext stanice)
- Šifrovaný obsah zprávy: uchováván na serveru maximálně 30 minut (expires_at default now() + 30 min); poté automaticky a nevratně mazán cron jobem
- Systémové kanály (101 Live drops, 111 Kafe & jídlo, 121 Péče o auto, 131 Speciál): zprávy v systémových kanálech jsou PLAINTEXT (is_system=true) a jsou vysílány Provozovatelem nebo jím autorizovanými partnery. Plní funkci marketing-light kanálu; zasílání marketingových obchodních sdělení v systémových kanálech podléhá souhlasu dle § 7 zákona č. 480/2004 Sb. (souhlas s push notifikacemi v Profil → Notifikace)
- Seznam Vašich oblíbených Frekvencí (radio_listening, max 5), uloženo v profiles tabulce na serveru
- Seznam blokovaných uživatelů na jednotlivých Frekvencích, uloženo lokálně
- Hlášení zpráv (radio_reports tabulka): pokud nahlásíte zprávu, k tomuto hlášení uchováváme šifrovaný obsah, identifikátor odesílatele, kategorii hlášení (illegal / harassment / spam / other), čas a Vaše ID nahlašujícího; uchováváme po dobu 30 dnů od dokončení posouzení nebo 1 rok pro účely případného sporu

3.8. Analytická a diagnostická data

PostHog (produktová analytika): Pro pochopení používání Aplikace využíváme PostHog, Inc. v EU instanci (host: https://eu.i.posthog.com). Sbíráme pseudonymizované analytické události: screen views, kliky, navigační akce, úspěch/selhání operací, easter egg progress, performance metrics. Identifikátor distinct_id v PostHog je při Užívání bez registrace install_id (anonymní per-instalace) a při Registrovaném Účtu Vaše Supabase user_id. To je tedy PSEUDONYMIZACE, ne plná anonymizace, uživatel je identifikován konzistentně přes jednotlivé sessions, ale identifikátor nelze samostatně dohledat zpět k Vaší osobě bez doplňkového údaje (e-mail / jméno) z naší databáze. Při odhlášení voláme posthog.reset(), nový session získá novou identitu.

Sentry (diagnostika chyb a pádů): Pro detekci a opravy bugů využíváme Sentry (Functional Software, Inc.) v US infrastruktuře s SCCs. Sentry zachycuje JavaScript chyby, native crashes, stack traces, breadcrumbs (zachycené trackEvent události forwardované do Sentry), device context (model, OS) a pseudonymizovaný identifikátor uživatele. Sentry retention 90 dnů.

- Kontext připojený automaticky k analytickým událostem: session_id, install_id, device_model, device_brand, os_version, timezone, locale, app_version, app_start_type (cold/warm), push_permission_status
- Konkrétní eventy: 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 a další technické události

- Geografická agregace pro statistiky: vaše GPS souřadnice se v analytických agregacích zaokrouhlují na ~10 km bloky (lat_bucket, lng_bucket) pro identifikaci geografických trendů, nikoli pro identifikaci konkrétního místa

3.9. Údaje z komunikace s podporou

- Obsah Vaší zprávy zaslané na podporu (support@phmarket.cz, privacy@phmarket.cz, legal@phmarket.cz, notice@phmarket.cz, csae@phmarket.cz)
- Naše odpovědi a jakákoli další komunikace
- Metadata komunikace (čas, e-mailová adresa, předmět)

4. ÚČELY ZPRACOVÁNÍ A PRÁVNÍ ZÁKLADY

Správce zpracovává Vaše osobní údaje pouze pro určité, výslovně vyjádřené a legitimní účely, na základě konkrétního právního základu podle čl. 6 odst. 1 GDPR. Detailní přehled:

4.1. Poskytování základních funkcí Aplikace (mapa, ceny paliv, navigace, Quality stanice, Fuel Quality v read-only) Uživatelům bez registrace i Registrovaným Uživatelům

Právní základ: Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR), tj. plnění Podmínek, které jsou smlouvou

Zpracovávané údaje: Technické údaje zařízení, lokalizační údaje (foreground only), preferenční nastavení

Doba uchování: Po dobu užívání Aplikace; preferenční nastavení po dobu existence Účtu nebo do odinstalace

4.2. Správa Registrovaného Účtu, autentifikace, obnovení hesla

Právní základ: Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR)

Zpracovávané údaje: Jméno/přezdívka, e-mail, hashované heslo, Apple/Google OAuth identifikátor

Doba uchování: Po dobu existence Účtu + 90 dnů po smazání pro rotaci záloh

4.3. Účast v Programu PHM Cash (přidělování Bodů, evidence tankování, výplaty); Aktivní od spuštění Programu, aktuálně coming soon

Právní základ: Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR); plnění právní povinnosti dle zákona o účetnictví a daňových zákonů (čl. 6 odst. 1 písm. c) GDPR) pro účetní účely

Zpracovávané údaje: Identifikační údaje, údaje o tankování, level, body, bankovní spojení (IBAN, jméno majitele), IBAN pouze při uplatnění výplaty

Doba uchování: Po dobu účasti v Programu; účetní doklady 10 let dle zákona č. 563/1991 Sb.

4.4. Služba PusHMe, odesílání a doručování šifrovaných zpráv mezi uživateli, moderace obsahu, prevence zneužití

Právní základ: Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR); oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR) pro moderaci a prevenci zneužití

Zpracovávané údaje: Metadata zprávy, šifrovaný obsah (nebo PLAIN: fallback), identifikátor odesílatele, blokovaní uživatelé, hlášení

Doba uchování: Šifrovaný/plaintext obsah max 30 minut; metadata max 90 dnů; hlášení do skončení posouzení + 1 rok

4.5. Komunitní hlášení cen, vytváření Komunitních stanic, recenze, hodnocení Partnerských stanic

Právní základ: Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR); oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR), provoz Aplikace a zkvalitnění informací; antifraud audit (prices_audit)

Zpracovávané údaje: Identifikátor uživatele, creator_display, obsah hlášení/stanice, časová známka, GPS pro snap-to-station verifikaci (neukládáme dlouhodobě), antifraud rate_limit_block záznamy

Doba uchování: Příspěvky: po dobu existence Účtu nebo do vymazání jednotlivého obsahu; antifraud audit: 3 roky

4.6. Hodnocení Fuel Quality, recenze (pozitivní / s výhradami), brand suggestions

Právní základ: Plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR) a oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR), informovanost spotřebitelů o kvalitě paliv

Zpracovávané údaje: fuel_station_id, is_positive, volitelný komentář (max 200 znaků), volitelný brand_suggestion, identifikátor uživatele, čas

Doba uchování: Po dobu existence Účtu nebo do vymazání jednotlivého hodnocení

4.7. Zveřejnění pokut udělených Českou obchodní inspekcí (ČOI) v sekci Fuel Quality

Právní základ: Oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR), informovanost spotřebitelů o veřejně dostupných údajích o kvalitě paliv; data pocházejí z veřejně publikovaných rozhodnutí ČOI

Zpracovávané údaje: Název stanice, město, rok pokuty, důvod, URL na zdrojový dokument ČOI

Doba uchování: Po dobu, kdy jsou data relevantní (aktivní pokuta) + 3 roky

4.8. Servisní push notifikace (změny Účtu, Body PHM Cash, moderace obsahu, Statement of Reasons)

Právní základ: Plnění smlouvy a oprávněný zájem (čl. 6 odst. 1 písm. b) a f) GDPR)

Zpracovávané údaje: Expo Push Token, údaje o událostech v Účtu

Doba uchování: Po dobu užívání Aplikace

4.9. Marketingové push notifikace, novinky, Flash Offers v PusHMe (aktuálně neaktivní; budou aktivovány v budoucích verzích)

Právní základ: Souhlas (čl. 6 odst. 1 písm. a) GDPR), udělený prostřednictvím opt-in dialogu v Profil → Notifikace

Zpracovávané údaje: Expo Push Token, preference (notif_nearby, notif_discount, notif_loyalty, notif_quality, notif_location)

Doba uchování: Do odvolání souhlasu

4.10. Produktová analytika (PostHog), zlepšování UX, prevence chyb, A/B testing

Právní základ: Oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR). Toto je důležitá změna oproti dřívějším verzím těchto Zásad, analytika byla původně podmíněna samostatným souhlasem v GDPR consent screenu; tato podmíněnost byla po revizi vyhodnocena jako neslučitelná s čl. 7 odst. 4 GDPR a

doporučeními EDPB 5/2020 (consent bundling). Nyní analytika probíhá na základě oprávněného zájmu s pseudonymizací, EU hostingem a snadným opt-outem v Profil → Soukromí.

Zpracovávané údaje: Pseudonymizované analytické události, install_id (před registrací), Supabase user_id (po registraci); device kontext (model, OS, locale)

Doba uchování: PostHog: 12 měsíců; agregované anonymní statistiky: neomezeně

4.11. Diagnostika chyb a pádů (Sentry)

Právní základ: Oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR)

Zpracovávané údaje: Stack trace, breadcrumbs, pseudonymizovaný identifikátor zařízení, verze OS/ aplikace, device kontext

Doba uchování: 90 dnů (Sentry retention)

4.12. Prevence podvodů, zneužití Programu PHM Cash, PusHMe, Flash Offers; automatizovaná moderace včetně shadowban systému (transparentně, dle DSA čl. 17)

Právní základ: Oprávněný zájem (čl. 6 odst. 1 písm. f) GDPR); plnění právní povinnosti dle DSA

Zpracovávané údaje: Údaje o aktivitě, contribution_score, IP adresa (anonymizovaná), zařízení, prices_audit záznamy

Doba uchování: Po dobu vyšetřování + 3 roky pro účely případného sporu

4.13. Plnění povinností podle DSA (notice-and-action, statement of reasons, interní stížnosti, transparency reporting)

Právní základ: Plnění právní povinnosti (čl. 6 odst. 1 písm. c) GDPR), Nařízení (EU) 2022/2065

Zpracovávané údaje: Údaje o hlášeních, rozhodnutích moderace, odvoláních, transparency reports

Doba uchování: 5 let od ukončení posouzení

4.14. Komunikace s podporou a řešení stížností

Právní základ: Plnění smlouvy a oprávněný zájem (čl. 6 odst. 1 písm. b) a f) GDPR)

Zpracovávané údaje: Obsah komunikace, e-mailová adresa, metadata

Doba uchování: 3 roky od posledního kontaktu

4.15. Plnění právních povinností (účetnictví, daně, AML, žádosti orgánů veřejné moci)

Právní základ: Plnění právní povinnosti (čl. 6 odst. 1 písm. c) GDPR)

Zpracovávané údaje: Účetní a daňové údaje vč. bankovních spojení pro výplaty PHM Cash, údaje pro plnění žádostí

Doba uchování: 5 až 10 let dle zákona o účetnictví a daňových zákonů

5. DOBA UCHOVÁNÍ ÚDAJŮ

5.1. Obecný princip: Údaje uchováváme jen po dobu nezbytně nutnou ke splnění příslušného účelu zpracování a v souladu s minimalizací zpracování. Po uplynutí doby uchování jsou údaje nevratně smazány nebo anonymizovány.

5.2. Smazání Účtu: V případě smazání Účtu zahájíme následující proces:

- Produkční databáze: 30 dnů od potvrzení žádosti
- Zálohy: 90 dnů od potvrzení žádosti (zálohy jsou rotovány automaticky)
- Účetní doklady a údaje pro AML a daňové účely: 5 až 10 let bez ohledu na smazání Účtu
- Údaje vztahující se k probíhajícímu sporu/vyšetřování: po dobu trvání + 3 roky
- Anonymizovaná data (agregované statistiky): mohou být uchovávána neomezeně
- PostHog distinct_id: voláme posthog.reset() při logoutu, po smazání Účtu už nový session nemá vazbu na user_id, ale historické eventy v PostHog vázané na user_id zůstávají do 12měsíční retence; po žádosti o výmaz volame i PostHog Delete API

5.3. Sign in with Apple revoke (závazek): Pokud jste se přihlašoval/a přes Sign in with Apple a požádáte o smazání Účtu, Správce v rámci procesu mazání volá Apple Sign In REST API revokeToken endpoint a zruší Vaše refresh + access tokeny u Apple Inc. Tento závazek je dán požadavkem Apple App Store Review Guideline 5.1.1(v); implementační detaily jsou zveřejněny v code-side change tracking dokumentu.

6. PŘÍJEMCI ÚDAJŮ A ZPRACOVATELÉ

Vaše osobní údaje předáváme následujícím kategoriím příjemců, vždy v rozsahu nezbytném pro daný účel a na základě zpracovatelských smluv podle čl. 28 GDPR:

6.1. Zpracovatelé (Data Processors)

Supabase Inc. (USA; database hosted in Frankfurt, EU)

Role: Hosting Postgres databáze (auth.users, profiles, stations, prices, radio_broadcasts, fuel_stations atd.), autentifikace, real-time funkce pro PusHMe a community price broadcast

Právní podklad: DPA + SCCs; data uchovávána výhradně v EU regionu (Frankfurt); ISO 27001/SOC 2

PostHog, Inc. (USA; EU instance: eu.i.posthog.com)

Role: Pseudonymizovaná produktová analytika

Právní podklad: DPA; EU instance bez transferu do USA pro analytical data

Functional Software, Inc. d/b/a Sentry (USA)

Role: Diagnostika chyb a pádů Aplikace

Právní podklad: DPA + SCCs; pseudonymizace identifikátorů; krátká retence (90 dnů)

Apple Inc. (USA / Irsko pro EU operace)

Role: Doručení push notifikací (APNs); Sign in with Apple autentifikace; App Store distribuce

Právní podklad: Apple Developer Program Agreement + Apple Privacy Policy; transfer mechanismy dle EU rozhodnutí o adekvátnosti / DPF

Google LLC (USA / Irsko pro EU)

Role: Doručení push notifikací (FCM); Sign in with Google; Maps API pro mapové dlaždice; Google Play distribuce

Právní podklad: Google API Terms + DPA; SCCs / DPF

Expo (650 Industries, Inc., USA)

Role: Expo Push Service jako brokerage layer mezi Aplikací a APNs/FCM; OTA updates infrastructure

Právní podklad: Expo Privacy Policy; Expo Push Token slouží jako proxy pro APNs/FCM token; SCCs

Resend / Mailgun nebo obdobný (poskytovatel transakčních e-mailů)

Role: Doručování transakčních e-mailů (potvrzení registrace, reset hesla, smazání účtu)

Právní podklad: DPA + SCCs; minimální retence

6.2. Příjemci údajů (Data Recipients)

- Partnerské stanice: V omezeném rozsahu při uplatnění Flash Offer (claim_code, čas, station_code) nebo registraci tankování v Programu PHM Cash (pseudonymizovaný identifikátor + údaje o tankování). Partnerské stanice nedostávají Vaše jméno, e-mail ani Apple/Google ID.
- Banka Provozovatele: Pro výplatu peněžní odměny z Programu PHM Cash (IBAN, jméno majitele, částka), od spuštění Programu.
- Daňová správa: Pokud výplata přesáhne zákonem stanovené reporting limity.
- Účetní kancelář Provozovatele: V rámci běžných účetních operací.
- Právní zástupci, auditoři: Při plnění právních povinností.
- Orgány činné v trestním řízení, soudy, dozorové orgány (ÚOOÚ, ČOI, ČTÚ, DSC dalších členských států EU): Na základě řádné žádosti a v souladu s platnými předpisy.
- National Center for Missing & Exploited Children (NCMEC) prostřednictvím Internet Watch Foundation: V případě detekce CSAM/CSAE obsahu (čl. 22 Podmínek a CSAE Policy).
- Důvěryhodní oznamovatelé (trusted flaggers, DSA čl. 22): Na základě jejich oznámení a v rozsahu nezbytném pro výkon jejich oprávnění.

7. MEZINÁRODNÍ PŘENOSY OSOBNÍCH ÚDAJŮ

7.1. Princip lokalizace v EU: Naši primární datovou infrastrukturu (databáze Supabase, PusHMe servery) provozujeme výhradně v rámci Evropského hospodářského prostoru (EHP), konkrétně v Německu (Frankfurt). Zde nedochází k mezinárodním přenosům do třetích zemí ve smyslu GDPR.

7.2. Přenosy do USA a třetích zemí: Někteří zpracovatelé (Apple, Google, Expo, Sentry, Resend/ Mailgun) sídlí ve Spojených státech amerických. Pro tyto přenosy aplikujeme:

- Standard Contractual Clauses (SCCs) podle Prováděcího rozhodnutí Komise (EU) 2021/914 jako právní mechanismus dle čl. 46 odst. 2 písm. c) GDPR
- Apple a Google: certifikovány v rámci EU-U.S. Data Privacy Framework (DPF), pokud je tento mechanismus účinný; alternativně SCCs
- Dodatečná opatření (Supplementary Measures): šifrování v přenosu (TLS 1.3) a v klidu (AES-256); pseudonymizace identifikátorů; minimalizace přenášených údajů

7.3. Transfer Impact Assessment: Pro každý systematický přenos do třetí země provádíme Transfer Impact Assessment (TIA) dle doporučení EDPB.

8. VAŠE PRÁVA JAKO SUBJEKTU ÚDAJŮ

V souvislosti se zpracováním Vašich osobních údajů Vám podle GDPR náleží následující práva. Můžete je kdykoli uplatnit na privacy@phmarket.cz nebo přímo v Aplikaci (kde to konkrétní právo umožňuje):

Právo na přístup (čl. 15 GDPR)

Máte právo získat potvrzení, zda jsou Vaše údaje zpracovávány, a pokud ano, právo na přístup k údajům a informacím o zpracování. Můžete požádat o kopii údajů, kterou poskytneme zdarma (za další kopie přiměřený poplatek).

Právo na opravu (čl. 16 GDPR)

Máte právo na opravu nepřesných údajů. Většinu údajů můžete přímo upravit v Profil → Upravit profil v Aplikaci.

Právo na výmaz (čl. 17 GDPR)

Můžete požadovat vymazání svých údajů, preferovaně přes funkci "Smazat účet" v Aplikaci (Profil → Nastavení → Smazat účet), přes web phmarket.cz/smazat-ucet, nebo e-mailem na support@phmarket.cz. Výmaz může být omezen plněním právních povinností (účetnictví, AML, DSA reporting).

Právo na omezení zpracování (čl. 18 GDPR)

Můžete požadovat omezení zpracování v případech čl. 18 odst. 1 GDPR.

Právo na přenositelnost (čl. 20 GDPR)

Máte právo získat údaje, které jste poskytl/a, ve strukturovaném, běžně používaném a strojově čitelném formátu (JSON), a předat je jinému správci.

Právo vznést námitku (čl. 21 GDPR)

Máte právo kdykoli vznést námitku proti zpracování založenému na oprávněném zájmu (čl. 6 odst. 1 písm. f). To se týká zejména: produktové analytiky (PostHog), diagnostiky (Sentry), prevence podvodů, moderace, geografické agregace. Námitku můžete podat v Profil → Soukromí → Vznést námitku, nebo e-mailem na privacy@phmarket.cz. Po podání námitky zpracování zastavíme, ledaže prokážeme závažné oprávněné důvody převažující nad Vašimi zájmy. PRO ANALYTIKU PostHog: lze jednoduše opt-outnout v Profil → Soukromí → Analytika (přepínač), po jeho vypnutí se PostHog v aplikaci přestane volat (čistě klient-side gate).

Právo nebýt předmětem automatizovaného rozhodování (čl. 22 GDPR)

Máte právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování s významnými dopady. Naše automatizovaná moderace (rate limity, plausibility check, shadowban na základě contribution_score) NENÍ výhradně automatizovaná, finální rozhodnutí o sankcích typu shadowban je revidováno lidským přezkumem a v každém případě máte právo na Statement of Reasons (DSA čl. 17) a podání vnitřní stížnosti (DSA čl. 20).

Právo odvolat souhlas (čl. 7 odst. 3 GDPR)

Pokud je zpracování založeno na souhlasu (marketing push notifikace), můžete souhlas kdykoli odvolat v nastavení Aplikace nebo systému OS.

Právo podat stížnost u dozorového úřadu (čl. 77 GDPR)

V ČR: Úřad pro ochranu osobních údajů (ÚOOÚ), Pplk. Sochora 27, 170 00 Praha 7, https://www.uoou.gov.cz. V jiných členských státech EU: dozorový úřad podle Vaší země obvyklého bydliště.

Lhůty pro vyřízení: Žádosti vyřídíme bez zbytečného odkladu, nejpozději do jednoho (1) měsíce. Lhůtu lze prodloužit o další dva měsíce. Vyřízení je zdarma; u zjevně neopodstatněných žádostí přiměřený poplatek nebo odmítnutí.

Ověření identity: Pro ochranu Vašich práv si vyhrazujeme právo ověřit Vaši identitu před vyřízením žádosti (typicky e-mailem z e-mailové adresy spojené s Účtem).

9. SOUHLASY V APLIKACI A ONBOARDING

Při prvním spuštění Aplikace zobrazíme úvodní obrazovku se souhlasy ("GDPR consent screen"). V aktuální verzi v3 této Politiky:

- Souhlas se zpracováním osobních údajů (BLOKUJÍCÍ): Tento souhlas reflektuje, že přijetím Podmínek užíváte Aplikaci a souhlasíte se zpracováním nezbytných osobních údajů pro plnění smlouvy (čl. 6 odst. 1 písm. b) GDPR). Bez tohoto souhlasu nelze Aplikaci užívat.
- Souhlas se sběrem analytických dat (NEBLOKUJÍCÍ, opt-out kdykoli): Analytika (PostHog) je primárně zpracovávána na základě oprávněného zájmu (čl. 6 odst. 1 písm. f) GDPR). Souhlas v consent screenu má informační charakter a poskytuje Vám možnost prvotního opt-outu. Kdykoli později můžete analytiku vypnout v Profil → Soukromí → Analytika.

Změna oproti předchozím verzím těchto Zásad: Předchozí verze podmiňovaly užívání Aplikace souhlasem s analytikou jako blokujícím checkboxem. Po revizi jsme tuto podmíněnost odstranili v souladu s čl. 7 odst. 4 GDPR a doporučeními EDPB 5/2020, souhlas s analytikou nemůže být platnou podmínkou užívání služby, která analytiku nepotřebuje pro své fungování.

10. COOKIES A PODOBNÉ TECHNOLOGIE

10.1. V mobilní Aplikaci: Aplikace nepoužívá standardní webové cookies. Místo toho:

- Lokální MMKV úložiště zařízení: pro preferenční nastavení, install_id, autentifikační tokeny (uložené šifrovaně), feature flags, cached data
- Klasifikace klíčů (lib/dataLifecycle.ts): DEVICE_LEVEL_KEYS (přežívají logout, install_id, jazyk, měna, push_token) vs USER_LEVEL_KEYS (mazány při logoutu, cache, preferences)
- install_id generované Aplikací: pro identifikaci instalace v analytics; NENÍ to systémový IDFA (Apple) ani AAID (Google)
- Expo Push Token: pro doručování push notifikací

10.2. Na webových stránkách phmarket.cz: Pokud navštívíte naše webové stránky (např. phmarket.cz/smazat-ucet), můžeme využívat nezbytné technické cookies dle Cookies Policy na webu.

11. BEZPEČNOST OSOBNÍCH ÚDAJŮ

11.1. Technická a organizační opatření:

- Šifrování v přenosu: TLS 1.3 pro veškerou komunikaci s servery; HSTS na webu
- Šifrování v klidu: AES-256 pro citlivé údaje v Supabase databázi; bcrypt pro hashování hesel
- PusHMe šifrování: XOR s SHA-256 derived klíčem (z phmarket:radio:v1:Frekvence); server nevidí obsah v běžném provozu, ale POZOR, v případě fallbacku PLAIN: (selhání crypto API na zařízení) je zpráva uložena v plaintextu po dobu 30minutového retention
- Pseudonymizace identifikátorů v analytických datech
- Princip minimálních oprávnění (least privilege) pro přístup k údajům, Row-Level Security (RLS) v Supabase
- Pravidelné bezpečnostní aktualizace a patchování infrastruktury
- Automatizované zálohování s pravidelným testováním obnovitelnosti
- Logování bezpečnostních událostí a jejich monitoring (Sentry, Supabase audit logs)
- Penetrační testování, code review nového kódu
- Politiky bezpečnosti informací a školení zaměstnanců
- Server-side validace všech RPC volání: rate limity, plausibility check (±50 % mediánu cen), geofence (25 až 50 km), duplicate detection (50 m)

11.2. Oznámení porušení zabezpečení: V případě porušení s vysokým rizikem pro Vaše práva Vás bez zbytečného odkladu uvědomíme dle čl. 34 GDPR. Závažná porušení rovněž ohlašujeme ÚOOÚ ve lhůtě 72 hodin dle čl. 33 GDPR.

11.3. Doporučení pro Vás: Používejte silné a jedinečné heslo; chraňte přístup ke svému e-mailu; nesdílejte přihlašovací údaje; neprodleně oznamte podezření na neoprávněný přístup na support@phmarket.cz.

12. DĚTI A OCHRANA NEZLETILÝCH

12.1. Věkové omezení: Aplikace není určena dětem mladším sedmnácti (17) let. Hodnocení Mature 17+ na Google Play a kategorie 18+ na Apple App Store (podle systému věkového hodnocení Apple platného od roku 2026, který nahradil dřívější kategorii 17+) souvisí s funkcí PusHMe (komunikace s neznámými osobami).

12.2. Záruka uživatele: Užíváním Aplikace prohlašujete, že jste dosáhl/a věku nejméně 17 let.

12.3. CSAE / CSAM: Aplikace uplatňuje absolutní nulovou toleranci k materiálu sexuálního zneužívání dětí (CSAM/CSAE). Detekce probíhá hash-matching (PhotoDNA/Microsoft / IWF hash lists), report tlačítka v PusHMe a komunitních příspěvcích, automatizované heuristiky. Při detekci probíhá okamžité odstranění obsahu, trvalé zablokování Uživatele, reporting NCMEC prostřednictvím IWF a oznámení orgánům činným v trestním řízení dle nařízení (EU) 2021/1232. Kontakt: csae@phmarket.cz.

13. ZMĚNY ZÁSAD

Tyto Zásady můžeme čas od času aktualizovat. O podstatných změnách Vás informujeme s přiměřeným předstihem (nejméně 30 dnů před účinností) v Aplikaci, push notifikací nebo e-mailem. Aktuální verze je vždy dostupná v Aplikaci a na phmarket.cz/privacy-policy.

14. SPECIFICKÉ INFORMACE PRO PLATFORMU APPLE (iOS)

14.1. Privacy Manifests (PrivacyInfo.xcprivacy): Aplikace obsahuje Privacy Manifest dle Apple App Store Privacy requirements (od května 2024). SDK třetích stran (PostHog 3.x+, Sentry 8.x+) rovněž obsahují vlastní Privacy Manifests.

14.2. App Tracking Transparency (ATT): Správce neprovádí tracking ve smyslu Apple ATT framework, žádný cross-app tracking ani sdílení s data brokery. Aplikace tedy nezobrazuje ATT prompt.

14.3. Sign in with Apple: Při přihlášení přes Sign in with Apple můžete využít "Hide My Email" (Apple relay email). Při smazání Účtu voláme Apple Sign In REST API revokeToken endpoint a zrušíme tokeny u Apple. Tato implementace je zveřejněna v code-side change tracking dokumentu.

14.4. Family Sharing: Při sdílení Aplikace přes Family Sharing si každý člen rodiny vytváří vlastní Účet s vlastními údaji.

15. SPECIFICKÉ INFORMACE PRO PLATFORMU GOOGLE (Android)

15.1. Data Safety form: Vyplnili jsme Data Safety form v Google Play Console v souladu s Google User Data Policy. Detailně popisuje typy zpracovávaných údajů, účely a sdílení s třetími stranami.

15.2. Account deletion web resource: V souladu s Google Play User Data Policy je smazání Účtu možné iniciovat rovněž přes phmarket.cz/smazat-ucet, bez nutnosti instalace Aplikace.

15.3. Sign in with Google: Obdržíme od Google pouze jméno a e-mailovou adresu z Vašeho Google profilu.

15.4. Play Integrity API: Pro účely prevence zneužívání používáme (nebo budeme používat) Google Play Integrity API. Verdict obsahuje signály o integritě zařízení a aplikace; ukládáme jej pouze v anonymizované formě pro detekci podvodů (integrity_checks tabulka, pouze service_role čte/zapisuje).

16. JAK NÁS KONTAKTOVAT

Pro jakékoli dotazy, žádosti nebo stížnosti ve věci ochrany osobních údajů:

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Česká republika

IČO: 04529031 | Datová schránka: 234baq7

Ochrana osobních údajů: privacy@phmarket.cz

Obecná podpora: support@phmarket.cz

Právní záležitosti / DSA kontaktní bod: legal@phmarket.cz

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

Bezpečnost dětí (CSAE): csae@phmarket.cz

Webové stránky: https://www.phmarket.cz

Mazání účtu (web): https://www.phmarket.cz/smazat-ucet

Dozorový úřad ČR: Úřad pro ochranu osobních údajů (ÚOOÚ), Pplk. Sochora 27, 170 00 Praha 7, https://www.uoou.gov.cz, telefon: +420 234 665 111

Tyto Zásady ochrany osobních údajů nabývají účinnosti dne 1. června 2026 a nahrazují všechny předchozí verze.