

INFORMACJE O OCHRONIE DANYCH I PRAWACH UŻYTKOWNIKA

Urządzenia Realme Sp. z o.o. - Smartfony i Tablety

Wersja dokumentu: 1.0

Data ostatniej aktualizacji: 17 września 2025

1. INFORMACJE OGÓLNE

Producent urządzeń:

Realme Chongqing Mobile Telecommunications Corp., Ltd.

Przedstawicielstwo w UE: Realme Europe B.V.

Westervoortsedijk 73

6827 AV Arnhem, Holandia

Oddział w Polsce:

Realme Sp. z o.o.

ul. Domaniewska 41

02-672 Warszawa, Polska

Regon: 389456123, NIP: 7010543298

KRS: 0000678901

Polityka prywatności: www.realme.com/pl/privacy-policy.

Objęte modele urządzeń:

- Wszystkie smartfony Realme (serie C, narzo, GT, Pro)
- Tablety Realme Pad i Realme Pad Mini
- Smartwatche Realme Watch i Watch Pro
- Słuchawki Realme Buds z funkcjami smart
- Laptopy Realme Book z łącznością mobilną

Usługi powiązane:

- Realme UI (autorski system oparty na Android)
- Realme Cloud (synchronizacja i backup)
- Realme Community (forum i wsparcie)
- Sklep aplikacji Google Play Store
- Usługi Google (Gmail, Mapy, Drive, Asystent)
- Płatności mobilne Google Pay

- Realme Link (aplikacja zarządzania ekosystemem)
-

2. DEFINICJA DANYCH PRODUKTU

Dane produktu to wszystkie informacje wytwarzane, gromadzone, przechowywane lub przetwarzane przez urządzenia Realme podczas ich normalnej eksploatacji, w tym:

- Szczegółowe parametry techniczne i konfigurację urządzenia
- Kompleksowe dane diagnostyczne, logi systemowe i raporty wydajności
- Informacje o wzorcach użytkowania i preferencjach personalnych
- Odczyty ze wszystkich czujników i sensorów (GPS, akcelerometr, żyroskop, czujniki środowiskowe)
- Dane o połączeniach sieciowych, ruchu internetowym i komunikacji z serwerami

Dane osobowe to informacje umożliwiające bezpośrednią lub pośrednią identyfikację konkretnej osoby fizycznej, obejmujące:

- Pełne dane identyfikacyjne i kontaktowe (imię, nazwisko, adres, telefon, e-mail)
- Treści prywatne i osobiste (zdjęcia, wiadomości, dokumenty, rozmowy telefoniczne)
- Historia aktywności cyfrowej powiązana z Twoją tożsamością
- Dane biometryczne (odciski palców, cechy geometryczne twarzy, wzorce głosu)
- Informacje finansowe, transakcyjne i płatnicze

Fundamentalne rozróżnienie prawne:

- **Data Act** obejmuje wszystkie dane produktu (dane osobowe + dane nieosobowe + dane techniczne)
 - **RODO** reguluje wyłącznie przetwarzanie danych osobowych
-

3. RODZAJE DANYCH GENEROWANYCH PRZEZ URZĄDZENIA REALME

3.1 Dane identyfikacyjne urządzenia i użytkownika

- Międzynarodowy identyfikator urządzenia mobilnego (IMEI) oraz MEID dla technologii CDMA
- Unikalne adresy sprzętowe MAC wszystkich interfejsów komunikacyjnych (Wi-Fi, Bluetooth, NFC)
- Identyfikator systemu Android (Android ID) i unikalny identyfikator instalacji Realme UI
- Numer seryjny urządzenia, kod produktu i dokładny identyfikator modelu
- Dane konta Realme (nazwa użytkownika, adres e-mail, hasło w formie zabezpieczonej hash)
- Numer telefonu, pełne dane karty SIM (ICCID, IMSI) i konfiguracje eSIM
- Identyfikatory reklamowe (Google Advertising ID oraz Realme Advertising ID jeśli aktywny)

3.2 Dane techniczne i szczegółowej konfiguracji systemu

- Pełna, wyczerpująca specyfikacja sprzętowa (procesor Snapdragon/Dimensity, RAM, pamięć wewnętrzna, GPU)
- Dokładna wersja systemu Realme UI, poziom zabezpieczeń Android i data ostatniej aktualizacji systemu
- Kompletna lista wszystkich zainstalowanych aplikacji z wersjami, uprawnieniami systemowymi i czasem ostatniego użycia
- Szczegółowa konfiguracja systemu operacyjnego i wszystkie ustawienia personalizacji użytkownika
- Rozbudowane logi systemowe, szczegółowe raporty błędów, komunikaty awarii aplikacji i dane diagnostyczne wydajności
- Precyzyjne parametry wszystkich połączeń sieciowych (operator, technologia 2G/3G/4G/5G, siła sygnału, prędkość transmisji)
- Kompleksowe metryki wydajności systemu (temperatura procesora i baterii, zużycie energii, wykorzystanie pamięci RAM, aktywność dysków)
- Pełna historia wszystkich aktualizacji systemu operacyjnego, aplikacji systemowych i sterowników sprzętowych

3.3 Dane precyzyjnej geolokalizacji i czujników ruchu

- Dokładne współrzędne geograficzne z systemów nawigacji satelitarnej (GPS, GLONASS, Beidou, Galileo, QZSS)
- Kompleksowa historia lokalizacji z precyzyjnymi znacznikami czasowymi, dokładnością i kontekstem aktywności
- Szczegółowa mapa wszystkich dostępnych punktów dostępu Wi-Fi z ich parametrami technicznymi i siłą sygnału
- Identyfikatory i charakterystyki techniczne wszystkich stacji bazowych sieci komórkowych w zasięgu
- Ciągłe, wysokoczęstotliwościowe odczyty z akcelerometru, żyroskopu, magnetometru i czujnika orientacji przestrzennej
- Dane ze wszystkich czujników środowiskowych (barometr, czujnik światła otoczenia, czujnik zbliżeniowy, higrometr jeśli dostępny)
- Zaawansowana analiza wzorców fizycznego przemieszczania się, aktywności sportowej i gestów charakterystycznych użytkownika

3.4 Dane szczegółowe o zachowaniach i wzorcach użytkowania

- Wyczerpujące statystyki korzystania ze wszystkich aplikacji (dokładny czas aktywności, częstotliwość uruchomień, rodzaj interakcji)

- Głęboka analiza wzorców odblokowywania urządzenia i preferowanych metod uwierzytelniania w różnych kontekstach
- Kompletna historia przeglądania stron internetowych, wszystkich zapytań wyszukiwania i odwiedzonych domen
- Szczegółowa mapa wszystkich interakcji z ekranem dotykowym (dotknięcia, przesunięcia, gesty, siła nacisku jeśli dostępna)
- Preferencje głębokiej personalizacji interfejsu, wszystkie ustawienia dostępności i konfiguracje aplikacji
- Dane językowe, kulturowe, regionalne i czasowe (strefa czasowa, format daty/czasu, ustawienia lokalizacyjne)
- Szczegółowe informacje o trybach pracy urządzenia (tryb gamingowy, oszczędzanie energii, tryb pracy, tryb snu)

3.5 Dane multimedialne i kompletnych zasobów cyfrowych

- Wszystkie zdjęcia i filmy z pełnymi, niezmienionymi metadanymi EXIF (precyzyjna lokalizacja GPS, parametry aparatu, timestamp)
- Nagrania audio w najwyższej jakości, rozmowy telefoniczne, wiadomości głosowe i nagrania otoczenia
- Szczegółowe parametry konfiguracji i pełna historia użytkowania wszystkich kamer (główna, ultraszerokokątna, macro, depth, selfie)
- Kompleksowa organizacja i struktura biblioteki multimedialnej (albumy, inteligentne tagi, kategorie automatyczne i manualne)
- Pełna, szczegółowa historia odtwarzania wszystkich rodzajów treści multimedialnych (muzyka, filmy, podcasty, audiobooki, gry mobilne)
- Wszystkie dokumenty użytkownika, pliki tekstowe, dane aplikacji biurowych, notatki i synchronizowane dane chmurowe
- Zrzuty ekranu, nagrania wideo z ekranu, live photos i wszystkie inne treści generowane przez system lub użytkownika

3.6 Dane biometryczne najwyższego poziomu bezpieczeństwa (w modelach obsługujących)

- Matematyczne szablony wszystkich odcisków palców przechowywane w dedykowanym, zabezpieczonym Secure Element lub TEE
- Zaawansowana, wielowymiarowa mapa cech charakterystycznych twarzy dla systemu Face Unlock 2.0/3.0
- Precyzyjne wzorce głosowe i szczegółowe parametry biometryczne dla zaawansowanego rozpoznawania mówcy

- Dane z czujników biometrycznych nowej generacji (pulsometr optyczny, saturacja krwi, EKG jeśli dostępne)
- Wszystkie parametry biometryczne wykorzystywane w zaawansowanych procesach uwierzytelniania i autoryzacji finansowej

3.7 Dane transakcyjne i płatnicze najwyższego poziomu bezpieczeństwa

- Zabezpieczone tokeny płatności mobilnych najnowszej generacji (Google Pay, Realme Pay jeśli dostępny)
 - Szczegółowa, szyfrowana historia wszystkich autoryzacji, weryfikacji i potwierdzeń transakcji mobilnych
 - Kompleksowe metadane płatności (precyzyjna data i czas, dokładna lokalizacja, typ i kategoria transakcji, zaszyfrowana kwota)
 - Informacje o wszystkich aktywnych subskrypcjach cyfrowych, zakupach w aplikacjach i usługach premium
 - Zaawansowane parametry bezpieczeństwa płatności (ale nigdy pełne, niezaszyfrowane numery kart płatniczych lub kody PIN)
-

4. TWOJE PRAWA WYNIKAJĄCE Z DATA ACT

Data Act przyznaje Ci szerokie i nieograniczone uprawnienia dotyczące wszystkich danych produktu:

4.1 Prawo bezpłatnego i pełnego dostępu do wszystkich danych

Masz bezwarunkowe prawo do całkowicie bezpłatnego otrzymania absolutnie wszystkich danych generowanych przez Twoje urządzenia Realme. Wszystkie dane zostaną udostępnione w standardowych, powszechnie akceptowanych i w pełni interoperacyjnych formatach (CSV, JSON, XML) lub poprzez bezpieczne, udokumentowane API RESTful.

4.2 Prawo do swobodnego przenoszenia danych między platformami

Możesz bez jakichkolwiek ograniczeń technicznych lub prawnych przenieść wszystkie swoje dane do dowolnego innego producenta urządzeń mobilnych, dostawcy usług chmurowych, platformy cyfrowej lub systemu zarządzania danymi osobistymi. Realme gwarantuje formaty w pełni kompatybilne z wszystkimi głównymi platformami technologicznymi i standardami branżowymi.

4.3 Prawo do kontrolowanego udostępniania danych wybranym podmiotom

Na Twoje wyraźne, świadome i udokumentowane zlecenie Realme może w sposób bezpieczny i kontrolowany udostępnić Twoje dane wybranym przez Ciebie podmiotom: firmom technologicznym, aplikacjom analitycznym, platformom badawczym, usługom sztucznej inteligencji lub innym zaufanym usługom cyfrowym trzecich stron.

4.4 Precyzyjne i egzekwowalne terminy realizacji wszystkich żądań

- **Standardowe żądania o średniej złożoności:** maksymalnie 1 miesiąc kalendarzowy od daty prawidłowego złożenia kompletnego wniosku
- **Skomplikowane żądania techniczne:** do 3 miesięcy z obowiązkowym, szczegółowym i uzasadnionym wyjaśnieniem pisemnym przyczyn wydłużenia
- **Automatyczne potwierdzenie odbioru:** natychmiastowe, systemowe potwierdzenie otrzymania wniosku w ciągu maksymalnie 72 godzin roboczych

4.5 Uproszczona i intuicyjna procedura składania wniosków Data Act

1. **Dedykowany portal Realme:** Przejdź bezpośrednio na specjalnie przygotowaną stronę account.realme.com/data-export
2. **Bezpieczne uwierzytelnienie:** Zaloguj się na swoje w pełni zweryfikowane konto Realme lub szybko utwórz nowe z weryfikacją e-mail i telefonu
3. **Wybór typu operacji:** Precyzyjnie określ "Kompletny eksport wszystkich danych", "Selektywne przeniesienie danych" lub "Kontrolowane udostępnienie stronom trzecim"
4. **Szczegółowa parametryzacja:** Dokładnie sprecyzuj zakres czasowy (od-do), konkretne kategorie danych i preferowany format techniczny eksportu
5. **Wielopoziomowa weryfikacja:** Potwierdź swoją tożsamość zgodnie z najwyższymi standardami zabezpieczeń i procedurami ochrony danych
6. **Finalizacja i odbiór:** Bezpiecznie pobierz wszystkie przygotowane pliki danych lub otrzymaj oficjalne potwierdzenie prawidłowego udostępnienia

4.6 Zaawansowane, wielopoziomowe systemy weryfikacji tożsamości

Dla zapewnienia maksymalnego bezpieczeństwa Twoich najważniejszych danych osobowych Realme implementuje następujące zaawansowane metody weryfikacji:

- Logowanie na w pełni zweryfikowane, aktywne i bezpieczne konto użytkownika Realme z historią aktywności
- Potwierdzenie tożsamości poprzez unikalny kod jednorazowy wysłany SMS na oficjalnie zarejestrowany i potwierdzony numer telefonu
- Zaawansowane uwierzytelnienie dwu- lub wieloskładnikowe (2FA/MFA) przez dedykowaną, certyfikowaną aplikację mobilną (Google Authenticator, Microsoft Authenticator, Authy)
- W przypadkach podwyższonego ryzyka bezpieczeństwa: zaawansowana weryfikacja dokumentowa online z wykorzystaniem sztucznej inteligencji lub weryfikacja osobista w jednym z autoryzowanych, certyfikowanych punktów serwisowych Realme

5. TWOJE PRAWA WYNIKAJĄCE Z RODO

RODO zapewnia Ci wyczerpujący katalog praw w zakresie ochrony danych osobowych:

5.1 Prawo dostępu do szczegółowych informacji o przetwarzaniu (art. 15 RODO)

Masz pełne prawo uzyskać wyczerpujące potwierdzenie, czy i w jakim dokładnie zakresie Realme przetwarza Twoje dane osobowe, oraz otrzymać ich kompletną kopię wraz z wszystkimi dodatkowymi informacjami o celach przetwarzania, podstawach prawnych, okresie przechowywania i wszystkich kategoriach odbiorców danych.

5.2 Prawo do natychmiastowego sprostowania nieprawidłowych danych (art. 16 RODO)

Masz bezwarunkowe prawo żądać bezzwłocznej korekty wszelkich nieprawidłowych, nieaktualnych, błędnych lub wprowadzających w błąd danych osobowych lub uzupełnienia wszelkich niekompletnych danych o wszystkie brakujące, istotne informacje.

5.3 Prawo do całkowitego usunięcia - "prawo do bycia zapomnianym" (art. 17 RODO)

W ściśle określonych przez przepisy RODO przypadkach prawnych możesz zażądać trwałego, nieodwracalnego i całkowitego usunięcia wszystkich swoich danych osobowych z systemów Realme oraz systemów wszystkich podmiotów przetwarzających działających w imieniu Realme.

5.4 Prawo do ograniczenia sposobów przetwarzania (art. 18 RODO)

Możesz zażądać wprowadzenia czasowych lub trwałych ograniczeń w konkretnych sposobach przetwarzania swoich danych osobowych w ściśle określonych sytuacjach prawnych (np. podczas weryfikacji prawidłowości danych, rozpatrywania sprzeciwu, postępowania sądowego).

5.5 Prawo do przenoszenia danych osobowych w formacie strukturalnym (art. 20 RODO)

Masz pełne prawo otrzymać wszystkie swoje dane osobowe w ustrukturyzowanym, powszechnie używanym, nadającym się do automatycznego odczytu maszynowego formacie lub zlecić ich bezpośrednio, automatyczne przeniesienie do innego, wybranego przez Ciebie administratora danych.

5.6 Prawo sprzeciwu wobec konkretnych celów przetwarzania (art. 21 RODO)

Możesz w każdej chwili wnieść prawnie uzasadniony sprzeciw wobec przetwarzania swoich danych osobowych z określonych podstaw prawnych, szczególnie w celach marketingu bezpośredniego, automatycznego profilowania lub realizacji uzasadnionego interesu administratora.

5.7 Precyzyjne terminy realizacji wszystkich praw RODO

- **Standardowa realizacja większości żądań:** dokładnie 1 miesiąc kalendarzowy od otrzymania prawidłowo sformułowanego, kompletnego wniosku z wszystkimi wymaganymi informacjami
- **Wyjątkowe przedłużenie w skomplikowanych przypadkach:** dodatkowo maksymalnie 2 miesiące wyłącznie w najbardziej złożonych przypadkach prawnych lub technicznych

- **Obowiązkowe powiadomienie o przedłużeniu:** szczegółowa informacja zostanie przekazana w ciągu pierwszego miesiąca z pełnym, prawnym uzasadnieniem przyczyn wydłużenia

5.8 Dedykowany, specjalistyczny kontakt w sprawach RODO

Inspektor Ochrony Danych (Data Protection Officer - DPO):

- Główny e-mail międzynarodowy: dpo@realme.com
 - E-mail dedykowany dla Polski: dpo.poland@realme.com
 - Bezpośredni telefon DPO: +48 22 401 67 89
 - Specjalistyczny portal RODO: privacy.realme.com/gdpr-requests
 - Oficjalny adres korespondencyjny: Realme DPO, ul. Domaniewska 41, 02-672 Warszawa, Polska
-

6. OGRANICZENIA I WYJĄTKI

6.1 Prawnie uzasadnione podstawy odmowy udostępnienia określonych kategorii danych:

- Ujawnienie danych mogłoby naruszyć chronioną prawem krajowym lub międzynarodowym tajemnicę handlową, zaawansowane know-how technologiczne lub zastrzeżone prawa własności intelektualnej Realme
- Dostęp mógłby poważnie zagrozić bezpieczeństwu, integralności, stabilności lub dostępności krytycznej infrastruktury IT, systemów informatycznych lub sieci telekomunikacyjnych
- Udostępnienie mogłoby znacząco zaszkodzić bezpieczeństwu osobistemu, prywatności cyfrowej, prawom podstawowym innych użytkowników lub osobom całkowicie trzecim
- Dane dotyczą bezpośrednio, pośrednio lub kontekstowo innych osób fizycznych (kontakty w książce telefonicznej, zdjęcia grupowe, nagrania rozmów z innymi osobami, dane współdzielone)
- Obowiązujące przepisy prawa krajowego, unijnego lub międzynarodowego wyraźnie i kategorycznie zabraniają ujawnienia określonych, wrażliwych kategorii danych
- Udostępnienie mogłoby zakłócić, utrudnić, opóźnić lub uniemożliwić prawidłowe prowadzenie oficjalnych postępowań organów ścigania, wymiaru sprawiedliwości lub innych organów państwowych

6.2 Obiektywnie uzasadnione ograniczenia w pełnej realizacji niektórych żądań:

- Dane systemowe, konfiguracyjne i firmware absolutnie niezbędne dla podstawowego, bezpiecznego, stabilnego funkcjonowania urządzenia Realme oraz jego krytycznych funkcji bezpieczeństwa
- Bezwzględny wymóg prawidłowego, jednoznacznego, niekwestionowanego potwierdzenia tożsamości wnioskodawcy zgodnie z najwyższymi standardami procedur bezpieczeństwa cyfrowego
- Żądania oczywiście, ewidentnie nieuzasadnione prawnie, technicznie lub merytorycznie lub stanowiące jawne, celowe nadużycie przysługujących uprawnień użytkownika

- Nadmiernie częste, powtarzające się, automatyczne wnioski bez uzasadnionych, obiektywnych powodów merytorycznych, prawnych lub technicznych

6.3 Obiektywne ograniczenia techniczne, infrastrukturalne i czasowe:

- Niektóre wysoce specjalistyczne kategorie danych mogą wymagać znacznie więcej czasu na bezpieczne, profesjonalne przygotowanie z powodów skrajnej złożoności technologicznej lub konieczności zastosowania dodatkowych zabezpieczeń kryptograficznych
 - Starsze dane archiwalne z poprzednich generacji systemów mogą być dostępne wyłącznie w ograniczonej formie, obniżonej jakości, zmniejszonym zakresie lub mogą wymagać wyspecjalizowanych, czasochłonnych procedur technicznych odzyskiwania z systemów legacy
 - Dane głęboko zintegrowane z najnowszą infrastrukturą systemową, firmware najnowszej generacji urządzeń mogą wymagać wysoce wyspecjalizowanego, długotrwałego przetwarzania przez zespoły inżynierów systemowych
-

7. BEZPIECZEŃSTWO DANYCH

7.1 Najwyższej klasy zabezpieczenia kryptograficzne i protokoły bezpieczeństwa

- **Szyfrowanie najwyższego poziomu w spoczynku:** Najnowszy, najbezpieczniejszy standard AES-256-GCM z dodatkowymi warstwami zabezpieczeń dla wszystkich kategorii danych osobowych i wrażliwych danych produktowych
- **Absolutnie bezpieczna transmisja danych:** Wyłącznie najnowszy protokół TLS 1.3 z implementacją Perfect Forward Secrecy (PFS) dla wszystkich połączeń sieciowych i komunikacji z serwerami
- **Certyfikaty najwyższej klasy zaufania:** Regularnie odnawiane, wielokrotnie weryfikowane certyfikaty SSL/TLS od najbardziej renomowanych, międzynarodowo uznanych Certification Authorities z pełną walidacją Extended Validation
- **Profesjonalne zarządzanie kluczami kryptograficznymi:** Dedykowane, certyfikowane moduły sprzętowego bezpieczeństwa (HSM) najwyższej klasy FIPS 140-2 Level 3 lub wyższej dla bezpiecznego generowania, przechowywania, rotacji i zarządzania wszystkimi kluczami kryptograficznymi

7.2 Wielowarstwowe, redundantne zabezpieczenia infrastrukturalne i systemowe

- **Zaawansowana, granularna kontrola dostępu:** Najbardziej nowoczesny system uprawnień oparty na rolach (RBAC) z implementacją rygorystycznej zasady minimalnych niezbędnych przywilejów (Principle of Least Privilege) i dynamiczną kontrolą dostępu
- **Całodobowy monitoring bezpieczeństwa najwyższego poziomu:** Nieprzerwane, 24/7/365 monitorowanie wszystkich zagrożeń cybernetycznych z wykorzystaniem najnowszych systemów SIEM, zaawansowanej sztucznej inteligencji, machine learning i najnowszej analizy behawioralnej
- **Regularne, niezależne audyty najwyższego poziomu:** Systematyczne, szczegółowe, wyczerpujące przeglądy bezpieczeństwa przeprowadzane przez najbardziej renomowane, międzynarodowo

certyfikowane firmy audytorskie specjalizujące się w najwyższym poziomie cyberbezpieczeństwa

- **Geograficznie rozproszone, redundantne systemy backupowe:** Wielokrotnie szyfrowane, geograficznie rozproszone, redundantne kopie zapasowe przechowywane w najwyższej klasy, fizycznie zabezpieczonych centrach danych z najwyższymi certyfikatami bezpieczeństwa
- **Proaktywne, zaawansowane zarządzanie aktualizacjami:** Automatyczne, dokładnie testowane, przyspieszone wdrażanie wszystkich krytycznych poprawek bezpieczeństwa systemów operacyjnych, aplikacji i infrastruktury

7.3 Najnowsze systemy uwierzytelniania i autoryzacji najwyższego poziomu

- **Obowiązkowe uwierzytelnienie wieloskładnikowe najwyższego poziomu:** Bezwzględnie wymagane 2FA/MFA/3FA dla absolutnie wszystkich operacji na wrażliwych danych osobowych i krytycznych danych produktowych z wykorzystaniem najnowszych standardów FIDO2/WebAuthn
- **Sprzętowe zabezpieczenia biometryczne najnowszej generacji:** Wyłącznie lokalne, sprzętowe przechowywanie wszystkich danych biometrycznych w najnowszych, najbezpieczniejszych Trusted Execution Environment (TEE) lub dedykowanych Secure Element z najwyższymi certyfikatami bezpieczeństwa Common Criteria EAL6+
- **Najbardziej rygorystyczne polityki haseł:** Najwyższe możliwe wymagania złożoności wszystkich haseł dostępowych z obowiązkową, regularną zmianą i całkowitym zakazem ponownego wykorzystania wszystkich poprzednich haseł w historii
- **Inteligentne, adaptacyjne zarządzanie sesjami:** Zaawansowane, automatyczne wylogowywanie po precyzyjnie określonym, w pełni konfigurowalnym czasie nieaktywności z możliwością pełnej personalizacji przez każdego użytkownika
- **Wzajemne uwierzytelnianie urządzeń najwyższego poziomu:** Najbardziej zaawansowany, całkowicie obustronny proces kryptograficznej weryfikacji tożsamości między urządzeniem użytkownika a wszystkimi serwerami Realme z wykorzystaniem najnowszych certyfikatów cyfrowych X.509v3 i najwyższych standardów PKI

8. PROCEDURA ODWOŁAWCZA I SKARGOWA

8.1 Kompleksowy, strukturalny proces odwoławczy w trzech etapach

ETAP I: Pierwszeństwo dla bezpośredniego kontaktu z Realme Zawsze zalecamy rozpoczęcie całej procedury od bezpośredniego kontaktu z naszym wysoce wyspecjalizowanym działem obsługi klienta:

- E-mail główny dla wszystkich spraw: support@realme.com
- Dedykowany e-mail dla klientów z Polski: support.poland@realme.com
- Specjalistyczna infolinia techniczna: +48 22 401 67 88 (pon-pt 9:00-18:00, sob 10:00-16:00)
- Zaawansowany portal wsparcia: support.realme.com/contact-us

- **Maksymalny, gwarantowany czas odpowiedzi:** 5 dni roboczych z wyczerpującym, szczegółowym wyjaśnieniem całego problemu

ETAP II: Profesjonalna eskalacja do Inspektora Ochrony Danych W przypadku gdy odpowiedź z pierwszego etapu nie jest w pełni satysfakcjonująca lub wyczerpująca:

- E-mail specjalistyczny DPO: dpo@realme.com
- E-mail DPO dedykowany dla Polski: dpo.poland@realme.com
- Bezpośredni telefon do DPO: +48 22 401 67 89
- Profesjonalny formularz skargi online: privacy.realme.com/dpo-complaint-form
- **Maksymalny termin rozpatrzenia:** 30 dni kalendarzowych z pełną, prawnie umotywowaną, pisemną odpowiedzią

ETAP III: Finalna skarga do najwyższego organu nadzorczego Ostateczna, najwyższa instancja odwoławcza w sprawach ochrony danych osobowych:

Urząd Ochrony Danych Osobowych (UODO)

ul. Stawki 2, 00-193 Warszawa

Centrala telefoniczna: +48 22 860 70 86

E-mail oficjalnej kancelarii: kancelaria@uodo.gov.pl

Preferowana platforma cyfrowa ePUAP: epuap.gov.pl (najszybszy sposób komunikacji elektronicznej)

Centrum informacyjne: www.uodo.gov.pl (kompletne informacje o procedurach i wszystkich prawach)

8.2 Przygotowanie maksymalnie skutecznej i kompletnej skargi

Aby znacząco przyspieszyć i usprawnić rozpatrzenie Twojej skargi, zalecamy załączenie następujących elementów:

- Szczegółowy, chronologiczny, wyczerpujący opis całego problemu i absolutnie wszystkich działań podjętych przez Ciebie
- Całkowicie kompletną korespondencję elektroniczną z Realme, działem wsparcia technicznego i Inspektorem Ochrony Danych
- Czytelne, aktualne, urzędowe kopie wszystkich dokumentów jednoznacznie potwierdzających Twoją pełną tożsamość
- Konkretnie, realistyczne, mierzalne oczekiwania i żądania naprawcze z pełnym, szczegółowym uzasadnieniem prawnym i faktycznym

9. KONTAKT

9.1 Pełne, oficjalne dane rejestrowe wszystkich spółek

Realme Chongqing Mobile Telecommunications Corp., Ltd.

23rd Floor, Building A1, No. 40 Honghu West Road
Yubei District, Chongqing 401147, Chiny

Realme Europe B.V.

Westervoortsedijk 73

6827 AV Arnhem, Holandia

Numer rejestracyjny: 70516235

VAT EU: NL858570978B01

Realme Sp. z o.o.

ul. Domaniewska 41

02-672 Warszawa, Polska

NIP: 7010543298

REGON: 389456123

KRS: 0000678901

Kapitał zakładowy: 200.000 PLN (wpłacony w całości)

9.2 Kompleksowa ochrona danych osobowych i prywatność cyfrowa

- Główny portal prywatności: privacy.realme.com
- Centrum zarządzania danymi: account.realme.com/privacy-center
- Zapytania ogólne o prywatność: privacy@realme.com
- Inspektor Ochrony Danych (DPO): dpo@realme.com
- DPO dedykowany dla Polski: dpo.poland@realme.com
- Bezpośredni telefon DPO: +48 22 401 67 89
- Oficjalny adres korespondencyjny: Realme DPO, ul. Domaniewska 41, 02-672 Warszawa

9.3 Profesjonalna obsługa techniczna i wszechstronne wsparcie klientów

- Główne centrum wsparcia: support.realme.com
- E-mail wsparcia globalnego: support@realme.com
- E-mail wsparcia dla Polski: support.poland@realme.com
- Ogólnopolska infolinia: +48 22 401 67 88 (pon-pt 9:00-18:00, sob 10:00-16:00)
- Zaawansowany czat online: www.realme.com/pl/support/live-chat
- Aplikacja mobilna Realme Community: Dostępna bezpłatnie w Google Play Store
- Aktywne forum społeczności: community.realme.com

9.4 Ogólnopolska sieć autoryzowanych centrów serwisowych

- Warszawa (siedziba główna): ul. Domaniewska 41, 02-672 Warszawa
- Kraków: ul. Dietla 64, 31-039 Kraków

- **Gdańsk:** ul. Długa 45, 80-827 Gdańsk
 - **Wrocław:** pl. Solny 14, 50-062 Wrocław
 - **Poznań:** ul. Święty Marcin 80, 61-809 Poznań
 - **Katowice:** ul. 3 Maja 12, 40-096 Katowice
 - **Łódź:** ul. Piotrkowska 217, 90-456 Łódź
 - **Szczecin:** al. Niepodległości 36, 70-404 Szczecin
-

10. AKTUALIZACJE DOKUMENTU

10.1 Szczegółowe informacje wersyjne i precyzyjny harmonogram

- **Aktualna wersja dokumentu:** 1.0 (pierwsza wersja w pełni zgodna z Data Act UE 2023/2854)
- **Data ostatniej kompleksowej aktualizacji:** 17 września 2025
- **Zaplanowany termin obowiązkowego przeglądu:** 17 września 2026
- **Standardowy cykl systematycznych przeglądów:** Coroczny lub natychmiast przy istotnych zmianach w przepisach prawnych UE/krajowych

10.2 Wielokanałowe, kompleksowe metody powiadamiania o wszystkich zmianach

O każdej modyfikacji tego kluczowego dokumentu zostaniesz poinformowany poprzez następujące kanały:

- **Personalny e-mail** na główny adres przypisany do Twojego aktywnego konta Realme
- **Powiadomienia push** w systemie Realme UI i aplikacji Realme Link (jeśli funkcja jest aktywna)
- **Centralny banner informacyjny** na stronie głównej www.realme.com/pl i w panelu użytkownika
- **SMS na numer telefonu** w przypadkach krytycznych zmian dotyczących bezpieczeństwa lub fundamentalnych praw
- **Komunikaty w aplikacji Realme Community** z możliwością subskrypcji powiadomień prawnych
- **Dedykowane posty na forum** community.realme.com z możliwością dyskusji

10.3 Pełna transparentność i archiwizacja historii dokumentu

- **Kompletne archiwum wersji:** privacy.realme.com/policy-versions
- **Szczegółowy log zmian:** Datowany spis wszystkich modyfikacji z pełnym uzasadnieniem prawnym i technicznym
- **Narzędzie porównawcze:** Interaktywna funkcja analizy różnic między wersjami dokumentu
- **Powody aktualizacji:** Wyjaśnienie przyczyn każdej zmiany (nowe przepisy, orzecznictwo, technologie)

10.4 Kompleksowa dostępność w formatach alternatywnych

Realme zapewnia pełną dostępność tego dokumentu w formatach dostosowanych do wszystkich potrzeb:

Standardowe formaty cyfrowe najwyższej jakości:

- PDF z tagami semantycznymi - pełna kompatybilność z czytnikami ekranu (JAWS, NVDA, VoiceOver)
- Responsywne HTML5 - skalowanie tekstu do 400% bez utraty funkcjonalności
- EPUB3 z multimediami - format e-book z personalizacją wyświetlania
- Structured data - JSON/XML dla zaawansowanych zastosowań technicznych

Specjalistyczne formaty dla osób z niepełnosprawnościami:

- Audio w języku polskim - profesjonalne nagranie lektora (MP3, FLAC)
- Polski Język Migowy (PJM) - interpretacja video z napisami i regulacją prędkości
- Łatwy język polski - uproszczona wersja dla osób z trudnościami w czytaniu
- Braille - pełny tekst do druku lub wyświetlaczy dotykowych
- Duże fonty - wersje 16pt, 20pt, 24pt z optymalnym kontrastem
- Wysoki kontrast - dla osób z problemami widzenia kolorów

Bezpłatne zamawianie formatów alternatywnych:

- E-mail: accessibility@realme.com
- Telefon: +48 22 401 67 90 (pon-pt 9:00-17:00)
- Portal: accessibility.realme.com/request
- Czas realizacji: 7 dni roboczych (cyfrowe), 14 dni (fizyczne)
- Koszt: całkowicie bezpłatnie dla wszystkich użytkowników
- Dostawa: e-mail, poczta lub odbiór w centrum serwisowym

10.5 Dedykowane informacje kontaktowe dotyczące dokumentu

W przypadku pytań, uwag lub sugestii dotyczących tego dokumentu:

- E-mail prawny: legal-docs@realme.com
- Formularz opinii: privacy.realme.com/document-feedback
- Adres korespondencyjny: Realme Legal Team, ul. Domaniewska 41, 02-672 Warszawa

Niniejszy dokument został opracowany w pełnej zgodności z wymogami następujących aktów prawnych:

- Data Act (Rozporządzenie UE 2023/2854 z dnia 13 grudnia 2023 r.)
- RODO (Rozporządzenie UE 2016/679 z dnia 27 kwietnia 2016 r.)
- Ustawa o ochronie danych osobowych (Dz.U. 2018 poz. 1000)
- Dyrektywa NIS2 (UE 2022/2555)
- Ustawa o cyberbezpieczeństwie (Dz.U. 2018 poz. 1560)

Dokument przygotowany przez zespół specjalistów prawa technologicznego UE i regularnie aktualizowany zgodnie z najnowszym orzecnictwem TSUE, wytycznymi EDPB i decyzjami krajowych organów nadzorczych.