



# **DATENSCHUTZERKLÄRUNG**

## **MOBILE APPLIKATION PHMARKET**

*Gültig ab: 1. Juni 2026*

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Tschechische Republik

IČO (Firmen-ID): 04529031 | USt-IdNr.: CZ04529031 | Datenbox: 234baq7

Bundle ID: cz.phmarket.app

## 1. EINLEITUNG UND KONTAKT ZUM VERANTWORTLICHEN

Diese Datenschutzerklärung (die "Erklärung") beschreibt, wie die Gesellschaft PHMarket s.r.o., IČO: 04529031, mit Sitz in Hlavní třída 87/2, 737 01 Český Těšín, Tschechische Republik, eingetragen im Handelsregister des Kreisgerichts in Ostrava, Abteilung C, Einlage 64228 ("PHMarket", der "Verantwortliche", "wir" oder "unser"), die personenbezogenen Daten der Nutzer der mobilen Applikation PHMarket (Bundle Identifier cz.phmarket.app, die "App") verarbeitet.

Diese Erklärung ist integraler Bestandteil der Allgemeinen Geschäftsbedingungen (die "Bedingungen") und ist in Verbindung mit diesen auszulegen. Großgeschriebene Begriffe, die hier nicht definiert sind, haben die in den Bedingungen festgelegte Bedeutung.

Die Verarbeitung erfolgt im Einklang mit der Verordnung (EU) 2016/679 ("DSGVO"), dem tschechischen Gesetz Nr. 110/2019 Slg. über die Verarbeitung personenbezogener Daten, dem Gesetz Nr. 480/2004 Slg. über bestimmte Dienste der Informationsgesellschaft, der Verordnung (EU) 2022/2065 (DSA) und weiteren anwendbaren Vorschriften.

### Kontaktdaten des Verantwortlichen:

PHMarket s.r.o., Hlavní třída 87/2, 737 01 Český Těšín, Tschechische Republik

IČO: 04529031 | USt-IdNr.: CZ04529031 | Datenbox: 234baq7

Datenschutz: [privacy@phmarket.cz](mailto:privacy@phmarket.cz) | Allgemeiner Support: [support@phmarket.cz](mailto:support@phmarket.cz)

Website: <https://www.phmarket.cz>

Angesichts der Art und des Umfangs der Verarbeitung ist der Verantwortliche nicht verpflichtet, einen Datenschutzbeauftragten (DSB) gemäß Art. 37 DSGVO zu benennen. Die gesamte Kommunikation in Datenschutzangelegenheiten erfolgt über die dedizierte Adresse [privacy@phmarket.cz](mailto:privacy@phmarket.cz).

## 2. ANWENDUNGSBEREICH UND SCHLÜSSELKONZEPTE

2.1. Geografischer Anwendungsbereich: Die App ist primär für Nutzer aus den EU-Mitgliedstaaten, dem Vereinigten Königreich, Norwegen, Island, Liechtenstein und der Schweiz bestimmt. Bei Nutzung aus einer anderen Jurisdiktion erfolgt die Verarbeitung im Einklang mit der DSGVO.

2.2. Betroffene Person: Sie als natürliche Person, die die App herunterlädt, installiert, ein Konto erstellt oder sie anderweitig nutzt, sei es im Modus "Nutzung ohne Registrierung" oder als registrierter Nutzer.

2.3. Wesentlicher Unterschied zwischen den Modi:

- **Nutzung ohne Registrierung:** Die App funktioniert ohne Erstellung eines Kontos; verfügbar sind die Grundfunktionen (Karte, Preise, Navigation, Quality-Stationen, Fuel Quality im Nur-Lese-Modus). Die verarbeiteten Daten beschränken sich auf technische Gerätekennungen (install\_id, eine von der App generierte UUID), Präferenzeinstellungen (Sprache, Währung) und pseudonymisierte Analysedaten. Dies ist KEIN anonymes Supabase-Konto; ein formales Nutzerkonto in unserer Datenbank (auth.users) wird erst bei der Registrierung erstellt.
- **Registriertes Konto:** Ein vollwertiges Konto einschließlich Name/Spitzname, E-Mail und weiterer Daten, die für die Teilnahme am PHM-Cash-Programm, den PushMe-Dienst,

Community-Preismeldungen, die Erstellung von Community-Stationen, Fuel-Quality-Bewertungen und die Einlösung von Flash Offers erforderlich sind.

### 3. KATEGORIEN VERARBEITETER PERSONENBEZOGENER DATEN

Der Verantwortliche erhebt und verarbeitet die folgenden Kategorien personenbezogener Daten, stets in dem für den konkreten Zweck erforderlichen Umfang und im Einklang mit dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DSGVO:

#### 3.1. Identifikations- und Kontaktdaten (nur registriertes Konto)

- Name oder Spitzname (ein echter bürgerlicher Name ist nicht erforderlich; gespeichert in user\_metadata.nickname oder user\_metadata.first\_name)
- E-Mail-Adresse (kann eine "Relay"-E-Mail aus Apple Hide My Email sein, wenn Sie sich über Sign in with Apple anmelden; in diesem Fall erhalten wir Ihre echte Adresse nicht)
- Apple ID oder Google ID (nur eine vom OAuth-Prozess bereitgestellte interne Kennung, nicht das Passwort zu Ihrem Apple-/Google-Konto)
- Passwort (gespeichert in gehashter Form mittels bcrypt mit Salt in Supabase Auth, niemals im Klartext); nur wenn Sie sich per E-Mail registrieren

#### 3.2. Technische Daten und Gerätekennungen

- install\_id: Eine eindeutige Kennung der App-Installation, die beim ersten Start generiert und lokal gespeichert wird (MMKV). Es handelt sich nicht um eine Systemkennung (IDFA auf iOS / AID auf Android); sie kann nicht für App-übergreifendes Tracking verwendet werden.
- Typ und Modell des Mobilgeräts (z. B. iPhone 15, Samsung Galaxy S24); erfasst über expo-device
- Herstellermarke des Geräts (Apple, Samsung usw.)
- Betriebssystemversion (iOS 18, Android 14 usw.)
- App-Version (app\_version aus expo-application)
- IP-Adresse (anonymisiert; wir speichern nur die ersten drei Oktette, z. B. 192.168.1.\* statt 192.168.1.45, ausschließlich für grobe geografische Analysen)
- Spracheinstellungen und Zeitzone (locale, timezone); aus expo-localization
- Push-Benachrichtigungstoken (Expo Push Token; der Expo Push Service leitet ihn an Apple APNs oder Google FCM weiter)

#### 3.3. Standortdaten

Die App arbeitet mit Ihrer aktuellen Position, um nahegelegene Partnerstationen anzuzeigen, Entfernungen zu berechnen, zu navigieren, das Land für Fuel Quality zu erkennen und den Snap-to-Station-Mechanismus bei Preismeldungen zu betreiben. Die Verarbeitung erfolgt wie folgt:

**Nur-Vordergrund-Tracking:** Die App erhält Ihren Standort ausschließlich, während sie sich im Vordergrund befindet. Wir verfolgen den Standort NICHT im Hintergrund. Beim Schließen der App oder beim Wechsel in den Hintergrund endet die GPS-Subscription (auf Ebene des iOS-/Android-

Betriebssystem). Wir verwenden nur die Vordergrund-Berechtigung (Location.requestForegroundPermissionsAsync in expo-location).

**Standortgenauigkeit:** Wir verwenden eine einheitliche Genauigkeitsstufe, Location.Accuracy.Balanced (etwa ~100 Meter). Wir nutzen nicht die höchste Genauigkeit (High accuracy, ~5 bis 20 Meter), da Balanced für die Funktionalität der App ausreicht.

**Kontinuierliche Erfassung im Vordergrund:** Nach erteilter Einwilligung ruft das Betriebssystem watchPositionAsync mit einem 30-Sekunden-Intervall und einer 50-Meter-Schwelle auf; in unserer App speichern wir einen neuen Zustand nur, wenn sich der Nutzer mehr als 100 Meter bewegt hat oder eine bestimmte Zeit vergangen ist. Der Standort wird also nicht alle 30 Sekunden auf dem Server oder lokal gespeichert; er wird nur für die aktuelle App-Sitzung gespeichert.

**Persistenz des Standorts:** Wir speichern Ihre GPS-Koordinaten nicht dauerhaft auf Servern, außer wenn sie Teil eines konkreten Datensatzes sind (z. B. eine Betankung im PHM-Cash-Programm, eine Community-Preismeldung, die Erstellung einer Community-Station). In diesen Fällen speichern wir nur die mit dem jeweiligen Datensatz verbundenen Koordinaten, keine historische Bewegungspur.

**Erkanntes Land (Cache):** Für die Fuel-Quality-Funktion erkennen wir das Land (CZ/PL/SK/DE/AT/HU) anhand des letzten Standorts und speichern diesen Ländercode lokal in MMKV (fq\_detected\_country). Er dient der automatischen Initialisierung des Fuel-Quality-Bereichs beim nächsten Öffnen, nicht der Profilbildung.

**Snap-to-Station:** Bei der Meldung eines Kraftstoffpreises (Community-Meldung) ruft die App die Funktion find\_nearest\_station(GPS) auf, die Ihren Standort an die nächstgelegene Katalogstation im Umkreis von 25 km "anheftet". Dies ist eine ANTI-SABOTAGE-Maßnahme; ein Preis kann nicht für eine beliebige GPS-Koordinate gemeldet werden, sondern nur für eine existierende Station. Ihr GPS zum Zeitpunkt der Meldung bleibt nicht als Teil des Preises gespeichert; gespeichert wird nur die fuel\_station\_id.

**Widerruf der Standorteinwilligung:** Sie können sie jederzeit in den iOS-/Android-Einstellungen widerrufen. Die App funktioniert auch ohne Standort; sie kann lediglich Stationen nicht nach Entfernung sortieren, nicht navigieren und Preise nicht anheften. Anstelle des aktuellen Standorts wird der vom Betriebssystem zwischengespeicherte "letzte bekannte Standort" verwendet, oder der Nutzer wird aufgefordert, ein Ziel als Text einzugeben.

### 3.4. Fahrzeug- und Fahrerprofildaten

- Kraftstoffart (Natural 95, Diesel, LPG, CNG, AdBlue, HVO, EV)
- Kraftstoffverbrauch (l/100 km oder kWh/100 km)
- Tank- oder Batteriekapazität (bei EVs)
- Fahrzeugtyp (Pkw, leichtes Nutzfahrzeug, Lkw usw.)
- Bevorzugte Währung für die Preisanzeige (CZK, EUR, PLN, HUF, USD)
- Bevorzugte Entfernungseinheit (Kilometer / Meilen)
- Bevorzugte Navigations-App (Apple Maps, Google Maps, Waze, Mapy.cz)

Das Fahrzeugprofil wird sowohl lokal (ein Cache in MMKV unter dem Schlüssel vehicle\_cache für das Stale-while-revalidate-Muster) als auch auf dem Server in user\_metadata zur Synchronisierung zwischen Geräten gespeichert.

**Profilfoto (ausschließlich auf dem Gerät verarbeitet):** Wenn Sie ein Profilfoto festlegen, verkleinert die App es auf 200 x 200 Pixel und speichert es ausschließlich lokal im Speicher Ihres Geräts (documentDirectory). Das Profilfoto wird NIEMALS an die Server des Betreibers oder Dritter gesendet und ist nicht Teil irgendeiner Datenübertragung. Sie entfernen es im App-Profil oder durch Deinstallation der App. Die Fotobibliotheks-Berechtigung wird nur im Moment der Fotoauswahl angefordert und dient ausschließlich diesem Zweck.

### 3.5. Daten über die Aktivität in der App

- Verlauf der in der App besuchten Partnerstationen (Öffnen eines Stationsdetails)
- Im PHM-Cash-Programm erfasster Betankungsverlauf (Datum, Uhrzeit, Partnerstation, Kraftstoffart, Menge, Preis, GPS zum Zeitpunkt der Betankung zur Verifizierung)
- Community-Preismeldungen: Preis, fuel\_station\_id, Kraftstoffart, Zeitstempel, source\_currency, Währung, FX-Kurs
- Erstellte Community-Stationen: Name, Adresse, Stadt, GPS-Koordinaten, creator\_display (ein gekürzter Name aus user\_metadata.display\_name oder dem E-Mail-Präfix)
- Fuel-Quality-Bewertungen: fuel\_station\_id, is\_positive (Boolean), ein optionaler Kommentar (max. 200 Zeichen), eine optionale brand\_suggestion (Markenvorschlag für die Station)
- Rezensionen und Bewertungen von Partnerstationen
- Gefolgte Partnerstationen ("Favoriten")
- Routen und Navigationsanfragen (nur vorübergehend zur Berechnung gespeichert; der Cache recent\_destinations\_v1, FIFO max. 8 Einträge, lokal)
- Easter-Egg-Fortschritt (ee\_station\_detail\_count, ee\_app\_open\_count, ee\_radio\_unlocked, radio\_cooldown\_sent\_at): lokale Zähler zum Freischalten von PusHMe

### 3.6. Daten des PHM-Cash-Programms

Hinweis: Das PHM-Cash-Programm befindet sich zum Zeitpunkt des Inkrafttretens dieser Erklärung in Vorbereitung (coming soon). Die nachstehenden Datenkategorien werden ab dem Start des Programms verarbeitet.

- Stand der PHM-Cash-Punkte und aktuelles Level
- Verlauf des Erwerbs und der Einlösung von Punkten (Transaktionsprotokoll)
- Referral-Kennung (wenn Sie von einem anderen Nutzer eingeladen wurden)
- Bankverbindung: IBAN und Name des Kontoinhabers (nur wenn Sie die jährliche Auszahlung der Geldprämie beantragen; gespeichert nur im Moment der Geltendmachung der Auszahlung, nicht automatisch)
- Contribution Score (ein internes Reputationsscore, typischerweise im Bereich ab -10 aufwärts), verwendet für die automatisierte Moderation (siehe Artikel 4.4 unten, Shadowban und transparente Moderation)

### 3.7. Daten des PusHMe-Dienstes

PusHMe ist ein System verschlüsselter Kurznachrichten auf nutzerdefinierten Frequenzen (1000 bis 9999). Die Verschlüsselung erfolgt auf dem Gerät des Absenders vor dem Senden an den Server. Verarbeitungsdetails:

**Chiffrierschlüssel:** Der Schlüssel wird mittels SHA-256 aus der Zeichenkette 'phmarket:radio:v1:' + der Frequenz abgeleitet (z. B. 'phmarket:radio:v1:4242'). Es handelt sich nicht um ein triviales XOR mit der numerischen Frequenz als Schlüssel, sondern um XOR mit einem 256-Bit-Hash-abgeleiteten Schlüssel. Im Normalbetrieb kann der PHMarket-Server den Inhalt der Nachrichten ohne Kenntnis der Frequenz nicht lesen.

**PLAIN:-Fallback (wichtig):** Wenn die kryptografische API (Crypto.digestStringAsync) auf dem Gerät des Nutzers fehlschlägt, typischerweise auf sehr alten Geräten, verfügt die App über einen Fallback-Modus, in dem sie die Nachricht mit dem Präfix "PLAIN:" im Klartext speichert. In diesem Fall ist der Nachrichteninhalt auch ohne Kenntnis der Frequenz lesbar, und zwar für die Dauer der 30-minütigen Aufbewahrungsfrist. Die Wahrscheinlichkeit dieses Zustands ist in der Praxis gering (ca. <0,5 % der Geräte), wir legen ihn jedoch zur vollständigen Transparenz offen.

- Nachrichtenmetadaten (auf dem Server gespeichert): Sendezeitpunkt, anonymisierte Absenderkennung (die UUID auth.users.id, nicht E-Mail/Name), die Frequenz (numerischer Kanal 1000 bis 9999), optional eine station\_id (Stationskontext)
- Verschlüsselter Nachrichteninhalt: auf dem Server maximal 30 Minuten gespeichert (expires\_at standardmäßig now() + 30 min); danach automatisch und unwiderruflich durch einen Cron-Job gelöscht
- Systemkanäle (101 Live Drops, 111 Kaffee & Essen, 121 Autopflege, 131 Spezial): Nachrichten in Systemkanälen sind KLARTEXT (is\_system=true) und werden vom Betreiber oder von ihm autorisierten Partnern ausgestrahlt. Sie dienen als Marketing-Light-Kanal; das Versenden kommerzieller Mitteilungen in Systemkanälen unterliegt der Einwilligung gemäß § 7 des Gesetzes Nr. 480/2004 Slg. (Einwilligung zu Push-Benachrichtigungen in Profil, Benachrichtigungen)
- Die Liste Ihrer Lieblingsfrequenzen (radio\_listening, max. 5): gespeichert in der Tabelle profiles auf dem Server
- Die Liste blockierter Nutzer auf einzelnen Frequenzen: lokal gespeichert
- Nachrichtenmeldungen (Tabelle radio\_reports): Wenn Sie eine Nachricht melden, bewahren wir zu dieser Meldung den verschlüsselten Inhalt, die Absenderkennung, die Meldekategorie (illegal / harassment / spam / other), die Zeit und Ihre Melder-ID auf; aufbewahrt für 30 Tage ab Abschluss der Prüfung oder 1 Jahr für Zwecke eines etwaigen Rechtsstreits

### 3.8. Analyse- und Diagnosedaten

**PostHog (Produktanalytik):** Um zu verstehen, wie die App genutzt wird, verwenden wir PostHog, Inc. auf einer EU-Instanz (Host: <https://eu.i.posthog.com>). Wir erfassen pseudonymisierte Analyseereignisse: Screen Views, Taps, Navigationsaktionen, Erfolg/Misserfolg von Vorgängen, Easter-Egg-Fortschritt, Performance-Metriken. Die Kennung distinct\_id in PostHog ist bei der Nutzung ohne Registrierung die install\_id (anonym pro Installation) und bei einem registrierten Konto Ihre Supabase user\_id. Es handelt sich also um PSEUDONYMISIERUNG, nicht um vollständige Anonymisierung; der Nutzer wird sitzungsübergreifend konsistent identifiziert, die Kennung kann jedoch für sich genommen nicht ohne einen zusätzlichen Datenpunkt (E-Mail / Name) aus unserer Datenbank zu Ihrer Person zurückverfolgt werden. Beim Abmelden rufen wir posthog.reset() auf; eine neue Sitzung erhält eine neue Identität.

**Sentry (Fehler- und Absturzdiagnostik):** Zur Erkennung und Behebung von Fehlern verwenden wir Sentry (Functional Software, Inc.) auf US-Infrastruktur mit SCCs. Sentry erfasst JavaScript-Fehler, native Abstürze, Stack Traces, Breadcrumbs (erfasste trackEvent-Ereignisse, die an Sentry weitergeleitet werden), Gerätekontext (Modell, OS) und eine pseudonymisierte Nutzerkennung. Die Sentry-Aufbewahrung beträgt 90 Tage.

- Automatisch an Analyseereignisse angehängter Kontext: session\_id, install\_id, device\_model, device\_brand, os\_version, timezone, locale, app\_version, app\_start\_type (cold/warm), push\_permission\_status
- Konkrete Ereignisse: 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 und weitere technische Ereignisse
- Geografische Aggregation für Statistiken: Ihre GPS-Koordinaten werden in analytischen Aggregationen auf ~10-km-Blöcke gerundet (lat\_bucket, lng\_bucket), um geografische Trends zu identifizieren, nicht um einen konkreten Ort zu identifizieren

### 3.9. Daten aus der Kommunikation mit dem Support

- Der Inhalt Ihrer an den Support gesendeten Nachricht (support@phmarket.cz, privacy@phmarket.cz, legal@phmarket.cz, notice@phmarket.cz, csae@phmarket.cz)
- Unsere Antworten und jegliche weitere Kommunikation
- Kommunikationsmetadaten (Zeit, E-Mail-Adresse, Betreff)

## 4. VERARBEITUNGSZWECKE UND RECHTSGRUNDLAGEN

Der Verantwortliche verarbeitet Ihre personenbezogenen Daten nur für festgelegte, ausdrücklich genannte und legitime Zwecke auf Grundlage einer konkreten Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO. Detaillierte Übersicht:

### 4.1. Bereitstellung der Grundfunktionen der App (Karte, Kraftstoffpreise, Navigation, Quality-Stationen, Fuel Quality im Nur-Lese-Modus) für Nutzer ohne Registrierung und registrierte Nutzer.

Rechtsgrundlage: Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO), d. h. Erfüllung der Bedingungen, die den Vertrag darstellen. Daten: technische Gerätedaten, Standortdaten (nur Vordergrund), Präferenzeinstellungen. Aufbewahrung: für die Dauer der Nutzung der App; Präferenzeinstellungen für die Dauer des Kontos oder bis zur Deinstallation.

### 4.2. Verwaltung des registrierten Kontos, Authentifizierung, Passwort-Zurücksetzung.

Rechtsgrundlage: Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO). Daten: Name/Spitzname, E-Mail, gehashtes Passwort, Apple/Google-OAuth-Kennung. Aufbewahrung: für die Dauer des Kontos + 90 Tage nach der Löschung für die Backup-Rotation.

### 4.3. Teilnahme am PHM-Cash-Programm (Punktevergabe, Betankungsaufzeichnungen, Auszahlungen); aktiv ab dem Programmstart, derzeit coming soon.

Rechtsgrundlage: Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO); rechtliche Verpflichtung nach dem

Rechnungslegungsgesetz und den Steuergesetzen (Art. 6 Abs. 1 Buchst. c DSGVO) für Buchhaltungszwecke. Daten: Identifikationsdaten, Betankungsdaten, Level, Punkte, Bankverbindung (IBAN, Kontoinhaber), die IBAN nur bei Geltendmachung einer Auszahlung. Aufbewahrung: für die Dauer der Teilnahme am Programm; Buchhaltungsunterlagen 10 Jahre gemäß Gesetz Nr. 563/1991 Slg.

**4.4. Der PusHMe-Dienst: Senden und Zustellen verschlüsselter Nachrichten zwischen Nutzern, Inhaltsmoderation, Missbrauchsprävention.** Rechtsgrundlage: Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO); berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO) für Moderation und Missbrauchsprävention. Daten: Nachrichtenmetadaten, verschlüsselter Inhalt (oder PLAIN:-Fallback), Absenderkennung, blockierte Nutzer, Meldungen. Aufbewahrung: verschlüsselter/Klartext-Inhalt max. 30 Minuten; Metadaten max. 90 Tage; Meldungen bis zum Abschluss der Prüfung + 1 Jahr.

**4.5. Community-Preismeldungen, Erstellung von Community-Stationen, Rezensionen, Bewertungen von Partnerstationen.** Rechtsgrundlage: Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO); berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO), Betrieb der App und Informationsqualität; Anti-Fraud-Audit (prices\_audit). Daten: Nutzerkennung, creator\_display, Inhalt der Meldung/Station, Zeitstempel, GPS für die Snap-to-Station-Verifizierung (nicht langfristig gespeichert), Anti-Fraud-rate\_limit\_block-Aufzeichnungen. Aufbewahrung: Beiträge für die Dauer des Kontos oder bis zur Löschung des einzelnen Inhalts; Anti-Fraud-Audit 3 Jahre.

**4.6. Fuel-Quality-Bewertungen: Rezensionen (positiv / mit Vorbehalten), Markenvorschläge.** Rechtsgrundlage: Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO) und berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO), Verbraucherinformation über Kraftstoffqualität. Daten: fuel\_station\_id, is\_positive, ein optionaler Kommentar (max. 200 Zeichen), eine optionale brand\_suggestion, Nutzerkennung, Zeit. Aufbewahrung: für die Dauer des Kontos oder bis zur Löschung der einzelnen Bewertung.

**4.7. Veröffentlichung von Bußgeldern der Tschechischen Handelsinspektion (ČOI) im Bereich Fuel Quality.** Rechtsgrundlage: berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO), Verbraucherinformation über öffentlich verfügbare Daten zur Kraftstoffqualität; die Daten stammen aus öffentlich veröffentlichten Entscheidungen der ČOI. Daten: Stationsname, Stadt, Bußgeldjahr, Grund, URL des ČOI-Quelldokuments. Aufbewahrung: solange die Daten relevant sind (aktives Bußgeld) + 3 Jahre.

**4.8. Service-Push-Benachrichtigungen (Kontoänderungen, PHM-Cash-Punkte, Inhaltsmoderation, Statement of Reasons).** Rechtsgrundlage: Vertragserfüllung und berechtigtes Interesse (Art. 6 Abs. 1 Buchst. b und f DSGVO). Daten: Expo Push Token, Daten zu Kontoereignissen. Aufbewahrung: für die Dauer der Nutzung der App.

**4.9. Marketing-Push-Benachrichtigungen, Neuigkeiten, Flash Offers in PusHMe (derzeit inaktiv; werden in künftigen Versionen aktiviert).** Rechtsgrundlage: Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO), erteilt über den Opt-in-Dialog in Profil, Benachrichtigungen. Daten: Expo Push Token, Präferenzen (notif\_nearby, notif\_discount, notif\_loyalty, notif\_quality, notif\_location). Aufbewahrung: bis zum Widerruf der Einwilligung.

**4.10. Produktanalytik (PostHog): Verbesserung der UX, Fehlervermeidung, A/B-Testing.** Rechtsgrundlage: berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO). Dies ist eine wichtige Änderung gegenüber früheren Fassungen dieser Erklärung; die Analytik war ursprünglich an eine

separate Einwilligung im GDPR-Consent-Screen geknüpft; nach einer Überprüfung wurde diese Bedingtheit als unvereinbar mit Art. 7 Abs. 4 DSGVO und den EDPB-Leitlinien 5/2020 (Consent Bundling) bewertet. Die Analytik erfolgt nun auf Grundlage des berechtigten Interesses mit Pseudonymisierung, EU-Hosting und einem einfachen Opt-out in Profil, Datenschutz. Daten: pseudonymisierte Analyseereignisse, install\_id (vor der Registrierung), Supabase user\_id (nach der Registrierung); Gerätekontext (Modell, OS, locale). Aufbewahrung: PostHog 12 Monate; aggregierte anonyme Statistiken unbegrenzt.

**4.11. Fehler- und Absturzdiagnostik (Sentry).** Rechtsgrundlage: berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO). Daten: Stack Trace, Breadcrumbs, pseudonymisierte Geräteerkennung, OS-/App-Version, Gerätekontext. Aufbewahrung: 90 Tage (Sentry-Retention).

**4.12. Betrugsprävention, Verhinderung des Missbrauchs des PHM-Cash-Programms, von PushMe und Flash Offers; automatisierte Moderation einschließlich des Shadowban-Systems (transparent, gemäß Art. 17 DSA).** Rechtsgrundlage: berechtigtes Interesse (Art. 6 Abs. 1 Buchst. f DSGVO); rechtliche Verpflichtung nach dem DSA. Daten: Aktivitätsdaten, contribution\_score, IP-Adresse (anonymisiert), Gerät, prices\_audit-Aufzeichnungen. Aufbewahrung: für die Dauer der Untersuchung + 3 Jahre für einen etwaigen Rechtsstreit.

**4.13. Erfüllung der Pflichten nach dem DSA (Notice-and-Action, Statement of Reasons, interne Beschwerden, Transparenzberichterstattung).** Rechtsgrundlage: rechtliche Verpflichtung (Art. 6 Abs. 1 Buchst. c DSGVO), Verordnung (EU) 2022/2065. Daten: Daten zu Meldungen, Moderationsentscheidungen, Beschwerden, Transparenzberichten. Aufbewahrung: 5 Jahre ab Abschluss der Prüfung.

**4.14. Kommunikation mit dem Support und Beschwerdebearbeitung.** Rechtsgrundlage: Vertragserfüllung und berechtigtes Interesse (Art. 6 Abs. 1 Buchst. b und f DSGVO). Daten: Kommunikationsinhalt, E-Mail-Adresse, Metadaten. Aufbewahrung: 3 Jahre ab dem letzten Kontakt.

**4.15. Erfüllung rechtlicher Verpflichtungen (Buchhaltung, Steuern, AML, Anfragen öffentlicher Stellen).** Rechtsgrundlage: rechtliche Verpflichtung (Art. 6 Abs. 1 Buchst. c DSGVO). Daten: Buchhaltungs- und Steuerdaten einschließlich Bankverbindungen für PHM-Cash-Auszahlungen, Daten zur Erfüllung von Anfragen. Aufbewahrung: 5 bis 10 Jahre nach dem Rechnungslegungsgesetz und den Steuergesetzen.

## 5. AUFBEWAHRUNGSDAUER

5.1. Allgemeiner Grundsatz: Wir bewahren Daten nur für den Zeitraum auf, der zur Erfüllung des jeweiligen Verarbeitungszwecks unbedingt erforderlich ist, und im Einklang mit der Datenminimierung. Nach Ablauf der Aufbewahrungsfrist werden die Daten unwiderruflich gelöscht oder anonymisiert.

5.2. Kontolöschung: Bei der Löschung des Kontos leiten wir folgenden Prozess ein:

- Produktionsdatenbank: 30 Tage ab Bestätigung des Antrags
- Backups: 90 Tage ab Bestätigung des Antrags (Backups werden automatisch rotiert)
- Buchhaltungsunterlagen und Daten für AML- und Steuerzwecke: 5 bis 10 Jahre unabhängig von der Kontolöschung

- Daten im Zusammenhang mit einem laufenden Rechtsstreit/einer Untersuchung: für dessen Dauer + 3 Jahre
- Anonymisierte Daten (aggregierte Statistiken): können unbegrenzt aufbewahrt werden
- PostHog distinct\_id: Wir rufen posthog.reset() beim Abmelden auf; nach der Kontolöschung hat eine neue Sitzung keine Verknüpfung mehr zur user\_id, historische Ereignisse in PostHog, die an die user\_id gebunden sind, verbleiben jedoch innerhalb der 12-monatigen Aufbewahrung; auf einen Löschantrag hin rufen wir auch die PostHog Delete API auf

5.3. Sign in with Apple Revoke (Verpflichtung): Wenn Sie sich über Sign in with Apple angemeldet haben und die Löschung des Kontos beantragen, ruft der Verantwortliche im Rahmen des Löschvorgangs den Apple Sign In REST API revokeToken-Endpunkt auf und widerruft Ihre Refresh- und Access-Tokens bei Apple Inc. Diese Verpflichtung ergibt sich aus der Apple App Store Review Guideline 5.1.1(v); Implementierungsdetails sind im Code-Side-Change-Tracking-Dokument veröffentlicht.

## 6. DATENEMPFÄNGER UND AUFTRAGSVERARBEITER

Wir übermitteln Ihre personenbezogenen Daten an die folgenden Kategorien von Empfängern, stets in dem für den jeweiligen Zweck erforderlichen Umfang und auf Grundlage von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO:

### 6.1. Auftragsverarbeiter (Data Processors)

**Supabase Inc. (USA; Datenbank gehostet in Frankfurt, EU)** Rolle: Hosting der Postgres-Datenbank (auth.users, profiles, stations, prices, radio\_broadcasts, fuel\_stations usw.), Authentifizierung, Echtzeitfunktionen für PusHMe und Community-Preis-Broadcast. Rechtsgrundlage: DPA + SCCs; Daten ausschließlich in der EU-Region (Frankfurt) gespeichert; ISO 27001/SOC 2.

**PostHog, Inc. (USA; EU-Instanz: eu.i.posthog.com)** Rolle: pseudonymisierte Produktanalytik. Rechtsgrundlage: DPA; eine EU-Instanz ohne Übermittlung analytischer Daten in die USA.

**Functional Software, Inc. d/b/a Sentry (USA)** Rolle: Fehler- und Absturzdiagnostik der App. Rechtsgrundlage: DPA + SCCs; Pseudonymisierung von Kennungen; kurze Aufbewahrung (90 Tage).

**Apple Inc. (USA / Irland für EU-Operationen)** Rolle: Zustellung von Push-Benachrichtigungen (APNs); Sign-in-with-Apple-Authentifizierung; App-Store-Distribution. Rechtsgrundlage: Apple Developer Program Agreement + Apple Privacy Policy; Übermittlungsmechanismen gemäß EU-Angemessenheitsbeschluss / DPF.

**Google LLC (USA / Irland für die EU)** Rolle: Zustellung von Push-Benachrichtigungen (FCM); Sign in with Google; Maps API für Kartenkacheln; Google-Play-Distribution. Rechtsgrundlage: Google API Terms + DPA; SCCs / DPF.

**Expo (650 Industries, Inc., USA)** Rolle: der Expo Push Service als Vermittlungsschicht zwischen der App und APNs/FCM; OTA-Updates-Infrastruktur. Rechtsgrundlage: Expo Privacy Policy; der Expo Push Token dient als Proxy für den APNs/FCM-Token; SCCs.

**Resend / Mailgun oder vergleichbar (Anbieter transaktionaler E-Mails)** Rolle: Zustellung transaktionaler E-Mails (Registrierungsbestätigung, Passwort-Zurücksetzung, Kontolöschung). Rechtsgrundlage: DPA + SCCs; minimale Aufbewahrung.

## 6.2. Datenempfänger (Data Recipients)

- Partnerstationen: in begrenztem Umfang bei der Einlösung einer Flash Offer (claim\_code, Zeit, station\_code) oder der Registrierung einer Betankung im PHM-Cash-Programm (eine pseudonymisierte Kennung + Betankungsdaten). Partnerstationen erhalten weder Ihren Namen noch Ihre E-Mail oder Apple/Google ID.
- Die Bank des Betreibers: für die Auszahlung der Geldprämie aus dem PHM-Cash-Programm (IBAN, Name des Kontoinhabers, Betrag); ab dem Start des Programms.
- Steuerverwaltung: wenn eine Auszahlung gesetzliche Meldegrenzen überschreitet.
- Das Buchhaltungsbüro des Betreibers: im Rahmen gewöhnlicher Buchhaltungsvorgänge.
- Rechtsvertreter, Wirtschaftsprüfer: bei der Erfüllung rechtlicher Pflichten.
- Strafverfolgungsbehörden, Gerichte, Aufsichtsbehörden (ÚOOÚ, ČOI, ČTÚ, die DSCs anderer EU-Mitgliedstaaten): auf ordnungsgemäß gestellte Anfrage und im Einklang mit geltendem Recht.
- Das National Center for Missing & Exploited Children (NCMEC) über die Internet Watch Foundation: bei Erkennung von CSAM-/CSAE-Inhalten (Art. 22 der Bedingungen und die CSAE Policy).
- Vertrauenswürdige Hinweisgeber (Trusted Flaggers, Art. 22 DSA): auf Grundlage ihrer Meldungen und in dem für die Ausübung ihrer Befugnisse erforderlichen Umfang.

## 7. INTERNATIONALE DATENÜBERMITTLUNGEN

7.1. Grundsatz der EU-Lokalisierung: Wir betreiben unsere primäre Dateninfrastruktur (die Supabase-Datenbank, die PusHMe-Server) ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR), konkret in Deutschland (Frankfurt). Dort finden keine internationalen Übermittlungen in Drittländer im Sinne der DSGVO statt.

7.2. Übermittlungen in die USA und in Drittländer: Einige Auftragsverarbeiter (Apple, Google, Expo, Sentry, Resend/Mailgun) haben ihren Sitz in den Vereinigten Staaten. Für diese Übermittlungen wenden wir an:

- Standardvertragsklauseln (SCCs) gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission als rechtlichen Mechanismus nach Art. 46 Abs. 2 Buchst. c DSGVO
- Apple und Google: zertifiziert im Rahmen des EU-U.S. Data Privacy Framework (DPF), sofern dieser Mechanismus wirksam ist; alternativ SCCs
- Ergänzende Maßnahmen: Verschlüsselung bei der Übertragung (TLS 1.3) und im Ruhezustand (AES-256); Pseudonymisierung von Kennungen; Minimierung der übermittelten Daten

7.3. Transfer Impact Assessment: Für jede systematische Übermittlung in ein Drittland führen wir ein Transfer Impact Assessment (TIA) gemäß den EDPB-Empfehlungen durch.

## 8. IHRE RECHTE ALS BETROFFENE PERSON

Im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten stehen Ihnen nach der DSGVO die folgenden Rechte zu. Sie können sie jederzeit unter [privacy@phmarket.cz](mailto:privacy@phmarket.cz) oder direkt in der App geltend machen (wo das konkrete Recht dies ermöglicht):

**Auskunftsrecht (Art. 15 DSGVO)** Sie haben das Recht, eine Bestätigung darüber zu erhalten, ob Ihre Daten verarbeitet werden, und falls ja, das Recht auf Auskunft über die Daten und Informationen über die Verarbeitung. Sie können eine Kopie der Daten anfordern, die wir kostenlos bereitstellen (für weitere Kopien ein angemessenes Entgelt).

**Recht auf Berichtigung (Art. 16 DSGVO)** Sie haben das Recht auf Berichtigung unrichtiger Daten. Die meisten Daten können Sie direkt in Profil, Profil bearbeiten in der App ändern.

**Recht auf Löschung (Art. 17 DSGVO)** Sie können die Löschung Ihrer Daten verlangen, vorzugsweise über die Funktion "Konto löschen" in der App (Profil, Einstellungen, Konto löschen), über die Website [phmarket.cz/delete-account](https://phmarket.cz/delete-account) oder per E-Mail an [support@phmarket.cz](mailto:support@phmarket.cz). Die Löschung kann durch die Erfüllung rechtlicher Pflichten eingeschränkt sein (Buchhaltung, AML, DSA-Reporting).

**Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)** Sie können die Einschränkung der Verarbeitung in den Fällen des Art. 18 Abs. 1 DSGVO verlangen.

**Recht auf Datenübertragbarkeit (Art. 20 DSGVO)** Sie haben das Recht, die von Ihnen bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format (JSON) zu erhalten und sie einem anderen Verantwortlichen zu übermitteln.

**Widerspruchsrecht (Art. 21 DSGVO)** Sie haben das Recht, jederzeit Widerspruch gegen eine auf berechtigtem Interesse beruhende Verarbeitung (Art. 6 Abs. 1 Buchst. f) einzulegen. Dies betrifft insbesondere: Produktanalytik (PostHog), Diagnostik (Sentry), Betrugsprävention, Moderation, geografische Aggregation. Sie können den Widerspruch in Profil, Datenschutz, Widerspruch einlegen, oder per E-Mail an [privacy@phmarket.cz](mailto:privacy@phmarket.cz) einreichen. Nach Eingang des Widerspruchs stellen wir die Verarbeitung ein, es sei denn, wir weisen zwingende berechtigte Gründe nach, die Ihre Interessen überwiegen. FÜR DIE PostHog-ANALYTIK: Sie können sich einfach in Profil, Datenschutz, Analytik (ein Schalter) abmelden; nach dem Ausschalten wird PostHog in der App nicht mehr aufgerufen (ein rein clientseitiges Gate).

**Recht, keiner automatisierten Entscheidungsfindung unterworfen zu sein (Art. 22 DSGVO)** Sie haben das Recht, keiner ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung mit erheblichen Auswirkungen unterworfen zu sein. Unsere automatisierte Moderation (Rate Limits, Plausibilitätsprüfungen, der Shadowban auf Grundlage des `contribution_score`) ist NICHT ausschließlich automatisiert; die endgültige Entscheidung über Sanktionen wie einen Shadowban wird von einem Menschen überprüft, und in jedem Fall haben Sie das Recht auf ein Statement of Reasons (Art. 17 DSA) und auf Einreichung einer internen Beschwerde (Art. 20 DSA).

**Recht auf Widerruf der Einwilligung (Art. 7 Abs. 3 DSGVO)** Soweit die Verarbeitung auf einer Einwilligung beruht (Marketing-Push-Benachrichtigungen), können Sie die Einwilligung jederzeit in den App- oder Betriebssystemeinstellungen widerrufen.

**Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO)** In der Tschechischen Republik: das Amt für den Schutz personenbezogener Daten (ÚOOÚ), Pplk. Sochora 27, 170 00 Prag 7, <https://www.uoou.gov.cz>. In anderen EU-Mitgliedstaaten: die Aufsichtsbehörde Ihres Landes des gewöhnlichen Aufenthalts.

**Bearbeitungsfristen:** Anträge bearbeiten wir ohne unangemessene Verzögerung, spätestens innerhalb eines (1) Monats. Die Frist kann um weitere zwei Monate verlängert werden. Die

Bearbeitung ist kostenlos; bei offensichtlich unbegründeten Anträgen ein angemessenes Entgelt oder Ablehnung.

Identitätsprüfung: Zum Schutz Ihrer Rechte behalten wir uns das Recht vor, Ihre Identität vor der Bearbeitung eines Antrags zu überprüfen (typischerweise per E-Mail von der mit dem Konto verknüpften Adresse).

## 9. EINWILLIGUNGEN IN DER APP UND ONBOARDING

Beim ersten Start der App zeigen wir einen einführenden Einwilligungsbildschirm an (den "GDPR-Consent-Screen"). In der aktuellen Fassung 3 dieser Erklärung:

- Einwilligung in die Verarbeitung personenbezogener Daten (BLOCKIEREND): Diese Einwilligung spiegelt wider, dass Sie durch die Annahme der Bedingungen die App nutzen und der Verarbeitung der für die Vertragserfüllung erforderlichen personenbezogenen Daten zustimmen (Art. 6 Abs. 1 Buchst. b DSGVO). Ohne diese Einwilligung kann die App nicht genutzt werden.
- Einwilligung in die Erhebung analytischer Daten (NICHT BLOCKIEREND, Opt-out jederzeit): Die Analytik (PostHog) wird primär auf Grundlage des berechtigten Interesses verarbeitet (Art. 6 Abs. 1 Buchst. f DSGVO). Die Einwilligung auf dem Consent-Screen hat informativen Charakter und gibt Ihnen die Möglichkeit eines anfänglichen Opt-outs. Sie können die Analytik jederzeit später in Profil, Datenschutz, Analytik ausschalten.

Änderung gegenüber früheren Fassungen dieser Erklärung: Frühere Fassungen knüpften die Nutzung der App an die Einwilligung in die Analytik als blockierendes Kontrollkästchen. Nach einer Überprüfung haben wir diese Bedingtheit im Einklang mit Art. 7 Abs. 4 DSGVO und den EDPB-Leitlinien 5/2020 entfernt; eine Einwilligung in die Analytik kann keine gültige Bedingung für die Nutzung eines Dienstes sein, der die Analytik für seine Funktion nicht benötigt.

## 10. COOKIES UND ÄHNLICHE TECHNOLOGIEN

10.1. In der mobilen App: Die App verwendet keine Standard-Web-Cookies. Stattdessen:

- Lokaler MMKV-Gerätespeicher: für Präferenzeinstellungen, die `install_id`, Authentifizierungstoken (verschlüsselt gespeichert), Feature Flags, zwischengespeicherte Daten
- Schlüsselklassifizierung (`lib/dataLifecycle.ts`): `DEVICE_LEVEL_KEYS` (überleben das Abmelden: `install_id`, Sprache, Währung, `push_token`) vs. `USER_LEVEL_KEYS` (werden beim Abmelden gelöscht: Cache, Präferenzen)
- Die von der App generierte `install_id`: zur Identifizierung der Installation in der Analytik; sie ist NICHT die System-IDFA (Apple) oder AAID (Google)
- Der Expo Push Token: für die Zustellung von Push-Benachrichtigungen

10.2. Auf der Website `phmarket.cz`: Wenn Sie unsere Website besuchen (z. B. `phmarket.cz/delete-account`), können wir notwendige technische Cookies gemäß der Cookies Policy auf der Website verwenden.

## 11. SICHERHEIT PERSONENBEZOGENER DATEN

### 11.1. Technische und organisatorische Maßnahmen:

- Verschlüsselung bei der Übertragung: TLS 1.3 für die gesamte Kommunikation mit den Servern; HSTS auf der Website
- Verschlüsselung im Ruhezustand: AES-256 für sensible Daten in der Supabase-Datenbank; bcrypt für das Passwort-Hashing
- PushMe-Verschlüsselung: XOR mit einem SHA-256-abgeleiteten Schlüssel (aus phmarket:radio:v1:Frequenz); der Server sieht den Inhalt im Normalbetrieb nicht, aber ACHTUNG: im Fall des PLAIN:-Fallbacks (Ausfall der Krypto-API auf dem Gerät) wird die Nachricht für die 30-minütige Aufbewahrung im Klartext gespeichert
- Pseudonymisierung von Kennungen in Analysedaten
- Das Least-Privilege-Prinzip für den Datenzugriff; Row-Level Security (RLS) in Supabase
- Regelmäßige Sicherheitsupdates und Infrastruktur-Patching
- Automatisierte Backups mit regelmäßigen Wiederherstellbarkeitstests
- Protokollierung von Sicherheitsereignissen und deren Überwachung (Sentry, Supabase Audit Logs)
- Penetrationstests, Code Review neuen Codes
- Informationssicherheitsrichtlinien und Mitarbeiterschulungen
- Serverseitige Validierung aller RPC-Aufrufe: Rate Limits, Plausibilitätsprüfungen ( $\pm 50$  % des Preismedians), Geofence (25 bis 50 km), Duplikaterkennung (50 m)

11.2. Benachrichtigung über eine Sicherheitsverletzung: Im Fall einer Verletzung, die voraussichtlich ein hohes Risiko für Ihre Rechte zur Folge hat, benachrichtigen wir Sie ohne unangemessene Verzögerung gemäß Art. 34 DSGVO. Schwerwiegende Verletzungen melden wir zudem der ÚOOÚ innerhalb von 72 Stunden gemäß Art. 33 DSGVO.

11.3. Empfehlungen für Sie: Verwenden Sie ein starkes und einzigartiges Passwort; schützen Sie den Zugang zu Ihrer E-Mail; teilen Sie Anmeldedaten nicht; melden Sie jeden Verdacht auf unbefugten Zugriff umgehend an support@phmarket.cz.

## 12. KINDER UND SCHUTZ MINDERJÄHRIGER

12.1. Altersbeschränkung: Die App ist nicht für Kinder unter siebzehn (17) Jahren bestimmt. Die Einstufung Mature 17+ bei Google Play und die Kategorie 18+ im Apple App Store (nach dem ab 2026 wirksamen Altersbewertungssystem von Apple, das die frühere Kategorie 17+ ersetzt hat) beziehen sich auf die PushMe-Funktion (Kommunikation mit unbekanntem Personen).

12.2. Zusicherung des Nutzers: Durch die Nutzung der App erklären Sie, dass Sie mindestens 17 Jahre alt sind.

12.3. CSAE / CSAM: Die App verfolgt eine absolute Nulltoleranz gegenüber Material über sexuellen Kindesmissbrauch (CSAM/CSAE). Die Erkennung erfolgt über Hash-Matching (PhotoDNA/Microsoft / IWF-Hashlisten), Meldeschaltflächen in PushMe und Community-Beiträgen sowie automatisierte Heuristiken. Bei Erkennung wird der Inhalt sofort entfernt, der Nutzer dauerhaft gesperrt, das

NCMEC über die IWF benachrichtigt und die Strafverfolgungsbehörden gemäß Verordnung (EU) 2021/1232 informiert. Kontakt: csae@phmarket.cz.

### **13. ÄNDERUNGEN DIESER ERKLÄRUNG**

Wir können diese Erklärung von Zeit zu Zeit aktualisieren. Über wesentliche Änderungen informieren wir Sie mit angemessenem Vorlauf (mindestens 30 Tage vor dem Wirksamwerden) in der App, per Push-Benachrichtigung oder per E-Mail. Die aktuelle Fassung ist stets in der App und unter [phmarket.cz/privacy-policy](https://phmarket.cz/privacy-policy) verfügbar.

### **14. PLATTFORMSPEZIFISCHE INFORMATIONEN FÜR APPLE (iOS)**

14.1. Privacy Manifests (PrivacyInfo.xcprivacy): Die App enthält ein Privacy Manifest gemäß den Apple App Store Privacy Requirements (wirksam seit Mai 2024). SDKs von Drittanbietern (PostHog 3.x+, Sentry 8.x+) enthalten ebenfalls eigene Privacy Manifests.

14.2. App Tracking Transparency (ATT): Der Verantwortliche betreibt kein Tracking im Sinne des Apple-ATT-Frameworks; kein App-übergreifendes Tracking und keine Weitergabe an Datenhändler. Die App zeigt daher keinen ATT-Prompt an.

14.3. Sign in with Apple: Bei der Anmeldung über Sign in with Apple können Sie "Hide My Email" (eine Apple-Relay-E-Mail) verwenden. Bei der Kontolöschung rufen wir den Apple Sign In REST API revokeToken-Endpunkt auf und widerrufen Ihre Tokens bei Apple. Diese Implementierung ist im Code-Side-Change-Tracking-Dokument veröffentlicht.

14.4. Family Sharing: Wenn Sie die App über Family Sharing teilen, erstellt jedes Familienmitglied ein eigenes Konto mit eigenen Daten.

### **15. PLATTFORMSPEZIFISCHE INFORMATIONEN FÜR GOOGLE (Android)**

15.1. Data-Safety-Formular: Wir haben das Data-Safety-Formular in der Google Play Console gemäß der Google User Data Policy ausgefüllt. Es beschreibt detailliert die Arten der verarbeiteten Daten, die Zwecke und die Weitergabe an Dritte.

15.2. Web-Ressource zur Kontolöschung: Im Einklang mit der Google Play User Data Policy kann die Kontolöschung auch über [phmarket.cz/delete-account](https://phmarket.cz/delete-account) eingeleitet werden, ohne die App zu installieren.

15.3. Sign in with Google: Wir erhalten von Google nur Ihren Namen und Ihre E-Mail-Adresse aus Ihrem Google-Profil.

15.4. Play Integrity API: Zur Missbrauchsprävention verwenden wir (oder werden wir verwenden) die Google Play Integrity API. Das Verdict enthält Signale über die Integrität des Geräts und der App; wir speichern es nur in anonymisierter Form zur Betrugserkennung (Tabelle integrity\_checks, gelesen/geschrieben nur durch die service\_role).

## 16. SO ERREICHEN SIE UNS

Für alle Anfragen, Anträge oder Beschwerden zum Schutz personenbezogener Daten:

PHMarket s.r.o.

Hlavní třída 87/2, 737 01 Český Těšín, Tschechische Republik

IČO: 04529031 | Datenbox: 234baq7

**Datenschutz:** [privacy@phmarket.cz](mailto:privacy@phmarket.cz)

**Allgemeiner Support:** [support@phmarket.cz](mailto:support@phmarket.cz)

**Rechtsangelegenheiten / DSA-Kontaktstelle:** [legal@phmarket.cz](mailto:legal@phmarket.cz)

**DSA Notice-and-Action:** [notice@phmarket.cz](mailto:notice@phmarket.cz)

**Kindersicherheit (CSAE):** [csae@phmarket.cz](mailto:csae@phmarket.cz)

**Website:** <https://www.phmarket.cz>

**Kontolöschung (Web):** <https://www.phmarket.cz/delete-account>

**Aufsichtsbehörde CZ:** Amt für den Schutz personenbezogener Daten (ÚOOÚ), Pplk. Sochora 27, 170 00 Prag 7, Tschechische Republik, <https://www.uoou.gov.cz>, Telefon: +420 234 665 111

*Diese Datenschutzerklärung tritt am 1. Juni 2026 in Kraft und ersetzt alle vorherigen Fassungen.*

*© Copyright 2026 PHMarket s.r.o. Alle Rechte vorbehalten.*