POLITYKA PRYWATNOŚCI SERWISU WSPOLNOTY.APP

Wersja 1.1 (październik 2026 r.) - ogólne zasady przetwarzania danych osobowych oraz wykorzystywania pamięci przeglądarki (cookies) w usłudze wspolnoty.app. Stan prawny i techniczny: 4 października 2026 r.

Niniejszy dokument określa zasady przetwarzania danych osobowych oraz stosowania mechanizmów pamięci przeglądarki (w tym plików cookies, pamięci lokalnej i powiadomień Push) w ramach platformy teleinformatycznej wspolnoty.app, obejmującej Panel Zarządcy, Panel Serwisowy oraz Portal Mieszkańca. Serwis został zaprojektowany w sposób realizujący zasadę prywatności w fazie projektowania (Privacy by Design) oraz domyślnej ochrony danych (Privacy by Default) zgodnie z art. 25 RODO.

§ 1. Dwie odrębne role Usługodawcy w ochronie danych

Korzystanie z platformy wspolnoty.app wiąże się z przetwarzaniem danych w dwóch niezależnych reżimach prawnych:

1. **Administrator Danych Osobowych (ADO)** - Usługodawca (OP-KOM) pełni rolę Administratora Danych w odniesieniu do danych kont użytkowników logujących się do serwisu (pracowników zarządców, mieszkańców, kont serwisowych), danych logowania, sesji, dziennika zdarzeń (audit log), bezpieczeństwa sieciowego oraz korespondencji ze wsparciem technicznym. Niniejsza Polityka Prywatności w pełni reguluje te procesy.

2. **Podmiot Przetwarzający (Procesor)** - w odniesieniu do danych wprowadzonych do bazy Konta Klienta przez Zarządcę lub Wspólnotę Mieszkaniową (takich jak ewidencja kartotek lokali, salda księgowe, rozliczenia mediów, treści uchwał, struktura własnościowa) Administratorem Danych jest Klient (Wspólnota Mieszkaniowa lub Zarządca - Wariant A/B Regulaminu). Usługodawca przetwarza te dane wyłącznie na podstawie Umowy Powierzenia Przetwarzania Danych. W sprawach dotyczących danych ewidencji lokatorskiej mieszkańcy kierują wnioski bezpośrednio do swojego Zarządcy.

§ 2. Administrator danych osobowych i kontakt

1. Administratorem danych osobowych użytkowników serwisu jest:

OP-KOM Przedsiębiorstwo Produkcyjno Handlowo Usługowe Robert Poźniak

ul. Klonowa 6A/8, 11-400 Kętrzyn

NIP: 7421048077, REGON: 510388541

2. Kontakt w sprawach ochrony danych osobowych:

dedykowany adres e-mail ds. RODO: **rodo@wspolnoty.app**

adres e-mail do zgłoszeń ogólnych i wsparcia: **serwis@wspolnoty.app**

adres korespondencyjny: ul. Klonowa 6A/8, 11-400 Kętrzyn

3. Inspektor Ochrony Danych: z uwagi na skalę i charakter prowadzonej działalności Usługodawca nie ma prawnego obowiązku wyznaczenia Inspektora Ochrony Danych (art. 37 RODO). Nadzór nad prawidłowością przetwarzania danych sprawuje bezpośrednio właściciel firmy - Robert Poźniak.

§ 3. Zakres stosowania polityki i grupy osób

Niniejsza Polityka Prywatności ma zastosowanie do następujących kategorii osób:

1. **Użytkownicy Panelu Zarządcy** - osoby fizyczne upoważnione przez Klienta (zarządcy, administratorzy, księgowi) posiadające konta w formacie nazwa@konto.

2. **Użytkownicy Portalu Mieszkańca** - właściciele lokali, najemcy oraz mieszkańcy korzystający z portalu po aktywacji konta (login w formie adresu e-mail).

3. **Użytkownicy Kont Serwisowych** - personel techniczny Usługodawcy wykonujący czynności utrzymaniowe i serwisowe.

4. **Osoby kontaktujące się z Usługodawcą** - osoby składające zapytania ofertowe, wnioski o założenie Konta, zgłoszenia techniczne lub reklamacje.

§ 4. Kategorie przetwarzanych danych i ich źródła

Zakres przetwarzanych danych osobowych wynika bezpośrednio ze specyfiki technicznej platformy wspolnoty.app:

1. **Dane konta użytkownika** - adres e-mail, nazwa użytkownika, imię i nazwisko, rola i uprawnienia w systemie, przypisane wspólnoty i lokale, status aktywności, data utworzenia konta oraz identyfikator podmiotu zakładającego. Źródło: administrator Klienta (dla pracowników) lub samodzielna rejestracja po zaproszeniu (dla mieszkańców).

2. **Dane logowania i bezpieczeństwa** - kryptograficzny skrót hasła (system nigdy nie przechowuje haseł w postaci jawnej), data ostatniej zmiany hasła, daty udanych i nieudanych logowań, szyfrowany sekret TOTP dla uwierzytelniania dwuskładnikowego (2FA), kody odzyskiwania dostępu, znaczniki zaufanych urządzeń, znaczniki znanych przeglądarek (podstawa powiadomienia o logowaniu z nowej przeglądarki).

3. **Dane sesji i identyfikatory sieciowe** - unikalny token sesji, adres IP, nagłówek przeglądarki (User-Agent), znacznik czasu ostatniej aktywności.

4. **Dziennik zdarzeń (audit log)** - szczegółowy zapis operacji wykonywanych w serwisie (logowanie, zmiana danych, generowanie wydruków, eksporty, modyfikacje kartotek) obejmujący identyfikator użytkownika, czas zdarzenia, adres IP oraz metadane zdarzenia. Dziennik stanowi trwały materiał dowodowy archiwizowany w niezależnym archiwum audytu.

5. **Ustawienia i preferencje** - subskrybowane kategorie ostrzeżeń systemowych, data zapoznania się z informacjami o nowościach w programie, wybrany motyw interfejsu (jasny/ciemny, przechowywany wyłącznie w przeglądarce).

6. **Powiadomienia Push** - unikalny identyfikator subskrypcji nadany przez przeglądarkę internetową (Web Push API) po wyrażeniu dobrowolnej zgody przez użytkownika Portalu Mieszkańca.

7. **Korespondencja wsparcia technicznego** - treść zgłoszeń, załączniki oraz historia korespondencji prowadzonej przez kanały e-mail lub formularze zgłoszeniowe.

8. **Logi serwerowe i tunelu sieciowego** - adres IP, czas nadejścia żądania, adres URL, kod odpowiedzi HTTP oraz parametry transmisji rejestrowane przez serwer WWW oraz infrastrukturę brzegową Cloudflare.

§ 5. Cele przetwarzania i podstawy prawne (RODO)

Przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 RODO, zgodnie z poniższym zestawieniem:

Tabela 1. Cele przetwarzania, podstawy prawne i kategorie danych

Cel przetwarzania	Podstawa prawna (RODO)	Kategorie przetwarzanych danych
Świadczenie usługi SaaS, obsługa Konta i udostępnienie funkcji panelu i portalu	Art. 6 ust. 1 lit. b (wykonanie umowy z Klientem) oraz lit. f (uzasadniony interes - umożliwienie pracownikom i mieszkańcom dostępu do serwisu)	Dane konta, dane logowania, zakres uprawnień, powiadomienia e-mail
Zapewnienie bezpieczeństwa teleinformatycznego, ochrona kont (2FA), zapobieganie nadużyciom, prowadzenie dziennika zdarzeń	Art. 6 ust. 1 lit. f (uzasadniony interes Administratora) oraz lit. c w zw. z art. 32 RODO (obowiązek zapewnienia bezpieczeństwa)	Dane logowania, adresy IP, tokeny sesji, logi serwera, dziennik zdarzeń, kody 2FA, powiadomienia e-mail o zdarzeniach bezpieczeństwa konta (zmiana hasła, wyłączenie 2FA, zmiana adresu e-mail, logowanie z nowej przeglądarki)
Wykazanie rozliczalności (zapis akceptacji Regulaminu, Cennika i Umowy Powierzenia)	Art. 6 ust. 1 lit. c (obowiązek prawny) oraz lit. f (obrona przed roszczeniami)	Dane konta, daty akceptacji, identyfikator użytkownika, adres IP
Obsługa zgłoszeń technicznych, reklamacji i korespondencji ze wsparciem	Art. 6 ust. 1 lit. b (realizacja umowy) oraz lit. f (uzasadniony interes - obsługa klienta)	Imię, nazwisko, e-mail, treść zgłoszenia, historia korespondencji
Wysyłka powiadomień Push w przeglądarce (Portal Mieszkańca)	Art. 6 ust. 1 lit. a (dobrowolna zgoda wyrażona w przeglądarce)	Identyfikator subskrypcji Web Push API
Dochodzenie roszczeń, obrona przed roszczeniami oraz rozliczenia podatkowe	Art. 6 ust. 1 lit. c (przepisy podatkowe) oraz lit. f (uzasadniony interes - ochrona prawna)	Dane rozliczeniowe, ewidencja umów, dziennik zdarzeń

§ 6. Odbiorcy danych i podprocesorzy

Dane osobowe przetwarzane w ramach serwisu powierzane są wyłącznie podmiotom zapewniającym odpowiednie standardy bezpieczeństwa, zgodnie z wykazem zawartym w Umowie Powierzenia Przetwarzania Danych:

1. **OP-KOM Przedsiębiorstwo Produkcyjno Handlowo Usługowe Robert Poźniak (Polska, EOG)** - hosting aplikacji i baz danych, utrzymanie środowiska SaaS. Główna infrastruktura serwerowa i bazy danych wspolnoty.app znajdują się na terytorium Rzeczypospolitej Polskiej.

2. **Cloudflare, Inc. (San Francisco, USA)** - tunel sieciowy, ochrona brzegu przed atakami DDoS, optymalizacja dostępu (CDN). Serwery brzegowe rozmieszczone są globalnie, w tym w EOG.

3. **cyber_Folks S.A. (Poznań, Polska)** - wysyłka powiadomień e-mail z aplikacji (serwer SMTP w ramach usług hostingowych). Umowa powierzenia przetwarzania danych osobowych stanowiąca część warunków świadczenia usług cyber_Folks S.A., obowiązująca od rozpoczęcia korzystania z usług

hostingowych przez OP-KOM (hosting resellerski nieprzerwanie od lutego 2021 r.). Brak transferu poza EOG.

4. **Klient (Zarządca / Wspólnota)** - administrator Konta ma dostęp do dziennika zdarzeń w zakresie działań wykonywanych przez jego pracowników i upoważnionych użytkowników w ramach przydzielonego Konta.

5. **Uprawnione organy państwowe** - dane mogą zostać udostępnione organom ścigania lub sądom wyłącznie na podstawie bezwzględnie obowiązujących przepisów prawa.

§ 7. Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)

Główna baza danych serwisu oraz kopie zapasowe przechowywane są wyłącznie na terytorium Polski i nie opuszczają EOG. Przekazywanie danych do państwa trzeciego dotyczy wyłącznie dostawcy infrastruktury brzegowej Cloudflare, Inc. (USA) i odbywa się w oparciu o Standardowe Klauzule Umowne (SCC) przyjęte przez Komisję Europejską oraz decyzję wykonawczą Komisji w sprawie ram ochrony danych UE-USA (EU-US Data Privacy Framework).

§ 8. Okresy przechowywania danych (retencja)

Dane osobowe przechowywane są wyłącznie przez okres niezbędny do realizacji celów, dla których zostały zebrane:

Tabela 2. Okresy przechowywania danych

Kategoria danych	Okres przechowywania	Zasada usunięcia
Konto użytkownika (zarządcy / mieszkańca)	Przez czas istnienia Konta Klienta oraz 60 dni Okresu Przejściowego po rozwiązaniu umowy (z opcją płatnego przedłużenia do 12 miesięcy)	Bezpowrotne, automatyczne usunięcie bazy Konta i kont użytkowników po upływie Okresu Przejściowego
Aktywne sesje logowania	Do wylogowania lub wygaśnięcia sesji z powodu braku aktywności (limit ustawiony na Koncie Klienta)	Automatyczne czyszczenie wygasłych sesji
Zaufane urządzenia (2FA)	30 dni od oznaczenia urządzenia jako zaufane; krócej, gdy użytkownik zmieni hasło albo ponownie skonfiguruje 2FA	Automatyczne wygaśnięcie znacznika zaufania
Znane przeglądarki (powiadomienie o logowaniu z nowej przeglądarki)	365 dni od ostatniego logowania w danej przeglądarce	Automatyczne wygaśnięcie znacznika zapisanego w przeglądarce użytkownika
Kody tymczasowe (2FA, reset hasła, wybór Konta)	5 minut od wygenerowania	Automatyczne unieważnienie po upływie czasu
Dziennik zdarzeń (audit log) i archiwum audytu	Przez okres trwania Umowy z Klientem oraz okres przedawnienia roszczeń (6 lat od końca roku obrotowego)	Przechowywanie w trwałym archiwum audytu w celu wykazania rozliczalności
Protokoły usunięcia Konta	3 lata od dnia sporządzenia protokołu	Archiwizacja do celów dowodowych
Logi techniczne serwera i Cloudflare	30 dni od zarejestrowania	Nadpisywanie w cyklu rotacji logów
Korespondencja wsparcia technicznego	3 lata od dnia zamknięcia zgłoszenia	Usuwanie ze skrzynek Usługodawcy

§ 9. Prawa osób, których dane dotyczą

1. Każdej osobie, której dane dotyczą, przysługują następujące prawa wynikające z RODO:

a) **prawo dostępu do danych (art. 15 RODO)** - uzyskanie potwierdzenia, czy dane są przetwarzane, oraz otrzymanie ich kopii;

b) **prawo do sprostowania danych (art. 16 RODO)** - poprawienie nieprawidłowych lub uzupełnienie niekompletnych danych;

c) **prawo do usunięcia danych, „prawo do bycia zapomnianym" (art. 17 RODO)** - żądanie usunięcia danych w przypadkach określonych w przepisach;

d) **prawo do ograniczenia przetwarzania (art. 18 RODO)** - wstrzymanie operacji na danych z wyjątkiem ich przechowywania;

e) **prawo do przenoszenia danych (art. 20 RODO)** - otrzymanie danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (JSON/XML);

f) **prawo do sprzeciwu (art. 21 RODO)** - wobec przetwarzania opartego na prawnie uzasadnionym interesie;

g) **prawo do cofnięcia zgody** - w odniesieniu do powiadomień Push w Portalu Mieszkańca, w dowolnym momencie, w ustawieniach przeglądarki lub portalu.

2. Wnioski dotyczące danych konta należy kierować na adres **rodo@wspolnoty.app**. W przypadku danych wprowadzonych do bazy przez Zarządcę (np. wysokość zaliczek, stany liczników, dane kartoteki lokalu) mieszkaniec składa wniosek bezpośrednio do swojego Zarządcy (Wspólnoty). Usługodawca niezwłocznie przekazuje wnioski spływające do serwisu właściwemu Klientowi.

3. Każdej osobie przysługuje również prawo wniesienia skargi do organu nadzorczego: Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, www.uodo.gov.pl.

§ 10. Obowiązek podania danych

Podanie adresu e-mail oraz nazwy użytkownika jest wymogiem umownym i warunkiem koniecznym do założenia i obsługi Konta w serwisie wspolnoty.app. Brak tych danych uniemożliwia logowanie, obsługę uwierzytelniania dwuskładnikowego (2FA) oraz procedurę resetowania hasła. Podanie imienia i nazwiska pracowników jest wymagane przez Klienta w celu zapewnienia pełnej rozliczalności działań w dzienniku zdarzeń.

§ 11. Zautomatyzowane podejmowanie decyzji i profilowanie

Dane osobowe przetwarzane w serwisie wspolnoty.app nie podlegają profilowaniu ani zautomatyzowanemu podejmowaniu decyzji wywołującemu skutki prawne w rozumieniu art. 22 RODO. Mechanizmy automatycznej blokady konta lub adresu IP po serii nieudanych prób logowania stanowią wyłącznie środki bezpieczeństwa technicznego (ograniczanie liczby żądań, ochrona przed zgadywaniem haseł).

§ 12. Pliki cookies i pamięć przeglądarki

1. Serwis wspolnoty.app nie wykorzystuje plików cookies analitycznych, reklamowych ani pochodzących od zewnętrznych dostawców śledzących. Wszystkie wpisy w pamięci przeglądarki mają charakter wyłącznie techniczny i są niezbędne do świadczenia usługi żądanej przez użytkownika (art. 399 ustawy Prawo komunikacji elektronicznej). Z tego względu serwis nie wyświetla baneru z prośbą o zgodę na przechowywanie cookies na urządzeniu użytkownika.

2. Użytkownik może w każdej chwili wyczyścić pliki cookies oraz pamięć lokalną w ustawieniach swojej przeglądarki. Skutkiem usunięcia będzie konieczność ponownego zalogowania się do serwisu oraz ponownego przejścia weryfikacji 2FA, a kolejne logowanie zostanie potraktowane jak logowanie z nowej przeglądarki (powiadomienie e-mail). Wpisy stosowane przez serwis zestawia Tabela 3.

Tabela 3. Pliki cookies i pamięć przeglądarki

Nazwa wpisu	Rodzaj mechanizmu	Cel stosowania	Czas życia	Moment powstania
_administrator_key	Cookie (szyfrowane, HttpOnly, Secure, SameSite=Lax)	Identyfikacja sesji zalogowanego użytkownika, ochrona przed atakami CSRF, zapamiętanie wybranego Konta	Do zamknięcia przeglądarki lub wylogowania; nieaktywna sesja wygasa wg limitu Konta	Wejście na stronę logowania
_administrator_trusted_device	Cookie (podpisane, HttpOnly, Secure)	Pominięcie drugiego składnika uwierzytelniania (2FA) na zapamiętanym urządzeniu	30 dni	Zaznaczenie opcji „zapamiętaj to urządzenie" przy 2FA
_administrator_known_device	Cookie (podpisane, HttpOnly, Secure, SameSite=Lax)	Rozpoznanie przeglądarki, z której konto już się logowało, w celu wysłania powiadomienia e-mail o logowaniu z nowej przeglądarki; zawiera wyłącznie skróty identyfikatorów kont i nie daje dostępu do konta	365 dni od ostatniego logowania	Udane logowanie
phx:theme	Pamięć lokalna przeglądarki (localStorage)	Zapamiętanie wybranego motywu interfejsu (jasny/ciemny)	Do wyczyszczenia pamięci przeglądarki	Przełączenie motywu w aplikacji
Subskrypcja Push	Web Push API (przeglądarka)	Dostarczanie powiadomień w Portalu Mieszkańca	Do cofnięcia zgody	Wyrażenie zgody na powiadomienia

§ 13. Środki bezpieczeństwa technicznego i organizacyjnego

W celu zabezpieczenia przetwarzanych danych osobowych Usługodawca stosuje odpowiednie środki techniczne i organizacyjne:

1. **Szyfrowanie transmisji danych** - połączenia szyfrowane protokołem TLS.

2. **Bezpieczeństwo haseł i sekretów** - kryptograficzne skróty haseł oraz szyfrowanie sekretów 2FA w bazie danych.

3. **Uwierzytelnianie dwuskładnikowe (2FA)** - dostępne dla każdego użytkownika, oparte na standardzie TOTP oraz kodach jednorazowych przesyłanych e-mailem.

4. **Izolacja danych** - logiczne i architektoniczne odseparowanie baz danych poszczególnych Klientów.

5. **Kopie zapasowe** - regularne, szyfrowane kopie zapasowe przechowywane w bezpiecznej lokalizacji w Polsce.

6. **Ochrona brzegowa** - filtrowanie ruchu i ochrona przed atakami DDoS przy użyciu infrastruktury Cloudflare.

§ 14. Zmiany Polityki Prywatności

Usługodawca zastrzega sobie prawo do aktualizacji niniejszej Polityki Prywatności w przypadku zmian w przepisach prawa, rozwoju funkcji serwisu wspolnoty.app lub zmian w infrastrukturze technicznej. Aktualna wersja dokumentu jest zawsze dostępna pod adresem wspolnoty.app/polityka-prywatnosci oraz w formie pliku PDF pod adresem wspolnoty.app/polityka-prywatnosci/pdf.