POLITYKA PRYWATNOŚCI

APLIKACJA MOBILNA PHMARKET

Obowiązuje od: 1 czerwca 2026 r.

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Republika Czeska

IČO (nr identyfikacyjny): 04529031 | NIP UE: CZ04529031 | Skrzynka danych: 234baq7

1. WPROWADZENIE I KONTAKT Z ADMINISTRATOREM

Niniejsza Polityka prywatności ("Polityka") opisuje, w jaki sposób spółka PHMarket s.r.o., IČO: 04529031, z siedzibą pod adresem Hlavní třída 87/2, 737 01 Český Těšín, Republika Czeska, wpisana do rejestru handlowego prowadzonego przez Sąd Okręgowy w Ostrawie, dział C, wpis 64228 ("PHMarket", "Administrator", "my" lub "nasz"), przetwarza dane osobowe użytkowników aplikacji mobilnej PHMarket (bundle identifier cz.phmarket.app, "Aplikacja").

Niniejsza Polityka stanowi integralną część Ogólnych warunków świadczenia usług ("Regulamin") i należy ją interpretować łącznie z nimi. Terminy pisane wielką literą, które nie zostały tu zdefiniowane, mają znaczenie określone w Regulaminie.

Przetwarzanie odbywa się zgodnie z Rozporządzeniem (UE) 2016/679 ("RODO"), czeską ustawą nr 110/2019 Dz.U. o przetwarzaniu danych osobowych, ustawą nr 480/2004 Dz.U. o niektórych usługach społeczeństwa informacyjnego, Rozporządzeniem (UE) 2022/2065 (DSA) oraz innymi obowiązującymi przepisami.

Dane kontaktowe Administratora:

PHMarket s.r.o., Hlavní třída 87/2, 737 01 Český Těšín, Republika Czeska

IČO: 04529031 | NIP UE: CZ04529031 | Skrzynka danych: 234baq7

Ochrona danych osobowych: privacy@phmarket.cz | Wsparcie ogólne: support@phmarket.cz

Strona internetowa: https://www.phmarket.cz

Z uwagi na charakter i zakres przetwarzania Administrator nie ma obowiązku wyznaczenia inspektora ochrony danych (IOD) zgodnie z art. 37 RODO. Wszelka komunikacja w sprawach ochrony danych osobowych odbywa się za pośrednictwem dedykowanego adresu privacy@phmarket.cz.

2. ZAKRES STOSOWANIA I KLUCZOWE POJĘCIA

2.1. Zakres geograficzny: Aplikacja jest przeznaczona przede wszystkim dla użytkowników z państw członkowskich UE, Zjednoczonego Królestwa, Norwegii, Islandii, Liechtensteinu i Szwajcarii. W przypadku korzystania z innej jurysdykcji przetwarzanie odbywa się zgodnie z RODO.

2.2. Osoba, której dane dotyczą: Ty, jako osoba fizyczna, która pobiera, instaluje, tworzy Konto lub w jakikolwiek inny sposób korzysta z Aplikacji, czy to w trybie "Korzystanie bez rejestracji", czy jako użytkownik zarejestrowany.

2.3. Kluczowa różnica między trybami:

- Korzystanie bez rejestracji: Aplikacja działa bez utworzenia Konta; dostępne są podstawowe funkcje (mapa, ceny, nawigacja, stacje Quality, Fuel Quality w trybie tylko do odczytu). Przetwarzane dane ograniczają się do technicznych identyfikatorów urządzenia (install_id, UUID generowany przez Aplikację), ustawień preferencji (język, waluta) i pseudonimizowanych danych analitycznych. NIE jest to anonimowe konto Supabase; formalne konto użytkownika w naszej bazie danych (auth.users) jest tworzone dopiero przy rejestracji.
- Konto zarejestrowane: Pełnoprawne konto obejmujące imię/pseudonim, e-mail i inne dane niezbędne do udziału w Programie PHM Cash, korzystania z usługi PusHMe, zgłaszania cen

społecznościowych, tworzenia Stacji społecznościowych, ocen Fuel Quality oraz realizacji Flash Offers.

3. KATEGORIE PRZETWARZANYCH DANYCH OSOBOWYCH

Administrator gromadzi i przetwarza następujące kategorie danych osobowych, zawsze w zakresie niezbędnym dla konkretnego celu i zgodnie z zasadą minimalizacji danych zgodnie z art. 5 ust. 1 lit. c RODO:

3.1. Dane identyfikacyjne i kontaktowe (tylko Konto zarejestrowane)

- Imię lub pseudonim (prawdziwe imię i nazwisko nie jest wymagane; przechowywane w user_metadata.nickname lub user_metadata.first_name)
- Adres e-mail (może to być e-mail "relay" z Apple Hide My Email, jeśli logujesz się przez Sign in with Apple; w takim przypadku nie otrzymujemy Twojego prawdziwego adresu)
- Apple ID lub Google ID (wyłącznie wewnętrzny identyfikator dostarczony przez proces OAuth, a nie hasło do Twojego konta Apple/Google)
- Hasło (przechowywane w postaci zahaszowanej za pomocą bcrypt z solą w Supabase Auth, nigdy w postaci jawnej); tylko jeśli rejestrujesz się za pomocą e-maila

3.2. Dane techniczne i identyfikacyjne urządzenia

- install_id: Unikalny identyfikator instalacji Aplikacji generowany przy pierwszym uruchomieniu i przechowywany lokalnie (MMKV). Nie jest to identyfikator systemowy (IDFA na iOS / AAID na Androidzie); nie może być używany do śledzenia między aplikacjami.
- Typ i model urządzenia mobilnego (np. iPhone 15, Samsung Galaxy S24); zbierane przez expo-device
- Marka producenta urządzenia (Apple, Samsung itd.)
- Wersja systemu operacyjnego (iOS 18, Android 14 itd.)
- Wersja Aplikacji (app_version z expo-application)
- Adres IP (zanonimizowany; przechowujemy tylko pierwsze trzy oktety, np. 192.168.1.* zamiast 192.168.1.45, wyłącznie do przybliżonej analizy geograficznej)
- Ustawienia języka i strefa czasowa (locale, timezone); z expo-localization
- Token powiadomień push (Expo Push Token; usługa Expo Push Service, która przekazuje go dalej do Apple APNs lub Google FCM)

3.3. Dane lokalizacyjne

Aplikacja pracuje z informacją o Twojej bieżącej lokalizacji w celu wyświetlania pobliskich Stacji partnerskich, obliczania odległości, nawigacji, wykrywania kraju dla Fuel Quality oraz obsługi mechanizmu snap-to-station przy zgłaszaniu cen. Przetwarzanie odbywa się następująco:

Śledzenie wyłącznie na pierwszym planie: Aplikacja uzyskuje Twoją lokalizację wyłącznie wtedy, gdy znajduje się na pierwszym planie. NIE śledzimy lokalizacji w tle. Po zamknięciu aplikacji lub przejściu w tło subskrypcja GPS kończy się (na poziomie systemu iOS/Android). Używamy wyłącznie uprawnienia pierwszoplanowego (Location.requestForegroundPermissionsAsync w expo-location).

Dokładność lokalizacji: Używamy jednolitego poziomu dokładności, Location.Accuracy.Balanced (około ~100 metrów). Nie korzystamy z najwyższej dokładności (High accuracy, ~5 do 20 metrów), ponieważ balanced wystarcza dla funkcjonalności aplikacji.

Ciągłe śledzenie na pierwszym planie: Po udzieleniu zgody system operacyjny wywołuje watchPositionAsync z interwałem 30 sekund i progiem 50 metrów; w naszej aplikacji zapisujemy nowy stan tylko wtedy, gdy użytkownik przemieścił się o więcej niż 100 metrów lub upłynął określony czas. Lokalizacja nie jest zatem zapisywana na serwerze ani lokalnie co 30 sekund; jest przechowywana wyłącznie na potrzeby bieżącej sesji aplikacji.

Trwałość lokalizacji: Nie przechowujemy trwale Twoich współrzędnych GPS na serwerach, z wyjątkiem przypadków, gdy stanowią one część konkretnego rekordu (np. tankowanie w Programie PHM Cash, społecznościowe zgłoszenie ceny, utworzenie Stacji społecznościowej). W takich przypadkach przechowujemy wyłącznie współrzędne powiązane z danym rekordem, a nie historyczny ślad ruchu.

Wykryty kraj (cache): Na potrzeby funkcji Fuel Quality wykrywamy kraj (CZ/PL/SK/DE/AT/HU) na podstawie ostatniej lokalizacji i zapisujemy ten kod kraju lokalnie w MMKV (fq_detected_country). Służy on do automatycznej inicjalizacji sekcji Fuel Quality przy następnym otwarciu, a nie do profilowania.

Snap-to-station: Przy zgłaszaniu ceny paliwa (zgłoszenie społecznościowe) Aplikacja wywołuje funkcję find_nearest_station(GPS), która "przyciąga" Twoją lokalizację do najbliższej Stacji katalogowej w promieniu 25 km. Jest to środek ANTYSABOTAŻOWY; ceny nie można zgłosić dla dowolnej współrzędnej GPS, a wyłącznie dla istniejącej stacji. Twój GPS w momencie zgłoszenia nie pozostaje zapisany jako część ceny; zapisywany jest wyłącznie fuel_station_id.

Wycofanie zgody na lokalizację: Możesz ją wycofać w dowolnym momencie w ustawieniach iOS/ Android. Aplikacja działa również bez lokalizacji; jedynie nie może sortować stacji według odległości, nawigować ani przyciągać cen. Zamiast bieżącej lokalizacji używana jest "ostatnia znana lokalizacja" buforowana przez system operacyjny, ewentualnie użytkownik jest proszony o wpisanie celu tekstowo.

3.4. Dane o pojeździe i profilu kierowcy

- Rodzaj paliwa (Natural 95, Diesel, LPG, CNG, AdBlue, HVO, EV)
- Zużycie paliwa (l/100 km lub kWh/100 km)
- Pojemność zbiornika lub baterii (w przypadku EV)
- Typ pojazdu (osobowy, lekki dostawczy, ciężarówka itd.)
- Preferowana waluta wyświetlania cen (CZK, EUR, PLN, HUF, USD)
- Preferowana jednostka odległości (kilometry / mile)
- Preferowana aplikacja nawigacyjna (Apple Maps, Google Maps, Waze, Mapy.cz)

Profil pojazdu jest przechowywany zarówno lokalnie (cache w MMKV pod kluczem vehicle_cache dla wzorca stale-while-revalidate), jak i na serwerze w user_metadata w celu synchronizacji między urządzeniami.

Zdjęcie profilowe (przetwarzane wyłącznie na urządzeniu): Jeśli ustawisz zdjęcie profilowe, Aplikacja zmniejsza je do 200 x 200 pikseli i zapisuje wyłącznie lokalnie w pamięci Twojego urządzenia

(documentDirectory). Zdjęcie profilowe NIGDY nie jest wysyłane na serwery Operatora ani osób trzecich i nie stanowi części żadnej transmisji danych. Usuwasz je w profilu Aplikacji lub przez odinstalowanie Aplikacji. Uprawnienie do biblioteki zdjęć jest żądane wyłącznie w momencie wyboru zdjęcia i służy wyłącznie temu celowi.

3.5. Dane o aktywności w Aplikacji

- Historia odwiedzonych w Aplikacji Stacji partnerskich (otwarcie szczegółów stacji)
- Historia tankowań zarejestrowanych w Programie PHM Cash (data, godzina, Stacja partnerska, rodzaj paliwa, ilość, cena, GPS w momencie tankowania w celu weryfikacji)
- Społecznościowe zgłoszenia cen: cena, fuel_station_id, rodzaj paliwa, znacznik czasu, source_currency, waluta, kurs FX
- Utworzone Stacje społecznościowe: nazwa, adres, miasto, współrzędne GPS, creator_display (skrócona nazwa z user_metadata.display_name lub prefiks e-maila)
- Oceny Fuel Quality: fuel_station_id, is_positive (boolean), opcjonalny komentarz (maks. 200 znaków), opcjonalna brand_suggestion (sugestia marki stacji)
- Recenzje i oceny Stacji partnerskich
- Obserwowane Stacje partnerskie ("ulubione")
- Trasy i zapytania nawigacyjne (przechowywane wyłącznie tymczasowo na potrzeby obliczeń; cache recent_destinations_v1, FIFO maks. 8 pozycji, lokalnie)
- Postęp easter eggów (ee_station_detail_count, ee_app_open_count, ee_radio_unlocked, radio_cooldown_sent_at): lokalne liczniki do odblokowania PusHMe

3.6. Dane Programu PHM Cash

Uwaga: Program PHM Cash jest w przygotowaniu (coming soon) na dzień wejścia w życie niniejszej Polityki. Poniższe kategorie danych będą przetwarzane od momentu uruchomienia Programu.

- Stan Punktów PHM Cash i aktualny Poziom
- Historia zdobywania i wymiany Punktów (dziennik transakcji)
- Identyfikator polecenia (jeśli zostałeś zaproszony przez innego użytkownika)
- Dane bankowe: IBAN i imię i nazwisko właściciela rachunku (wyłącznie jeśli wnioskujesz o roczną wypłatę nagrody pieniężnej; zapisywane wyłącznie w momencie ubiegania się o wypłatę, nie automatycznie)
- Contribution score (wewnętrzny wskaźnik reputacji, typowo w zakresie od -10 wzwyż), używany do automatycznej moderacji (zob. artykuł 4.4 poniżej, shadowban i przejrzysta moderacja)

3.7. Dane usługi PusHMe

PusHMe to system szyfrowanych krótkich wiadomości na częstotliwościach definiowanych przez użytkowników (1000 do 9999). Szyfrowanie odbywa się na urządzeniu nadawcy przed wysłaniem na serwer. Szczegóły przetwarzania:

Klucz szyfru: Klucz jest wyprowadzany funkcją SHA-256 z ciągu 'phmarket:radio:v1:' + Częstotliwość (np. 'phmarket:radio:v1:4242'). Nie jest to trywialny XOR z numeryczną Częstotliwością jako kluczem,

lecz XOR z 256-bitowym kluczem wyprowadzonym z hasha. W normalnej eksploatacji serwer PHMarket nie może odczytać treści wiadomości bez znajomości Częstotliwości.

Fallback PLAIN: (ważne): Jeśli na urządzeniu użytkownika zawiedzie kryptograficzne API (Crypto.digestStringAsync), zazwyczaj na bardzo starych urządzeniach, Aplikacja posiada tryb awaryjny, w którym zapisuje wiadomość z prefiksem "PLAIN:" w postaci jawnej. W takim przypadku treść wiadomości jest czytelna nawet bez znajomości Częstotliwości, przez czas trwania 30-minutowego okresu przechowywania. Prawdopodobieństwo wystąpienia tego stanu jest w praktyce niskie (ok. <0,5 % urządzeń), ale ujawniamy je dla pełnej przejrzystości.

- Metadane wiadomości (przechowywane na serwerze): czas wysłania, zanonimizowany identyfikator nadawcy (UUID auth.users.id, nie e-mail/imię), Częstotliwość (kanał numeryczny 1000 do 9999), opcjonalnie station_id (kontekst stacji)
- Zaszyfrowana treść wiadomości: przechowywana na serwerze maksymalnie 30 minut (expires_at domyślnie now() + 30 min); następnie automatycznie i nieodwracalnie usuwana przez zadanie cron
- Kanały systemowe (101 Live drops, 111 Kawa i jedzenie, 121 Pielęgnacja auta, 131 Specjalny): wiadomości w kanałach systemowych są JAWNE (is_system=true) i są nadawane przez Operatora lub autoryzowanych przez niego partnerów. Pełnią funkcję kanału marketing-light; wysyłanie komercyjnych komunikatów w kanałach systemowych podlega zgodzie zgodnie z § 7 ustawy nr 480/2004 Dz.U. (zgoda na powiadomienia push w Profil, Powiadomienia)
- Lista Twoich ulubionych Częstotliwości (radio_listening, maks. 5): przechowywana w tabeli profiles na serwerze
- Lista zablokowanych użytkowników na poszczególnych Częstotliwościach: przechowywana lokalnie
- Zgłoszenia wiadomości (tabela radio_reports): jeśli zgłosisz wiadomość, w odniesieniu do tego zgłoszenia przechowujemy zaszyfrowaną treść, identyfikator nadawcy, kategorię zgłoszenia (illegal / harassment / spam / other), czas oraz Twój identyfikator zgłaszającego; przechowywane przez 30 dni od zakończenia rozpatrywania lub 1 rok na potrzeby ewentualnego sporu

3.8. Dane analityczne i diagnostyczne

PostHog (analityka produktowa): Aby zrozumieć sposób korzystania z Aplikacji, wykorzystujemy PostHog, Inc. na instancji UE (host: https://eu.i.posthog.com). Zbieramy pseudonimizowane zdarzenia analityczne: wyświetlenia ekranów, kliknięcia, akcje nawigacyjne, powodzenie/ niepowodzenie operacji, postęp easter eggów, metryki wydajności. Identyfikator distinct_id w PostHog to install_id podczas Korzystania bez rejestracji (anonimowy per instalacja) oraz Twój Supabase user_id przy Koncie zarejestrowanym. Jest to zatem PSEUDONIMIZACJA, a nie pełna anonimizacja; użytkownik jest identyfikowany spójnie między sesjami, ale identyfikator nie może samodzielnie zostać powiązany z Twoją osobą bez dodatkowej informacji (e-mail / imię) z naszej bazy danych. Przy wylogowaniu wywołujemy posthog.reset(); nowa sesja otrzymuje nową tożsamość.

Sentry (diagnostyka błędów i awarii): Do wykrywania i naprawiania błędów wykorzystujemy Sentry (Functional Software, Inc.) na infrastrukturze amerykańskiej z SCC. Sentry przechwytuje błędy JavaScript, natywne awarie, stack traces, breadcrumbs (przechwycone zdarzenia trackEvent

przekazywane do Sentry), kontekst urządzenia (model, OS) oraz pseudonimizowany identyfikator użytkownika. Okres przechowywania Sentry wynosi 90 dni.

- Kontekst automatycznie dołączany do zdarzeń analitycznych: session_id, install_id, device_model, device_brand, os_version, timezone, locale, app_version, app_start_type (cold/warm), push_permission_status
- Konkretne zdarzenia: 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 oraz inne zdarzenia techniczne
- Agregacja geograficzna do statystyk: Twoje współrzędne GPS są w agregacjach analitycznych zaokrąglane do bloków ~10 km (lat_bucket, lng_bucket) w celu identyfikacji trendów geograficznych, a nie identyfikacji konkretnego miejsca

3.9. Dane z komunikacji ze wsparciem

- Treść Twojej wiadomości wysłanej do wsparcia (support@phmarket.cz, privacy@phmarket.cz, legal@phmarket.cz, notice@phmarket.cz, csae@phmarket.cz)
- Nasze odpowiedzi i wszelka dalsza komunikacja
- Metadane komunikacji (czas, adres e-mail, temat)

4. CELE PRZETWARZANIA I PODSTAWY PRAWNE

Administrator przetwarza Twoje dane osobowe wyłącznie w określonych, wyraźnie wskazanych i prawnie uzasadnionych celach, na podstawie konkretnej podstawy prawnej zgodnie z art. 6 ust. 1 RODO. Szczegółowy przegląd:

4.1. Świadczenie podstawowych funkcji Aplikacji (mapa, ceny paliw, nawigacja, stacje Quality, Fuel Quality w trybie tylko do odczytu) użytkownikom bez rejestracji oraz użytkownikom zarejestrowanym. Podstawa prawna: wykonanie umowy (art. 6 ust. 1 lit. b RODO), tj. wykonanie Regulaminu, który stanowi umowę. Dane: dane techniczne urządzenia, dane lokalizacyjne (tylko pierwszy plan), ustawienia preferencji. Przechowywanie: przez czas korzystania z Aplikacji; ustawienia preferencji przez czas istnienia Konta lub do odinstalowania.

4.2. Zarządzanie Kontem zarejestrowanym, uwierzytelnianie, resetowanie hasła. Podstawa prawna: wykonanie umowy (art. 6 ust. 1 lit. b RODO). Dane: imię/pseudonim, e-mail, zahaszowane hasło, identyfikator OAuth Apple/Google. Przechowywanie: przez czas istnienia Konta + 90 dni po usunięciu na potrzeby rotacji kopii zapasowych.

4.3. Udział w Programie PHM Cash (przyznawanie Punktów, ewidencja tankowań, wypłaty); aktywne od uruchomienia Programu, obecnie coming soon. Podstawa prawna: wykonanie umowy (art. 6 ust. 1 lit. b RODO); obowiązek prawny wynikający z ustawy o rachunkowości i przepisów podatkowych (art. 6 ust. 1 lit. c RODO) dla celów księgowych. Dane: dane identyfikacyjne, dane o tankowaniach, poziom, punkty, dane bankowe (IBAN, właściciel rachunku), IBAN wyłącznie przy

ubieganiu się o wypłatę. Przechowywanie: przez czas udziału w Programie; dokumenty księgowe 10 lat zgodnie z ustawą nr 563/1991 Dz.U.

4.4. Usługa PusHMe: wysyłanie i dostarczanie szyfrowanych wiadomości między użytkownikami, moderacja treści, zapobieganie nadużyciom. Podstawa prawna: wykonanie umowy (art. 6 ust. 1 lit. b RODO); prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO) w zakresie moderacji i zapobiegania nadużyciom. Dane: metadane wiadomości, zaszyfrowana treść (lub fallback PLAIN:), identyfikator nadawcy, zablokowani użytkownicy, zgłoszenia. Przechowywanie: treść zaszyfrowana/jawna maks. 30 minut; metadane maks. 90 dni; zgłoszenia do zakończenia rozpatrywania + 1 rok.

4.5. Społecznościowe zgłoszenia cen, tworzenie Stacji społecznościowych, recenzje, oceny Stacji partnerskich. Podstawa prawna: wykonanie umowy (art. 6 ust. 1 lit. b RODO); prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO), funkcjonowanie Aplikacji i jakość informacji; audyt antyfraudowy (prices_audit). Dane: identyfikator użytkownika, creator_display, treść zgłoszenia/stacji, znacznik czasu, GPS do weryfikacji snap-to-station (nieprzechowywany długoterminowo), antyfraudowe rekordy rate_limit_block. Przechowywanie: wkłady przez czas istnienia Konta lub do usunięcia poszczególnej treści; audyt antyfraudowy 3 lata.

4.6. Oceny Fuel Quality: recenzje (pozytywne / z zastrzeżeniami), sugestie marek. Podstawa prawna: wykonanie umowy (art. 6 ust. 1 lit. b RODO) oraz prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO), informowanie konsumentów o jakości paliw. Dane: fuel_station_id, is_positive, opcjonalny komentarz (maks. 200 znaków), opcjonalna brand_suggestion, identyfikator użytkownika, czas. Przechowywanie: przez czas istnienia Konta lub do usunięcia poszczególnej oceny.

4.7. Publikacja kar nałożonych przez Czeską Inspekcję Handlową (ČOI) w sekcji Fuel Quality. Podstawa prawna: prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO), informowanie konsumentów o publicznie dostępnych danych o jakości paliw; dane pochodzą z publicznie ogłoszonych decyzji ČOI. Dane: nazwa stacji, miasto, rok kary, powód, URL dokumentu źródłowego ČOI. Przechowywanie: przez czas, gdy dane są aktualne (aktywna kara) + 3 lata.

4.8. Serwisowe powiadomienia push (zmiany Konta, Punkty PHM Cash, moderacja treści, Statement of Reasons). Podstawa prawna: wykonanie umowy i prawnie uzasadniony interes (art. 6 ust. 1 lit. b i f RODO). Dane: Expo Push Token, dane o zdarzeniach na Koncie. Przechowywanie: przez czas korzystania z Aplikacji.

4.9. Marketingowe powiadomienia push, nowości, Flash Offers w PusHMe (obecnie nieaktywne; zostaną aktywowane w przyszłych wersjach). Podstawa prawna: zgoda (art. 6 ust. 1 lit. a RODO), udzielona za pośrednictwem dialogu opt-in w Profil, Powiadomienia. Dane: Expo Push Token, preferencje (notif_nearby, notif_discount, notif_loyalty, notif_quality, notif_location). Przechowywanie: do wycofania zgody.

4.10. Analityka produktowa (PostHog): poprawa UX, zapobieganie błędom, testy A/B. Podstawa prawna: prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO). Jest to istotna zmiana w stosunku do wcześniejszych wersji niniejszej Polityki; analityka była pierwotnie uzależniona od odrębnej zgody na ekranie zgód GDPR; po przeglądzie ta warunkowość została oceniona jako niezgodna z art. 7 ust. 4 RODO i wytycznymi EROD 5/2020 (consent bundling). Analityka odbywa się obecnie na podstawie prawnie uzasadnionego interesu z pseudonimizacją, hostingiem w UE i łatwym opt-outem w Profil, Prywatność. Dane: pseudonimizowane zdarzenia analityczne, install_id (przed rejestracją), Supabase

user_id (po rejestracji); kontekst urządzenia (model, OS, locale). Przechowywanie: PostHog 12 miesięcy; zagregowane anonimowe statystyki bezterminowo.

4.11. Diagnostyka błędów i awarii (Sentry). Podstawa prawna: prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO). Dane: stack trace, breadcrumbs, pseudonimizowany identyfikator urządzenia, wersja OS/aplikacji, kontekst urządzenia. Przechowywanie: 90 dni (retencja Sentry).

4.12. Zapobieganie oszustwom, nadużyciom Programu PHM Cash, PusHMe i Flash Offers; automatyczna moderacja, w tym system shadowban (przejrzyście, zgodnie z art. 17 DSA). Podstawa prawna: prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO); obowiązek prawny wynikający z DSA. Dane: dane o aktywności, contribution_score, adres IP (zanonimizowany), urządzenie, rekordy prices_audit. Przechowywanie: przez czas trwania postępowania + 3 lata na potrzeby ewentualnego sporu.

4.13. Wypełnianie obowiązków wynikających z DSA (notice-and-action, statement of reasons, skargi wewnętrzne, raportowanie przejrzystości). Podstawa prawna: obowiązek prawny (art. 6 ust. 1 lit. c RODO), Rozporządzenie (UE) 2022/2065. Dane: dane o zgłoszeniach, decyzjach moderacyjnych, odwołaniach, raportach przejrzystości. Przechowywanie: 5 lat od zakończenia rozpatrywania.

4.14. Komunikacja ze wsparciem i rozpatrywanie reklamacji. Podstawa prawna: wykonanie umowy i prawnie uzasadniony interes (art. 6 ust. 1 lit. b i f RODO). Dane: treść komunikacji, adres e-mail, metadane. Przechowywanie: 3 lata od ostatniego kontaktu.

4.15. Wypełnianie obowiązków prawnych (rachunkowość, podatki, AML, żądania organów władzy publicznej). Podstawa prawna: obowiązek prawny (art. 6 ust. 1 lit. c RODO). Dane: dane księgowe i podatkowe, w tym dane bankowe do wypłat PHM Cash, dane do realizacji żądań. Przechowywanie: 5 do 10 lat zgodnie z ustawą o rachunkowości i przepisami podatkowymi.

5. OKRES PRZECHOWYWANIA DANYCH

5.1. Zasada ogólna: Przechowujemy dane wyłącznie przez okres ściśle niezbędny do realizacji danego celu przetwarzania i zgodnie z zasadą minimalizacji. Po upływie okresu przechowywania dane są nieodwracalnie usuwane lub anonimizowane.

5.2. Usunięcie Konta: W przypadku usunięcia Konta rozpoczynamy następujący proces:

- Produkcyjna baza danych: 30 dni od potwierdzenia żądania
- Kopie zapasowe: 90 dni od potwierdzenia żądania (kopie zapasowe są rotowane automatycznie)
- Dokumenty księgowe i dane do celów AML i podatkowych: 5 do 10 lat niezależnie od usunięcia Konta
- Dane związane z trwającym sporem/postępowaniem: przez czas jego trwania + 3 lata
- Dane zanonimizowane (zagregowane statystyki): mogą być przechowywane bezterminowo
- PostHog distinct_id: wywołujemy posthog.reset() przy wylogowaniu; po usunięciu Konta nowa sesja nie ma już powiązania z user_id, ale historyczne zdarzenia w PostHog powiązane z user_id pozostają w ramach 12-miesięcznej retencji; na żądanie usunięcia wywołujemy także PostHog Delete API

5.3. Sign in with Apple revoke (zobowiązanie): Jeśli logowałeś się przez Sign in with Apple i zażądasz usunięcia Konta, Administrator w ramach procesu usuwania wywołuje endpoint Apple Sign In REST API revokeToken i unieważnia Twoje tokeny refresh + access u Apple Inc. Zobowiązanie to wynika z wymogu Apple App Store Review Guideline 5.1.1(v); szczegóły implementacji są opublikowane w dokumencie code-side change tracking.

6. ODBIORCY DANYCH I PODMIOTY PRZETWARZAJĄCE

Przekazujemy Twoje dane osobowe następującym kategoriom odbiorców, zawsze w zakresie niezbędnym dla danego celu i na podstawie umów powierzenia przetwarzania zgodnie z art. 28 RODO:

6.1. Podmioty przetwarzające (Data Processors)

Supabase Inc. (USA; baza danych hostowana we Frankfurcie, UE) Rola: hosting bazy danych Postgres (auth.users, profiles, stations, prices, radio_broadcasts, fuel_stations itd.), uwierzytelnianie, funkcje czasu rzeczywistego dla PusHMe i społecznościowego rozgłaszania cen. Podstawa prawna: DPA + SCC; dane przechowywane wyłącznie w regionie UE (Frankfurt); ISO 27001/SOC 2.

PostHog, Inc. (USA; instancja UE: eu.i.posthog.com) Rola: pseudonimizowana analityka produktowa. Podstawa prawna: DPA; instancja UE bez przekazywania danych analitycznych do USA.

Functional Software, Inc. d/b/a Sentry (USA) Rola: diagnostyka błędów i awarii Aplikacji. Podstawa prawna: DPA + SCC; pseudonimizacja identyfikatorów; krótka retencja (90 dni).

Apple Inc. (USA / Irlandia dla operacji UE) Rola: dostarczanie powiadomień push (APNs); uwierzytelnianie Sign in with Apple; dystrybucja App Store. Podstawa prawna: Apple Developer Program Agreement + Apple Privacy Policy; mechanizmy przekazywania zgodnie z decyzją UE o adekwatności / DPF.

Google LLC (USA / Irlandia dla UE) Rola: dostarczanie powiadomień push (FCM); Sign in with Google; Maps API dla kafelków map; dystrybucja Google Play. Podstawa prawna: Google API Terms + DPA; SCC / DPF.

Expo (650 Industries, Inc., USA) Rola: Expo Push Service jako warstwa pośrednicząca między Aplikacją a APNs/FCM; infrastruktura aktualizacji OTA. Podstawa prawna: Expo Privacy Policy; Expo Push Token służy jako proxy dla tokena APNs/FCM; SCC.

Resend / Mailgun lub podobny (dostawca e-maili transakcyjnych) Rola: dostarczanie e-maili transakcyjnych (potwierdzenie rejestracji, reset hasła, usunięcie konta). Podstawa prawna: DPA + SCC; minimalna retencja.

6.2. Odbiorcy danych (Data Recipients)

- Stacje partnerskie: w ograniczonym zakresie przy realizacji Flash Offer (claim_code, czas, station_code) lub rejestracji tankowania w Programie PHM Cash (pseudonimizowany identyfikator + dane o tankowaniu). Stacje partnerskie nie otrzymują Twojego imienia, e-maila ani Apple/Google ID.
- Bank Operatora: w celu wypłaty nagrody pieniężnej z Programu PHM Cash (IBAN, imię i nazwisko właściciela rachunku, kwota); od uruchomienia Programu.

- Administracja podatkowa: jeśli wypłata przekroczy ustawowe limity raportowania.
- Biuro księgowe Operatora: w ramach zwykłych operacji księgowych.
- Pełnomocnicy prawni, audytorzy: przy wypełnianiu obowiązków prawnych.
- Organy ścigania, sądy, organy nadzorcze (ÚOOÚ, ČOI, ČTÚ, DSC innych państw członkowskich UE): na podstawie należycie złożonego żądania i zgodnie z obowiązującymi przepisami.
- National Center for Missing & Exploited Children (NCMEC) za pośrednictwem Internet Watch Foundation: w przypadku wykrycia treści CSAM/CSAE (art. 22 Regulaminu i CSAE Policy).
- Zaufane podmioty sygnalizujące (trusted flaggers, art. 22 DSA): na podstawie ich zgłoszeń i w zakresie niezbędnym do wykonywania ich uprawnień.

7. MIĘDZYNARODOWE PRZEKAZYWANIE DANYCH OSOBOWYCH

7.1. Zasada lokalizacji w UE: Naszą podstawową infrastrukturę danych (bazę danych Supabase, serwery PusHMe) prowadzimy wyłącznie w ramach Europejskiego Obszaru Gospodarczego (EOG), konkretnie w Niemczech (Frankfurt). Nie dochodzi tam do międzynarodowego przekazywania danych do państw trzecich w rozumieniu RODO.

7.2. Przekazywanie do USA i państw trzecich: Niektóre podmioty przetwarzające (Apple, Google, Expo, Sentry, Resend/Mailgun) mają siedzibę w Stanach Zjednoczonych. Do tych przekazań stosujemy:

- Standardowe klauzule umowne (SCC) zgodnie z decyzją wykonawczą Komisji (UE) 2021/914 jako mechanizm prawny zgodnie z art. 46 ust. 2 lit. c RODO
- Apple i Google: certyfikowane w ramach EU-U.S. Data Privacy Framework (DPF), o ile mechanizm ten jest skuteczny; alternatywnie SCC
- Środki uzupełniające: szyfrowanie podczas przesyłania (TLS 1.3) i w spoczynku (AES-256); pseudonimizacja identyfikatorów; minimalizacja przekazywanych danych

7.3. Transfer Impact Assessment: Dla każdego systematycznego przekazania do państwa trzeciego przeprowadzamy Transfer Impact Assessment (TIA) zgodnie z zaleceniami EROD.

8. TWOJE PRAWA JAKO OSOBY, KTÓREJ DANE DOTYCZĄ

W związku z przetwarzaniem Twoich danych osobowych przysługują Ci zgodnie z RODO następujące prawa. Możesz je w każdej chwili zrealizować pod adresem privacy@phmarket.cz lub bezpośrednio w Aplikacji (tam, gdzie dane prawo to umożliwia):

Prawo dostępu (art. 15 RODO) Masz prawo uzyskać potwierdzenie, czy Twoje dane są przetwarzane, a jeśli tak, prawo dostępu do danych i informacji o przetwarzaniu. Możesz zażądać kopii danych, którą udostępnimy bezpłatnie (za kolejne kopie rozsądna opłata).

Prawo do sprostowania (art. 16 RODO) Masz prawo do sprostowania nieprawidłowych danych. Większość danych możesz edytować bezpośrednio w Profil, Edytuj profil w Aplikacji.

Prawo do usunięcia (art. 17 RODO) Możesz żądać usunięcia swoich danych, najlepiej za pomocą funkcji "Usuń konto" w Aplikacji (Profil, Ustawienia, Usuń konto), przez stronę phmarket.cz/delete-

account lub e-mailem na support@phmarket.cz. Usunięcie może być ograniczone wypełnianiem obowiązków prawnych (rachunkowość, AML, raportowanie DSA).

Prawo do ograniczenia przetwarzania (art. 18 RODO) Możesz żądać ograniczenia przetwarzania w przypadkach określonych w art. 18 ust. 1 RODO.

Prawo do przenoszenia danych (art. 20 RODO) Masz prawo otrzymać dane, które dostarczyłeś, w ustrukturyzowanym, powszechnie używanym i nadającym się do odczytu maszynowego formacie (JSON) oraz przekazać je innemu administratorowi.

Prawo do sprzeciwu (art. 21 RODO) Masz prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania opartego na prawnie uzasadnionym interesie (art. 6 ust. 1 lit. f). Dotyczy to w szczególności: analityki produktowej (PostHog), diagnostyki (Sentry), zapobiegania oszustwom, moderacji, agregacji geograficznej. Sprzeciw możesz wnieść w Profil, Prywatność, Wnieś sprzeciw, lub e-mailem na privacy@phmarket.cz. Po wniesieniu sprzeciwu zaprzestaniemy przetwarzania, chyba że wykażemy ważne prawnie uzasadnione podstawy nadrzędne wobec Twoich interesów. DLA ANALITYKI PostHog: możesz po prostu zrezygnować w Profil, Prywatność, Analityka (przełącznik); po jego wyłączeniu PostHog nie jest już wywoływany w aplikacji (czysto klienckie odcięcie).

Prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji (art. 22 RODO) Masz prawo nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu wywołującej istotne skutki. Nasza zautomatyzowana moderacja (limity, kontrole wiarygodności, shadowban na podstawie contribution_score) NIE jest wyłącznie zautomatyzowana; ostateczna decyzja o sankcjach typu shadowban podlega weryfikacji przez człowieka, a w każdym przypadku masz prawo do Statement of Reasons (art. 17 DSA) i wniesienia skargi wewnętrznej (art. 20 DSA).

Prawo do wycofania zgody (art. 7 ust. 3 RODO) Jeżeli przetwarzanie opiera się na zgodzie (marketingowe powiadomienia push), możesz wycofać zgodę w dowolnym momencie w ustawieniach Aplikacji lub systemu operacyjnego.

Prawo do wniesienia skargi do organu nadzorczego (art. 77 RODO) W Czechach: Urząd Ochrony Danych Osobowych (ÚOOÚ), Pplk. Sochora 27, 170 00 Praga 7, https://www.uoou.gov.cz. W innych państwach członkowskich UE: organ nadzorczy właściwy dla kraju Twojego zwykłego pobytu, w Polsce: Prezes Urzędu Ochrony Danych Osobowych (UODO), ul. Stawki 2, 00-193 Warszawa, https://uodo.gov.pl.

Terminy rozpatrzenia: Żądania rozpatrzymy bez zbędnej zwłoki, najpóźniej w ciągu jednego (1) miesiąca. Termin może zostać przedłużony o kolejne dwa miesiące. Rozpatrzenie jest bezpłatne; w przypadku żądań ewidentnie nieuzasadnionych rozsądna opłata lub odmowa.

Weryfikacja tożsamości: W celu ochrony Twoich praw zastrzegamy sobie prawo do weryfikacji Twojej tożsamości przed rozpatrzeniem żądania (zazwyczaj e-mailem z adresu powiązanego z Kontem).

9. ZGODY W APLIKACJI I ONBOARDING

Przy pierwszym uruchomieniu Aplikacji wyświetlamy początkowy ekran zgód ("ekran zgód GDPR"). W aktualnej wersji 3 niniejszej Polityki:

- Zgoda na przetwarzanie danych osobowych (BLOKUJĄCA): Zgoda ta odzwierciedla, że akceptując Regulamin korzystasz z Aplikacji i zgadzasz się na przetwarzanie danych osobowych

niezbędnych do wykonania umowy (art. 6 ust. 1 lit. b RODO). Bez tej zgody nie można korzystać z Aplikacji.

- Zgoda na zbieranie danych analitycznych (NIEBLOKUJĄCA, opt-out w dowolnym momencie): Analityka (PostHog) jest przetwarzana przede wszystkim na podstawie prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO). Zgoda na ekranie zgód ma charakter informacyjny i daje Ci możliwość początkowej rezygnacji. Analitykę możesz wyłączyć w dowolnym późniejszym momencie w Profil, Prywatność, Analityka.

Zmiana w stosunku do poprzednich wersji niniejszej Polityki: Poprzednie wersje uzależniały korzystanie z Aplikacji od zgody na analitykę jako blokującego pola wyboru. Po przeglądzie usunęliśmy tę warunkowość zgodnie z art. 7 ust. 4 RODO i wytycznymi EROD 5/2020; zgoda na analitykę nie może być ważnym warunkiem korzystania z usługi, która nie potrzebuje analityki do swojego funkcjonowania.

10. PLIKI COOKIE I PODOBNE TECHNOLOGIE

10.1. W aplikacji mobilnej: Aplikacja nie używa standardowych internetowych plików cookie. Zamiast tego:

- Lokalna pamięć urządzenia MMKV: dla ustawień preferencji, install_id, tokenów uwierzytelniających (przechowywanych w postaci zaszyfrowanej), flag funkcji, danych z pamięci podręcznej
- Klasyfikacja kluczy (lib/dataLifecycle.ts): DEVICE_LEVEL_KEYS (przetrwają wylogowanie: install_id, język, waluta, push_token) vs USER_LEVEL_KEYS (usuwane przy wylogowaniu: cache, preferencje)
- install_id generowany przez Aplikację: do identyfikacji instalacji w analityce; NIE jest to systemowy IDFA (Apple) ani AAID (Google)
- Expo Push Token: do dostarczania powiadomień push

10.2. Na stronie internetowej phmarket.cz: Jeśli odwiedzisz naszą stronę internetową (np. phmarket.cz/delete-account), możemy używać niezbędnych technicznych plików cookie zgodnie z Cookies Policy na stronie.

11. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

11.1. Środki techniczne i organizacyjne:

- Szyfrowanie podczas przesyłania: TLS 1.3 dla całej komunikacji z serwerami; HSTS na stronie internetowej
- Szyfrowanie w spoczynku: AES-256 dla danych wrażliwych w bazie danych Supabase; bcrypt do haszowania haseł
- Szyfrowanie PusHMe: XOR z kluczem wyprowadzonym z SHA-256 (z phmarket:radio:v1:Częstotliwość); serwer nie widzi treści w normalnej eksploatacji, ale UWAGA: w przypadku fallbacku PLAIN: (awaria API kryptograficznego na urządzeniu) wiadomość jest przechowywana w postaci jawnej przez czas 30-minutowej retencji
- Pseudonimizacja identyfikatorów w danych analitycznych

- Zasada najmniejszych uprawnień (least privilege) dla dostępu do danych; Row-Level Security (RLS) w Supabase
- Regularne aktualizacje bezpieczeństwa i łatanie infrastruktury
- Zautomatyzowane kopie zapasowe z regularnym testowaniem możliwości odtworzenia
- Logowanie zdarzeń bezpieczeństwa i ich monitorowanie (Sentry, logi audytowe Supabase)
- Testy penetracyjne, code review nowego kodu
- Polityki bezpieczeństwa informacji i szkolenia pracowników
- Walidacja po stronie serwera wszystkich wywołań RPC: limity, kontrole wiarygodności (±50 % mediany cen), geofence (25 do 50 km), wykrywanie duplikatów (50 m)

11.2. Powiadomienie o naruszeniu bezpieczeństwa: W przypadku naruszenia o wysokim ryzyku dla Twoich praw powiadomimy Cię bez zbędnej zwłoki zgodnie z art. 34 RODO. Poważne naruszenia zgłaszamy także do ÚOOÚ w terminie 72 godzin zgodnie z art. 33 RODO.

11.3. Zalecenia dla Ciebie: Używaj silnego i unikalnego hasła; chroń dostęp do swojego e-maila; nie udostępniaj danych logowania; niezwłocznie zgłaszaj podejrzenia nieautoryzowanego dostępu na support@phmarket.cz.

12. DZIECI I OCHRONA NIELETNICH

12.1. Ograniczenie wiekowe: Aplikacja nie jest przeznaczona dla dzieci poniżej siedemnastego (17) roku życia. Ocena Mature 17+ w Google Play oraz kategoria 18+ w Apple App Store (zgodnie z systemem ocen wiekowych Apple obowiązującym od 2026 r., który zastąpił wcześniejszą kategorię 17+) odnoszą się do funkcji PusHMe (komunikacja z nieznanymi osobami).

12.2. Zapewnienie użytkownika: Korzystając z Aplikacji oświadczasz, że masz ukończone co najmniej 17 lat.

12.3. CSAE / CSAM: Aplikacja stosuje absolutną zerową tolerancję wobec materiałów przedstawiających seksualne wykorzystywanie dzieci (CSAM/CSAE). Wykrywanie odbywa się poprzez dopasowanie hashy (PhotoDNA/Microsoft / listy hashy IWF), przyciski zgłaszania w PusHMe i wkładach społecznościowych oraz zautomatyzowane heurystyki. Po wykryciu następuje natychmiastowe usunięcie treści, trwałe zablokowanie Użytkownika, zgłoszenie do NCMEC za pośrednictwem IWF oraz powiadomienie organów ścigania zgodnie z rozporządzeniem (UE) 2021/1232. Kontakt: csae@phmarket.cz.

13. ZMIANY POLITYKI

Możemy od czasu do czasu aktualizować niniejszą Politykę. O istotnych zmianach poinformujemy Cię z odpowiednim wyprzedzeniem (co najmniej 30 dni przed wejściem w życie) w Aplikacji, powiadomieniem push lub e-mailem. Aktualna wersja jest zawsze dostępna w Aplikacji oraz na phmarket.cz/privacy-policy.

14. INFORMACJE SPECYFICZNE DLA PLATFORMY APPLE (iOS)

14.1. Privacy Manifests (PrivacyInfo.xcprivacy): Aplikacja zawiera Privacy Manifest zgodnie z wymogami Apple App Store Privacy (obowiązującymi od maja 2024 r.). SDK podmiotów trzecich (PostHog 3.x+, Sentry 8.x+) również zawierają własne Privacy Manifests.

14.2. App Tracking Transparency (ATT): Administrator nie prowadzi śledzenia w rozumieniu frameworka Apple ATT; brak śledzenia między aplikacjami i udostępniania brokerom danych. Aplikacja nie wyświetla zatem komunikatu ATT.

14.3. Sign in with Apple: Logując się przez Sign in with Apple, możesz skorzystać z "Hide My Email" (e-mail przekaźnikowy Apple). Przy usunięciu Konta wywołujemy endpoint Apple Sign In REST API revokeToken i unieważniamy Twoje tokeny u Apple. Ta implementacja jest opublikowana w dokumencie code-side change tracking.

14.4. Family Sharing: Przy udostępnianiu Aplikacji przez Family Sharing każdy członek rodziny tworzy własne Konto z własnymi danymi.

15. INFORMACJE SPECYFICZNE DLA PLATFORMY GOOGLE (Android)

15.1. Formularz Data Safety: Wypełniliśmy formularz Data Safety w Google Play Console zgodnie z Google User Data Policy. Opisuje on szczegółowo rodzaje przetwarzanych danych, cele oraz udostępnianie podmiotom trzecim.

15.2. Zasób internetowy do usuwania konta: Zgodnie z Google Play User Data Policy usunięcie Konta można zainicjować również przez phmarket.cz/delete-account, bez konieczności instalowania Aplikacji.

15.3. Sign in with Google: Od Google otrzymujemy wyłącznie imię i adres e-mail z Twojego profilu Google.

15.4. Play Integrity API: W celu zapobiegania nadużyciom używamy (lub będziemy używać) Google Play Integrity API. Werdykt zawiera sygnały o integralności urządzenia i aplikacji; przechowujemy go wyłącznie w formie zanonimizowanej do wykrywania oszustw (tabela integrity_checks, odczyt/zapis wyłącznie przez service_role).

16. JAK SIĘ Z NAMI SKONTAKTOWAĆ

W sprawie wszelkich pytań, żądań lub skarg dotyczących ochrony danych osobowych:

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Republika Czeska

IČO: 04529031 | Skrzynka danych: 234baq7

Ochrona danych osobowych: privacy@phmarket.cz

Wsparcie ogólne: support@phmarket.cz

Sprawy prawne / punkt kontaktowy DSA: legal@phmarket.cz

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

Bezpieczeństwo dzieci (CSAE): csae@phmarket.cz

Strona internetowa: https://www.phmarket.cz

Usunięcie konta (web): https://www.phmarket.cz/delete-account

Organ nadzorczy CZ: Urząd Ochrony Danych Osobowych (ÚOOÚ), Pplk. Sochora 27, 170 00 Praga 7, Republika Czeska, https://www.uoou.gov.cz, telefon: +420 234 665 111

Niniejsza Polityka prywatności wchodzi w życie z dniem 1 czerwca 2026 r. i zastępuje wszystkie poprzednie wersje.