# POLITYKA PRYWATNOŚCI I RODO HUMANLOCK360

Wersja 3.1 • obowiązuje od 19 października 2026 r.

Najważniejsza zasada prywatności HumanLock360 Premium
Analiza komunikatów podczas rozmowy odbywa się lokalnie na urządzeniu. HumanLock360 nie nagrywa, nie archiwizuje ani nie przesyła audio lub pełnego tekstu rozmowy na swoje serwery. Do statystyk mogą być przekazywane wyłącznie wykryte zakazane słowa lub frazy w formie anonimowej, niepowiązanej z kontem użytkownika.

## §1. Administrator danych osobowych

1. Administratorem danych osobowych związanych z korzystaniem z serwisu HumanLock360, HumanLock360 Premium oraz HumanLock360 SOS jest:

- Money Protection Prosta Spółka Akcyjna
- ul. Zawady 159, 15-697 Białystok
- NIP: 9662201481 • REGON: 540661462 • KRS: 0001149343
- e-mail: biuro@humanlock360.pl

2. W sprawach dotyczących danych osobowych i prywatności można kontaktować się z Administratorem pod adresem: biuro@humanlock360.pl.

3. Administrator przetwarza dane zgodnie z obowiązującymi przepisami prawa, w szczególności z RODO, stosując zasadę minimalizacji danych.

## §2. Zakres Polityki

Polityka dotyczy:

- HumanLock360 Premium - płatnej usługi ochronnej, obejmującej funkcje ochrony przed potencjalnymi oszustwami telefonicznymi oraz zintegrowany Moduł HumanLock360 SOS;
- HumanLock360 SOS - oddzielnej, bezpłatnej aplikacji bezpieczeństwa i wsparcia;
- strony internetowej humanlock360.pl, procesu zakupu, płatności, formularzy kontaktowych, reklamacji i obsługi użytkownika.

## §3. Analiza rozmów w HumanLock360 Premium

1. HumanLock360 Premium analizuje podczas aktywnego połączenia określone komunikaty w celu rozpoznawania słów, zwrotów i poleceń odpowiadających wzorcom bezpieczeństwa. W aktualnej wersji funkcja wymaga włączenia trybu głośnomówiącego.

2. Rozpoznawanie mowy i analiza komunikatów odbywają się lokalnie na urządzeniu użytkownika, przy użyciu lokalnego modelu. W tym procesie nie jest wykorzystywane zewnętrzne API rozpoznawania mowy ani zewnętrzne API AI.

3. HumanLock360 w ramach tej funkcji:

- nie nagrywa rozmów telefonicznych;
- nie zapisuje i nie archiwizuje audio rozmowy;
- nie przesyła żadnego fragmentu audio rozmowy na backend HumanLock360;
- nie przesyła pełnej treści ani tekstu rozmowy na backend;
- nie tworzy archiwum rozmów po zakończeniu połączenia.

4. Jeżeli lokalny mechanizm wykryje słowo lub frazę oznaczoną w zasobach systemu jako zakazaną lub ryzykowną, sama wykryta fraza może zostać przesłana jako anonimowa statystyka. Statystyka ta nie jest powiązana z kontem użytkownika i służy ocenie działania oraz rozwoju mechanizmów bezpieczeństwa.

5. Zasoby wzorców zostały przygotowane i wyselekcjonowane na podstawie ponad 50 metod i scenariuszy oszustw. Wykrycie wzorca jest sygnałem ostrzegawczym i nie oznacza stwierdzenia, że rozmówca jest oszustem lub dopuścił się czynu zabronionego.

## §4. Baza numerów potencjalnie niebezpiecznych

1. HumanLock360 Premium korzysta z prywatnej, rozwijanej bazy numerów telefonów oznaczonych jako potencjalnie niebezpieczne, uciążliwe lub wymagające zwiększonej ostrożności.

2. Baza może obejmować m.in. numery związane ze spamem telefonicznym, telemarketingiem, nękaniem, próbami wyłudzeń, podszywaniem się pod banki lub instytucje, phishingiem telefonicznym, próbami wyłudzenia kodów BLIK lub danych, fałszywymi ofertami, automatycznymi połączeniami oraz innymi zgłoszonymi zagrożeniami.

3. Numery mogą pochodzić ze zgłoszeń użytkowników, legalnie dostępnych źródeł oraz wewnętrznych procedur analizy i weryfikacji Administratora. Oznaczenie numeru ma charakter ostrzegawczy, a nie rozstrzygający.

## §5. Dane konta i identyfikacja użytkownika

W związku z kontem i dostępem do usługi Administrator przetwarza w szczególności:

- numer telefonu - backend HumanLock360;
- identyfikator konta - backend HumanLock360;
- dane techniczne automatycznie przetwarzane przez Firebase Authentication w zakresie działania tej usługi.
- Administrator nie wymaga w ramach podstawowego konta imienia i nazwiska ani adresu e-mail, chyba że użytkownik poda je w innym procesie, np. zakupie, reklamacji, kontakcie lub danych do dokumentu księgowego.

## §6. 30-dniowy bezpłatny dostęp Premium

1. Prawo do jednorazowego 30-dniowego bezpłatnego dostępu jest weryfikowane na podstawie numeru telefonu.

2. Na backendzie zapisywane są informacje potrzebne do obsługi trialu, w tym numer telefonu oraz data rozpoczęcia i data zakończenia bezpłatnego okresu.

3. Jeżeli dany numer telefonu wykorzystał już jednorazowy okres bezpłatny, ponowne uruchomienie trialu dla tego samego numeru nie będzie możliwe.

## §7. HumanLock360 SOS i osoby zaufane

1. Funkcje SOS są dostępne jako moduł zintegrowany z Premium oraz w oddzielnej bezpłatnej aplikacji HumanLock360 SOS.

2. Użytkownik samodzielnie wskazuje osoby zaufane. Dane kontaktowe i numery osób zaufanych są przechowywane na backendzie HumanLock360 w zakresie niezbędnym do działania funkcji.

3. Funkcja „Powiadom Bliskich” może wykorzystać lokalizację urządzenia po udzieleniu odpowiednich uprawnień. Lokalizacja SOS nie jest przesyłana do backendu HumanLock360; jest wykorzystywana do przygotowania i wysłania wiadomości SMS do wskazanej osoby bliskiej.

4. Treść komunikatu SMS, w tym komunikat „Potrzebuję pomocy”, jest generowana lokalnie na urządzeniu.

5. Administrator nie zapisuje historii treści wiadomości SOS. Firebase Analytics może rejestrować anonimowe zdarzenie polegające na kliknięciu przycisku SOS, bez własnych parametrów identyfikujących treść wiadomości lub lokalizację.

## §8. Dane techniczne i logi

1. Logi techniczne aplikacji nie są przesyłane do własnego backendu HumanLock360; mogą być przechowywane lokalnie na telefonie.

2. Model telefonu i wersja systemu nie są zbierane przez własny backend HumanLock360, jednak określone dane techniczne mogą być automatycznie przetwarzane przez usługi Firebase, w szczególności Crashlytics i Analytics, zgodnie z ich standardowym działaniem.

3. Administrator nie wykorzystuje własnego identyfikatora urządzenia/aplikacji do opisanych wyżej procesów, z zastrzeżeniem identyfikatorów technicznych, które mogą być automatycznie tworzone lub przetwarzane przez wykorzystywane usługi Firebase.

## §9. Usługi Firebase

Aplikacja wykorzystuje usługi Google Firebase w następującym zakresie:

| Usługa | Zakres / cel |
|---|---|
| Firebase Authentication | Uwierzytelnianie użytkownika; numer telefonu oraz dane techniczne automatycznie przetwarzane przez usługę. |
| Firebase App Check | Ochrona aplikacji i backendu przed nieautoryzowanymi klientami; standardowe dane techniczne wymagane przez usługę. |
| Firebase Analytics | Nazwy zdarzeń bez własnych parametrów, m.in. kliknięcia przycisków menu SOS, oraz dane automatycznie zbierane przez Firebase Analytics. |
| Firebase Crashlytics | Raporty awarii i podstawowe dane diagnostyczne, w tym dane o urządzeniu/systemie potrzebne do diagnostyki błędów. |
| Firebase Cloud Messaging | Dostarczanie powiadomień push, w tym powiadomień kierowanych według topicu. |

## §10. Dane dotyczące płatności i Premium

1. W związku z zakupem i aktywacją HumanLock360 Premium na backendzie mogą być przechowywane:

- data rozpoczęcia i zakończenia Premium;
- identyfikator zamówienia lub transakcji;
- wybrany pakiet;
- kwota i status płatności.

2. Do realizacji płatności wymagany może być również adres e-mail oraz informacja o wybranym wariancie płatności. Dane te są przetwarzane w zakresie niezbędnym do realizacji transakcji.

3. Płatności mogą być obsługiwane przez Przelewy24 / PayPro S.A. Jeżeli dane instrumentu płatniczego są wprowadzane bezpośrednio w systemie operatora płatności, Money Protection nie otrzymuje pełnego numeru karty ani danych uwierzytelniających do bankowości.

## §11. Formularze na stronie, korespondencja, reklamacje i faktury

1. Na stronie humanlock360.pl dostępne są dwa formularze:

- „Kontakt” - imię i nazwisko, adres e-mail, temat i treść wiadomości oraz, opcjonalnie, nazwa firmy lub instytucji;

- „Zgłoś numer” - numer, z którego dzwoniono, opis zdarzenia oraz, opcjonalnie, data i godzina połączenia, informacja, za kogo podawał się dzwoniący, adres e-mail do kontaktu i załącznik (zrzut ekranu lub nagranie).

2. Dane z formularzy są przetwarzane na podstawie zgody wyrażonej w formularzu: w celu odpowiedzi na wiadomość, a w przypadku formularza „Zgłoś numer” także w celu weryfikacji zgłoszenia i ewentualnego oznaczenia numeru w bazie, o której mowa w §4.

3. Po kliknięciu przycisku wysyłania treść formularza, wraz z ewentualnym załącznikiem, jest przesyłana przez usługę FormSubmit (formsubmit.co, operator: Devro LABS), która przekazuje ją e-mailem na adres biuro@humanlock360.pl. Według informacji dostawcy treść zgłoszeń może być przechowywana w tej usłudze do 30 dni, a załączniki nie są w niej przechowywane.

4. Dane przekazane dobrowolnie w korespondencji lub reklamacji są przetwarzane w celu obsługi sprawy.

5. Jeżeli użytkownik żąda wystawienia faktury lub innego dokumentu księgowego, Administrator przetwarza dane wymagane przepisami prawa.

6. Użytkownik powinien przekazywać wyłącznie dane niezbędne do załatwienia sprawy.

## §12. Cele i podstawy prawne

| Cel | Podstawa |
|---|---|
| utworzenie i obsługa konta, trial, Premium i funkcje SOS | art. 6 ust. 1 lit. b RODO - wykonanie umowy / działania przed zawarciem umowy |
| zakup i obsługa płatności | art. 6 ust. 1 lit. b RODO |
| obowiązki podatkowe i księgowe | art. 6 ust. 1 lit. c RODO |
| reklamacje i obsługa roszczeń | art. 6 ust. 1 lit. b, c lub f RODO - zależnie od sprawy |
| bezpieczeństwo, zapobieganie nadużyciom i diagnostyka | art. 6 ust. 1 lit. f RODO - prawnie uzasadniony interes Administratora |
| odpowiedź na wiadomość z formularza „Kontakt” i obsługa zgłoszenia z formularza „Zgłoś numer” | art. 6 ust. 1 lit. a RODO - zgoda wyrażona w formularzu |
| utrzymanie strony internetowej i jej bezpieczeństwo (logi serwera) | art. 6 ust. 1 lit. f RODO - prawnie uzasadniony interes Administratora |
| statystyki odwiedzin strony (Google Analytics) | art. 6 ust. 1 lit. a RODO - zgoda wyrażona w banerze cookies |
| działania wymagające zgody | art. 6 ust. 1 lit. a RODO |

Jeżeli podstawą przetwarzania jest zgoda, może ona zostać wycofana w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

## §13. Odbiorcy danych

Dane mogą być udostępniane podmiotom wspierającym Administratora wyłącznie w zakresie niezbędnym do danego celu, w szczególności:

- Google/Firebase - w zakresie wykorzystywanych usług Authentication, App Check, Analytics, Crashlytics i Cloud Messaging;
- Vercel Inc. - hosting strony humanlock360.pl;
- FormSubmit (Devro LABS) - przekazywanie wiadomości z formularzy na stronie na adres e-mail Administratora;

- Google Ireland Limited - Google Analytics na stronie (wyłącznie po zgodzie) oraz odtwarzacz YouTube (wyłącznie po kliknięciu w film);
- operatorowi płatności Przelewy24 / PayPro S.A.;
- dostawcom hostingu, infrastruktury IT, poczty elektronicznej i bezpieczeństwa;
- podmiotom świadczącym obsługę księgową lub prawną;
- organom publicznym - jeżeli obowiązek przekazania danych wynika z prawa.

## §14. Okres przechowywania

- dane konta - przez okres korzystania z konta, a następnie przez okres niezbędny do rozliczeń, obowiązków prawnych lub ochrony przed roszczeniami;
- dane trialu - przez okres konieczny do weryfikacji jednorazowego charakteru 30-dniowego dostępu oraz ochrony przed nadużyciami;
- dane Premium i transakcji - przez okres świadczenia usługi oraz wymagany do rozliczeń i ochrony przed roszczeniami;
- dokumentacja księgowa - przez okres wynikający z przepisów podatkowych i rachunkowych;
- reklamacje, korespondencja i wiadomości z formularzy na stronie - przez okres obsługi sprawy i dalszy okres uzasadniony ochroną przed roszczeniami;
- dane w usługach Firebase - zgodnie z konfiguracją Administratora, funkcją danej usługi i zasadami retencji właściwymi dla wykorzystywanej usługi;
- logi serwera strony - przez okres wynikający z ustawień dostawcy hostingu;
- dane statystyczne Google Analytics - zgodnie z ustawieniem przechowywania danych w Google Analytics, nie dłużej niż 14 miesięcy;
- audio i pełna treść analizowanych rozmów - nie są przechowywane przez Administratora.

## §15. Strona humanlock360.pl i pliki cookies

1. Strona humanlock360.pl nie wykorzystuje cookies reklamowych. Czcionki i obrazy strony są pobierane z jej własnego serwera, dlatego samo przeglądanie strony nie wysyła danych do Google.

2. Stronę utrzymuje Vercel Inc. (hosting). Serwer automatycznie zapisuje w logach dane techniczne potrzebne do wyświetlenia strony i zapewnienia jej bezpieczeństwa, np. adres IP, datę i godzinę, adres odwiedzanej podstrony oraz rodzaj przeglądarki.

3. Statystyki Google Analytics są uruchamiane wyłącznie po zgodzie wyrażonej w banerze cookies. Zgodę można w każdej chwili wycofać za pomocą odnośnika „Ustawienia cookies” w stopce strony.

4. Odtwarzacz YouTube jest ładowany dopiero po kliknięciu w film.

5. Szczegółowe informacje znajdują się w Polityce Cookies HumanLock360.

## §16. Przekazywanie danych poza EOG

Niektórzy dostawcy technologiczni mogą przetwarzać dane w państwach poza Europejskim Obszarem Gospodarczym, w szczególności w USA. Google LLC i Vercel Inc. uczestniczą w programie EU-U.S. Data Privacy Framework, dla którego Komisja Europejska stwierdziła odpowiedni stopień ochrony danych. W pozostałych przypadkach, jeżeli dochodzi do takiego transferu, Administrator korzysta z podstaw i zabezpieczeń przewidzianych w RODO, odpowiednich dla danego dostawcy i usługi.

## §17. Prawa użytkownika

W przypadkach przewidzianych przez RODO użytkownik ma prawo do:

- dostępu do danych i uzyskania ich kopii;
- sprostowania danych;

- usunięcia danych;
- ograniczenia przetwarzania;
- przenoszenia danych;
- wniesienia sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie;
- wycofania zgody, jeżeli przetwarzanie odbywa się na podstawie zgody.

Wnioski dotyczące realizacji praw należy kierować na: biuro@humanlock360.pl.

## §18. Skarga do Prezesa UODO

Jeżeli użytkownik uważa, że jego dane są przetwarzane niezgodnie z prawem, ma prawo wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych.

## §19. Uprawnienia urządzenia

W zależności od używanej funkcji aplikacja może wymagać dostępu m.in. do telefonu, SMS, lokalizacji, wybranych kontaktów lub numerów, internetu i powiadomień. Użytkownik może zarządzać uprawnieniami w ustawieniach urządzenia. Odmowa uprawnienia może uniemożliwić działanie funkcji, która z niego korzysta.

## §20. Bezpieczeństwo i automatyczne reakcje

1. Administrator stosuje środki techniczne i organizacyjne mające ograniczać ryzyko nieuprawnionego dostępu, utraty, zmiany, ujawnienia lub zniszczenia danych.

2. HumanLock360 Premium może automatycznie reagować na wykryty wzorzec bezpieczeństwa, np. komunikatem wizualnym, sygnałem ostrzegawczym lub - zgodnie z funkcjonalnością systemu - zakończeniem bieżącego połączenia.

3. Automatyczna reakcja ma charakter prewencyjny i nie jest decyzją stwierdzającą popełnienie oszustwa przez rozmówcę.

## §21. Dobrowolność podania danych

Podanie danych jest co do zasady dobrowolne, jednak niektóre dane są niezbędne do utworzenia konta, uruchomienia trialu lub Premium, realizacji funkcji SOS, zakupu, płatności, wystawienia dokumentu księgowego albo rozpatrzenia reklamacji. Brak wymaganych danych może uniemożliwić skorzystanie z danej funkcji.

## §22. Zmiany Polityki

Polityka może być aktualizowana w szczególności w przypadku zmian funkcjonalności HumanLock360, architektury technicznej, dostawców usług, sposobu przetwarzania danych lub przepisów prawa. Aktualna wersja będzie publikowana na stronie humanlock360.pl.

## §23. Kontakt

Money Protection Prosta Spółka Akcyjna
ul. Zawady 159, 15-697 Białystok
NIP: 9662201481 • REGON: 540661462 • KRS: 0001149343
biuro@humanlock360.pl