POLITYKA PRYWATNOŚCI

MIDAR RENT

Platforma marketplace wynajmu pojazdów

Wersja 1.0 | Maj 2025 | Obowiązuje od dnia publikacji

1. Administrator danych osobowych

Administratorem Twoich danych osobowych w rozumieniu art. 4 pkt 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) jest:

Dane administratora	
Firma / nazwa	MIDAR Dariusz Gregorczyk
NIP	7962321248
REGON	140529462
Adres rejestrowy	ul. Mleczna 33, 26-617 Radom, Polska
Kontakt w sprawach RODO	kontakt@midar.rent (dedykowany adres dla żądań związanych z ochroną danych)
Platforma	midar.rent

MIDAR RENT jest **operatorem marketplace** – technologicznym pośrednikiem pomiędzy najemcami a wynajmującymi (partnerami prywatnymi i biznesowymi). MIDAR **nie jest stroną umowy najmu** zawieranej pomiędzy użytkownikami platformy. Rola MIDAR ogranicza się do udostępnienia infrastruktury technicznej, obsługi płatności za pośrednictwem Stripe Connect oraz zapewnienia bezpieczeństwa transakcji.

2. Zakres zbieranych danych osobowych

Zbieramy wyłącznie dane niezbędne do działania platformy, realizacji usług i wypełnienia obowiązków prawnych. Poniższa tabela przedstawia pełen katalog kategorii danych przetwarzanych przez MIDAR RENT.

Kategoria	Konkretne dane	Dotyczy
Dane konta (podstawowe)	Imię, nazwisko, adres e-mail, numer telefonu, hasło (wyłącznie jako hash bcrypt – nigdy w postaci jawnej), zdjęcie profilowe (avatar), data urodzenia, preferowany język interfejsu, status konta (aktywne/zawieszone/usunięte)	Wszyscy użytkownicy
Dane adresowe i tożsamości	Adres zamieszkania/siedziby, kod pocztowy, miasto, kraj. Numer PESEL – wyłącznie w ramach historycznego przepływu weryfikacji tożsamości (legacy flow); aktualnie ograniczony do przypadków wymaganych prawem.	Użytkownicy indywidualni
Dane firmowe	Nazwa firmy, NIP, REGON, numer KRS, numer VAT-UE (dla firm zagranicznych), adres siedziby/oddziału, dane osoby kontaktowej (imię, nazwisko, stanowisko), firmowy adres e-mail i numer telefonu.	Partnerzy biznesowi
Dane transakcyjne	Historia rezerwacji (ID, daty, pojazdy, kwoty, status), dane płatnicze (tokeny Stripe, ostatnie 4 cyfry karty, typ instrumentu płatniczego – pełne dane kart NIE są przechowywane przez MIDAR), historia wypłat (payoutów), historia zwrotów (refundów), historia sporów (dispute history), faktury i dokumenty księgowe.	Wszyscy aktywni użytkownicy
Dane komunikacyjne	Wiadomości przesyłane w wewnętrznym czacie platformy, załączniki do wiadomości, zgłoszenia	Wszyscy użytkownicy

	do działu wsparcia (support tickets), ujawnione dane kontaktowe po opłaceniu rezerwacji (contact reveal – patrz pkt 2.1 poniżej).	
Dane techniczne i bezpieczeństwa	Adres IP, user-agent przeglądarki/aplikacji, fingerprint urządzenia, pliki cookies i localStorage, logi zdarzeń logowania (login events), lista zaufanych urządzeń (trusted devices), jednorazowe kody OTP (wyłącznie hash, nie wartość), logi bezpieczeństwa i logi audytowe (audit logs), scoring ryzyka logowania.	Wszyscy użytkownicy

2.1 Mechanizm ujawnienia danych kontaktowych (Contact Reveal)

Po dokonaniu opłacenia rezerwacji platforma automatycznie ujawnia najemcy i wynajmującemu wzajemne dane kontaktowe (numer telefonu i/lub adres e-mail) niezbędne do realizacji najmu. **Ujawnione dane są zapisywane w historii czatu** i przechowywane przez okres wskazany w sekcji 6 (Retencja danych). Podstawą prawną tego przetwarzania jest art. 6 ust. 1 lit. b RODO (wykonanie umowy). Użytkownik akceptuje ten mechanizm, przystępując do realizacji rezerwacji.

2.2 Numer PESEL – uwaga szczególna

Numer PESEL jest przetwarzany wyłącznie w ograniczonym, historycznym przepływie weryfikacji tożsamości. **MIDAR zobowiązuje się do minimalizacji zakresu przetwarzania PESEL** i docelowej eliminacji tego pola z nowych przepływów rejestracyjnych. Podstawą prawną jest art. 6 ust. 1 lit. c RODO w zw. z obowiązkami wynikającymi z przepisów o przeciwdziałaniu praniu pieniędzy (AML) lub – w zakresie wykraczającym poza obowiązek prawny – zgoda użytkownika (art. 6 ust. 1 lit. a RODO).

2.3 Dane, których nie zbieramy

MIDAR RENT nie zbiera i nie przetwarza danych szczególnych kategorii (art. 9 RODO), takich jak dane o stanie zdrowia, przekonaniach religijnych, przynależności rasowej czy danych biometrycznych, chyba że użytkownik samodzielnie umieści takie informacje w polach tekstowych (np. wiadomościach na czacie). W takim przypadku MIDAR nie ponosi odpowiedzialności za dobrowolne udostępnienie tych danych.

3. Cele przetwarzania i podstawy prawne

Każda czynność przetwarzania danych osobowych przez MIDAR RENT opiera się na jednej z dopuszczalnych podstaw prawnych przewidzianych w art. 6 RODO. Poniżej przedstawiamy pełny katalog celów i odpowiadających im podstaw prawnych.

Cel przetwarzania	Kategorie danych	Podstawa prawna	Uzasadnienie / uwagi
Rejestracja konta i zarządzanie profilem użytkownika	Dane konta, adresowe, firmowe	Art. 6 ust. 1 lit. b RODO (umowa)	Niezbędne do zawarcia i wykonania umowy o świadczenie usług drogą elektroniczną
Realizacja rezerwacji i zarządzanie transakcjami	Dane konta, transakcyjne, komunikacyjne	Art. 6 ust. 1 lit. b RODO (umowa)	Bez tych danych realizacja usługi pośrednictwa jest niemożliwa
Obsługa płatności przez Stripe Connect	Dane transakcyjne, konto	Art. 6 ust. 1 lit. b RODO (umowa)	Stripe przetwarza dane jako odrębny administrator – szczegóły w sekcji 4 i 5

Obsługa komunikacji użytkowników (czat, support)	Dane komunikacyjne, konto	Art. 6 ust. 1 lit. b RODO (umowa)	Komunikacja niezbędna do realizacji usługi; chat przechowuje historię wiadomości trwale przez okres wskazany w sekcji 6
Wystawianie faktur, prowadzenie dokumentacji księgowej	Dane konta, firmowe, transakcyjne	Art. 6 ust. 1 lit. c RODO (obowiązek prawny)	Ustawa o rachunkowości, przepisy podatkowe (5 lat)
Rozliczenia podatkowe i raportowanie VAT	Dane firmowe, transakcyjne	Art. 6 ust. 1 lit. c RODO (obowiązek prawny)	Ordynacja podatkowa, ustawa o VAT
Wykrywanie i zapobieganie oszustwom (fraud detection)	Dane techniczne, transakcyjne, konto	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes)	Ochrona użytkowników i platformy; przetwarzanie automatyczne; patrz sekcja 9
Bezpieczeństwo logowania, OTP, trusted devices, risk scoring	Dane techniczne, konto	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes)	Bezpośrednia ochrona konta użytkownika; logi audytowe są immutable (niezmienne)
Ograniczenie nadużyć kont (max 3 konta per numer telefonu)	Numer telefonu, dane konta	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes)	Zapobieganie wielokrotnej rejestracji; limit egzekwowany automatycznie
Obrona przed chargebackami i sporami płatniczymi	Dane transakcyjne, komunikacyjne, techniczne	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes)	Uzasadniony interes w dochodzeniu i obronie roszczeń
Moderacja treści i zapobieganie naruszeniom regulaminu	Dane komunikacyjne, konto	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes)	Ochrona innych użytkowników platformy
Newsletter i komunikacja marketingowa (e-mail/SMS)	E-mail, numer telefonu	Art. 6 ust. 1 lit. a RODO (zgoda)	Wymagana aktywna, oddzielna zgoda; cofnięcie zgody nie wpływa na inne przetwarzania
Google Analytics – analiza ruchu i zachowań użytkowników	Dane techniczne, cookies analytics	Art. 6 ust. 1 lit. a RODO (zgoda)	Wymaga zgody w bannerze cookies; bez zgody analytics nie jest aktywowane
Meta Pixel – remarketing i pomiar konwersji	Dane techniczne, cookies marketing	Art. 6 ust. 1 lit. a RODO (zgoda)	Wymaga zgody w bannerze cookies; dane mogą być przekazywane do USA
SMS OTP i przypomnienia bezpieczeństwa	Numer telefonu	Art. 6 ust. 1 lit. b lub f RODO	OTP niezbędne do logowania (wykonanie umowy); przypomnienia bezpieczeństwa – uzasadniony interes
Przypomnienia e-mail i SMS o rezerwacjach	E-mail, numer telefonu	Art. 6 ust. 1 lit. b RODO (umowa)	Bezpośrednio związane z realizacją rezerwacji

3.1 Przetwarzanie automatyczne i profilowanie

Platforma stosuje **automatyczne mechanizmy oceny ryzyka** (login risk scoring) przy każdym logowaniu oraz przy tworzeniu nowych kont. Scoring uwzględnia m.in.: lokalizację IP, user-agent, historię logowań, liczbę powiązanych kont i wzorce behawioralne. Mechanizm ten **nie stanowi zautomatyzowanego podejmowania decyzji w rozumieniu art. 22 RODO** – ostateczne decyzje o zablokowaniu konta wymagają weryfikacji przez administratora. Użytkownik ma prawo do uzyskania wyjaśnienia działania mechanizmu i zakwestionowania jego wyniku (kontakt: kontakt@midar.rent).

4. Odbiorcy danych osobowych (procesorzy i podprocesorzy)

Dane osobowe użytkowników mogą być udostępniane wyłącznie podmiotom niezbędnym do funkcjonowania platformy (procesorom danych, art. 28 RODO) lub organom publicznym na podstawie wyraźnego obowiązku prawnego. MIDAR nie sprzedaje danych osobowych stronom trzecim.

Podmiot	Rola	Kategoria danych	Cel i podstawa przekazania
Stripe Inc. / Stripe Payments Europe	Odrębny administrator / procesor (Stripe Connect)	Dane konta, transakcyjne, KYC	Realizacja płatności, wypłat, weryfikacja tożsamości partnerów (KYC), zarządzanie sporami. Stripe przetwarza dane na własnych zasadach (stripe.com/privacy). Umowa DPA zawarta.
Cloudflare Inc.	Procesor	Dane techniczne (IP, ruch sieciowy)	CDN, ochrona DDoS, przechowywanie plików statycznych (R2), weryfikacja CAPTCHA (Turnstile). Umowa DPA zawarta.
Google LLC	Procesor / odrębny administrator	Dane konta (OAuth), dane techniczne (Analytics)	Logowanie przez Google (OAuth2), integracja z Google Maps, analiza ruchu (Google Analytics 4 – wyłącznie za zgodą). Umowa DPA zawarta.
Meta Platforms Inc.	Odrębny administrator	Dane techniczne (Pixel, cookies)	Remarketing, pomiar konwersji (Meta Pixel – wyłącznie za zgodą). Meta przetwarza dane na własnych zasadach.
SMSAPI (Spółka SMSAPI Sp. z o.o.)	Procesor	Numer telefonu	Wysyłka SMS OTP, SMS transakcyjnych i powiadomień.
SEOHost / dostawca SMTP	Procesor	Adres e-mail, treść wiadomości transakcyjnych	Wysyłka wiadomości transakcyjnych e-mail (rezerwacje, potwierdzenia, bezpieczeństwo).
Chatway	Procesor	Dane konta, treści czatu supportowego	Widget obsługi klienta (live support chat). Umowa DPA zawarta. Dane mogą być przetwarzane poza EOG – patrz sekcja 5.
Infrastruktura własna (self-hosted)	MIDAR jako administrator	Wszystkie kategorie danych	Baza danych PostgreSQL, cache Redis, monitoring aplikacji – serwery zlokalizowane w EOG lub na serwerach zgodnych z wymogami RODO.
Organy publiczne (UODO, sądy, organy ścigania)	Odrębny administrator	Zakres wymagany prawem	Wyłącznie na podstawie wyraźnego obowiązku prawnego lub prawomocnego nakazu.

Uwaga dotycząca Stripe Connect: partnerzy wynajmujący przystępują do platformy Stripe Connect Express i w ramach tego procesu przechodzą weryfikację KYC (Know Your Customer) realizowaną bezpośrednio przez Stripe. W tym zakresie Stripe działa jako odrębny administrator danych, a MIDAR nie ma dostępu do pełnych dokumentów tożsamości partnerów przesłanych do Stripe.

5. Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)

Część naszych procesorów ma siedzibę lub przetwarza dane w Stanach Zjednoczonych lub innych krajach spoza EOG. Każdy taki transfer odbywa się wyłącznie na podstawie odpowiednich zabezpieczeń przewidzianych w Rozdziale V RODO.

5.1 Transfery do USA i zastosowane zabezpieczenia

Podmiot	Kraj	Mechanizm transferu	Uwagi
Google LLC	USA (serwery globalne)	Standardowe Klauzule Umowne (SCC) + EU-US Data Privacy Framework (DPF)	Google jest certyfikowany w ramach DPF. Dane Analytics mogą podlegać anonimizacji IP.
Meta Platforms Inc.	USA	Standardowe Klauzule Umowne (SCC) + EU-US Data Privacy Framework (DPF)	Meta certyfikowana w DPF. Transfer dotyczy wyłącznie danych z Meta Pixel (za zgodą użytkownika).
Stripe Inc.	USA / Irlandia (Stripe Payments Europe Ltd.)	Standardowe Klauzule Umowne (SCC); operacje europejskie przez podmiot irlandzki	Stripe Payments Europe Ltd. (Irlandia, w EOG) obsługuje płatności europejskie. Transfer do USA możliwy w ramach operacji globalnych.
Cloudflare Inc.	USA / EOG (Edge nodes)	Standardowe Klauzule Umowne (SCC) + EU-US Data Privacy Framework (DPF)	Ruch sieciowy może być przetwarzany w węzłach zlokalizowanych poza EOG. Cloudflare certyfikowany w DPF.
Chatway	USA / inny kraj poza EOG	Standardowe Klauzule Umowne (SCC)	Transfer danych supportowych (treści czatu) do operatora narzędzia. Weryfikacja aktualnego statusu DPF Chatway w toku.

5.2 Standardowe Klauzule Umowne (SCC)

Przekazywanie danych do państw spoza EOG, które nie zapewniają odpowiedniego stopnia ochrony (decyzja Komisji Europejskiej), odbywa się na podstawie **Standardowych Klauzul Umownych przyjętych przez Komisję Europejską decyzją 2021/914** z dnia 4 czerwca 2021 r. (Moduł 1 – controller-to-controller lub Moduł 2 – controller-to-processor, odpowiednio do relacji z danym podmiotem).

5.3 EU-US Data Privacy Framework (DPF)

W odniesieniu do podmiotów certyfikowanych w ramach EU-US Data Privacy Framework (decyzja adekwatności Komisji Europejskiej z dnia 10 lipca 2023 r., C(2023) 4745), transfer danych opiera się na tej

decyzji jako podstawie prawnej. Aktualny status certyfikacji procesorów dostępny jest pod adresem: https://www.dataprivacyframework.gov/list.

Masz prawo do uzyskania kopii zastosowanych zabezpieczeń transferowych. W tym celu skontaktuj się pod adresem **kontakt@midar.rent**.

6. Okres przechowywania danych (retencja)

Dane osobowe przechowywane są wyłącznie przez czas niezbędny do realizacji celów, dla których zostały zebrane, lub przez okres wymagany przez obowiązujące przepisy prawa. Po upływie okresu retencji dane są usuwane lub anonimizowane w sposób uniemożliwiający identyfikację osoby.

Kategoria danych	Okres retencji	Podstawa / uzasadnienie
Profil użytkownika (konto aktywne)	Do usunięcia konta + 30 dni	Możliwość przywrócenia konta przez 30 dni od usunięcia; po tym czasie – anonimizacja lub trwałe usunięcie
Dane transakcyjne i dokumentacja płatnicza	5 lat	Ustawa o rachunkowości (art. 74), przepisy podatkowe – licząc od końca roku podatkowego, w którym transakcja miała miejsce
Faktury i dokumenty księgowe	5 lat	Ordynacja podatkowa, ustawa o VAT – obowiązkowy okres przechowywania dokumentacji fiskalnej
Logi bezpieczeństwa, logi audytowe, logi IP	3 lata	Uzasadniony interes MIDAR (obrona przed roszczeniami, wykrywanie nadużyć); termin przedawnienia roszczeń cywilnych. Logi audytowe są IMMUTABLE – nie mogą być zmienione ani usunięte przed upływem okresu retencji.
Historia czatu i komunikacji między użytkownikami	3 lata	Uzasadniony interes (obrona przed roszczeniami, rozstrzyganie sporów dispute); ujawnione dane kontaktowe (contact reveal) podlegają temu samemu cyklowi.
Zgłoszenia supportowe i korespondencja z działem wsparcia	3 lata	Uzasadniony interes (dokumentacja obsługi klienta, obrona przed roszczeniami)
Dane analityczne (Google Analytics – zanonimizowane lub zagregowane)	Do 14 miesięcy w Google Analytics (ustawienia domyślne GA4)	Dane są anonimizowane lub zagregowane; nie stanowią danych osobowych po anonimizacji
Backupy lokalne baz danych	7 dni (rolling backup)	Krótki cykl backupu minimalizuje ryzyko wycieku w przypadku incydentu bezpieczeństwa; po 7 dniach backup jest nadpisywany
Zgody marketingowe (newsletter, SMS)	Do cofnięcia zgody + 3 lata (dowód udzielenia zgody)	Obowiązek wykazania ważności zgody (art. 7 ust. 1 RODO); samo przetwarzanie marketingowe kończy się z chwilą cofnięcia zgody
Dane z cookies analitycznych i marketingowych	Zgodnie z konfiguracją konkretnego narzędzia (GA4: do 13 mies., Meta	Szczegóły w sekcji 8 (Cookies). Przetwarzanie tylko za aktywną zgodą.

	Pixel: do 90 dni zdarzenia)	

6.1 Mechanizm usunięcia konta – ważne zastrzeżenie

Usunięcie konta (soft delete) powoduje anonimizację profilu użytkownika w ciągu 30 dni, **ale nie usuwa automatycznie** następujących kategorii danych:

- **danych transakcyjnych** i dokumentacji płatniczej (5-letni obowiązek prawny);
- **logów audytowych i bezpieczeństwa** (immutable – nieusuwalne przed upływem 3 lat);
- **historii czatu**, w tym ujawnionych danych kontaktowych (3 lata);
- **dokumentów księgowych** (faktury, 5 lat);
- **danych niezbędnych do obrony przed roszczeniami** do czasu ich przedawnienia.

Użytkownik jest o tym fakcie informowany w momencie wysyłania żądania usunięcia konta.

7. Prawa osób, których dane dotyczą

Na podstawie RODO przysługują Ci następujące prawa w zakresie przetwarzania danych osobowych przez MIDAR RENT. Żądania dotyczące realizacji praw można składać na adres e-mail: kontakt@midar.rent

7.1 Prawo dostępu do danych (art. 15 RODO)

Masz prawo uzyskać od MIDAR potwierdzenie, czy przetwarzamy Twoje dane osobowe, a jeśli tak – uzyskać do nich dostęp oraz informacje o celach przetwarzania, kategoriach danych, odbiorcach, planowanym okresie przechowywania i przysługujących Ci prawach.

7.2 Prawo do sprostowania danych (art. 16 RODO)

Masz prawo żądać niezwłocznego sprostowania nieprawidłowych danych osobowych lub uzupełnienia niekompletnych danych. Większość danych możesz zaktualizować samodzielnie w ustawieniach konta.

7.3 Prawo do usunięcia danych ("prawo do bycia zapomnianym", art. 17 RODO)

Masz prawo żądać usunięcia Twoich danych osobowych, jeśli nie są już niezbędne do celów, w których zostały zebrane, cofnąłeś/cofnęłaś zgodę będącą jedyną podstawą przetwarzania lub dane były przetwarzane niezgodnie z prawem. **Prawo to jest ograniczone** w zakresie danych, które MIDAR ma obowiązek przechowywać na podstawie przepisów prawa (dokumentacja księgowa, logi audytowe) – patrz sekcja 6.1.

7.4 Prawo do ograniczenia przetwarzania (art. 18 RODO)

Masz prawo żądać ograniczenia przetwarzania Twoich danych w przypadku kwestionowania ich prawidłowości, sprzeciwu wobec przetwarzania lub gdy dane nie są już potrzebne, ale są wymagane do ustalenia, dochodzenia lub obrony roszczeń.

7.5 Prawo do sprzeciwu (art. 21 RODO)

Masz prawo wnieść sprzeciw wobec przetwarzania danych na podstawie prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO), w tym profilowania. W takim przypadku MIDAR zaprzestanie przetwarzania, chyba że istnieją **ważne, prawnie uzasadnione podstawy** nadrzędne wobec Twoich interesów lub dane są niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

7.6 Prawo do przenoszenia danych (art. 20 RODO)

Masz prawo otrzymać dane osobowe dostarczone MIDAR w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (JSON/CSV). **Eksport danych realizowany jest obecnie manualnie** – skieruj żądanie na adres kontakt@midar.rent. MIDAR zrealizuje żądanie w terminie 30 dni od weryfikacji tożsamości wnioskodawcy. Prawo to dotyczy danych przetwarzanych na podstawie zgody lub umowy i w sposób zautomatyzowany.

7.7 Prawo do cofnięcia zgody (art. 7 ust. 3 RODO)

W każdej chwili możesz cofnąć zgodę na przetwarzanie danych w celach marketingowych (newsletter, SMS marketing) lub analitycznych (Google Analytics, Meta Pixel). Cofnięcie zgody jest możliwe: (a) poprzez link wypisania w każdej wiadomości marketingowej, (b) w ustawieniach konta w sekcji Powiadomienia i Prywatność, (c) poprzez zaktualizowanie preferencji cookie w bannerze cookies. **Cofnięcie zgody nie wpływa** na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

7.8 Prawo do wniesienia skargi do organu nadzorczego (art. 77 RODO)

Jeżeli uważasz, że przetwarzamy Twoje dane niezgodnie z RODO, masz prawo wnieść skargę do **Prezesa Urzędu Ochrony Danych Osobowych (UODO)**:

Dane UODO	
Adres	ul. Stawki 2, 00-193 Warszawa
Telefon	(22) 531 03 00
E-mail	kancelaria@uodo.gov.pl
Strona www	uodo.gov.pl

7.9 Terminy realizacji żądań

MIDAR realizuje żądania dotyczące praw osób bez zbędnej zwłoki, **w terminie do 30 dni** od dnia otrzymania żądania. W przypadku skomplikowanych lub licznych żądań termin może zostać przedłużony o kolejne 2 miesiące, o czym zostaniesz poinformowany/a przed upływem pierwszego miesiąca. Realizacja żądań jest **bezpłatna**, z wyjątkiem żądań ewidentnie nieuzasadnionych lub nadmiernych.

8. Pliki cookies i technologie śledzące

Platforma MIDAR RENT wykorzystuje pliki cookies (ciasteczka) i podobne technologie (localStorage, fingerprinting urządzenia) do zapewnienia prawidłowego działania serwisu, bezpieczeństwa kont oraz – wyłącznie za Twoją zgodą – celów analitycznych i marketingowych.

8.1 Szczegółowy rejestr cookies

Nazwa / kategoria	Typ / dostawca	Czas życia	Cel i uzasadnienie
session_id / refresh_token	Niezbędne – MIDAR	Sesja / 30 dni	Utrzymanie sesji użytkownika i obsługa odświeżania tokenów JWT. Niezbędne do działania platformy – brak wymogu udzielenia zgody.

csrf_token	Niezbędne – MIDAR	Sesja	Ochrona przed atakami Cross-Site Request Forgery (CSRF). Niezbędny do bezpieczeństwa każdej sesji.
oauth_state	Niezbędne – MIDAR	Sesja (jednorazowy)	Zabezpieczenie przepływu OAuth2 (logowanie przez Google). Usuwany po zakończeniu przepływu.
trusted_device_token	Bezpieczeństwo – MIDAR	90 dni	Oznaczenie zaufanego urządzenia użytkownika w celu ograniczenia częstotliwości weryfikacji dwuskładnikowej (2FA/OTP). Podstawa: uzasadniony interes (bezpieczeństwo konta).
_ga / _ga_[ID]	Analityczne – Google Analytics 4	13 miesięcy / 2 lata	Identyfikacja użytkownika dla celów analizy ruchu w Google Analytics 4. WYMAGA aktywnej zgody w bannerze cookies. Bez zgody – nie jest ustawiany.
_fbp / _fbc	Marketingowe – Meta Pixel	90 dni / 2 lata	Śledzenie konwersji i remarketingu przez Meta (Facebook/Instagram). WYMAGA aktywnej zgody w bannerze cookies. Bez zgody – nie jest ustawiany.
chatway_* / cw_visitor	Support – Chatway	Sesja / stały	Identyfikacja sesji czatu supportowego i powiązanie z historią rozmów. Ustawiany przy inicjalizacji widgetu Chatway.
localStorage: fingerprint, trusted_devices, preferences	Bezpieczeństwo / preferencje – MIDAR (localStorage, nie cookie HTTP)	Stały (do wylogowania / czyszczenia danych przeglądarki)	Przechowywanie fingerprinta urządzenia i preferencji interfejsu. Używany do wykrywania podejrzanych logowań z nowych urządzeń.

8.2 Zarządzanie zgodą na cookies

Przy pierwszej wizycie na platformie wyświetlany jest **banner zarządzania zgodą na cookies** (Consent Management Platform). Możesz zaakceptować wszystkie kategorie cookies, wybrać tylko wybrane lub odrzucić wszystkie z wyjątkiem niezbędnych. Swój wybór możesz zmienić w dowolnym momencie, klikając przycisk **"Ustawienia cookies"** dostępny w stopce serwisu lub w ustawieniach konta.

8.3 Instrukcja blokowania cookies w przeglądarkach

Możesz również zarządzać cookies bezpośrednio w ustawieniach przeglądarki internetowej: Chrome (Ustawienia → Prywatność i bezpieczeństwo → Pliki cookie), Firefox (Opcje → Prywatność i bezpieczeństwo), Safari (Preferencje → Prywatność), Edge (Ustawienia → Pliki cookie i uprawnienia witryn). Wyłączenie cookies niezbędnych może uniemożliwić korzystanie z platformy.

8.4 Wtyczki i sygnały przeglądarki

MIDAR RENT respektuje sygnał Global Privacy Control (GPC) wysyłany przez przeglądarki obsługujące ten standard. Wykrycie sygnału GPC jest traktowane równoznacznie z odmową udzielenia zgód na cookies analityczne i marketingowe.

9. Bezpieczeństwo danych osobowych

MIDAR wdrożył techniczne i organizacyjne środki bezpieczeństwa zgodne z wymogami art. 32 RODO, proporcjonalne do zidentyfikowanego ryzyka naruszenia praw i wolności osób fizycznych.

9.1 Wdrożone środki techniczne

- Szyfrowanie danych w transmisji (TLS 1.2/1.3) dla całej komunikacji z platformą.
- Szyfrowanie haseł wyłącznie przy użyciu funkcji skrótu bcrypt z solą (hasła w postaci jawnej nigdy nie są przechowywane).
- Weryfikacja dwuskładnikowa (2FA/OTP) – dostępna dla wszystkich użytkowników, obowiązkowa dla partnerów biznesowych.
- System oceny ryzyka logowania (login risk scoring) – automatyczne wykrywanie podejrzanych prób dostępu do konta.
- Niezmienne logi audytowe (immutable audit logs) – rejestracja wszystkich operacji krytycznych bez możliwości retroaktywnej modyfikacji.
- Ochrona DDoS i filtrowanie złośliwego ruchu przez Cloudflare.
- Weryfikacja CAPTCHA (Cloudflare Turnstile) przy rejestracji, logowaniu i operacjach wrażliwych.
- Limit kont powiązanych z jednym numerem telefonu (max. 3) – przeciwdziałanie zakładaniu fikcyjnych kont.
- Izolacja infrastruktury – baza danych PostgreSQL i cache Redis niedostępne bezpośrednio z Internetu.
- Rotacyjne backupy lokalne (7-dniowy cykl rolling backup) z procedurą testowania przywracania.

9.2 Środki organizacyjne

- Zasada minimalnych uprawnień (least privilege) – dostęp do danych osobowych mają wyłącznie osoby, dla których jest to niezbędne do wykonywania obowiązków.
- Szkolenia z zakresu ochrony danych i bezpieczeństwa informacji dla osób mających dostęp do danych.
- Procedura reagowania na incydenty bezpieczeństwa (Data Breach Response Procedure) – obejmuje ocenę ryzyka, zgłoszenie do UODO w ciągu 72 godzin (art. 33 RODO) i powiadamianie użytkowników, gdy jest to wymagane (art. 34 RODO).
- Regularne przeglądy bezpieczeństwa konfiguracji infrastruktury.

9.3 Przetwarzanie automatyczne i fraud detection

System fraud detection MIDAR przetwarza dane techniczne i transakcyjne w sposób zautomatyzowany w celu identyfikacji wzorców wskazujących na oszustwo, nadużycie konta lub próby obejścia ograniczeń platformy. System może automatycznie **tymczasowo ograniczyć dostęp do konta** w przypadku wykrycia podejrzanej aktywności. Użytkownik ma prawo do uzyskania informacji o zastosowanych ograniczeniach i odwołania się od decyzji systemu – kontakt: **kontakt@midar.rent**.

9.4 Zgłaszanie incydentów bezpieczeństwa

W przypadku podejrzenia naruszenia bezpieczeństwa danych (np. nieautoryzowanego dostępu do konta) prosimy o niezwłoczne zgłoszenie na adres: **kontakt@midar.rent**. MIDAR zobowiązuje się do rozpatrzenia zgłoszenia i powiadomienia użytkownika o podjętych działaniach w ciągu 72 godzin.

10. Kontakt w sprawach prywatności i składanie skarg

We wszelkich sprawach dotyczących ochrony danych osobowych – w tym realizacji praw, udzielenia dodatkowych informacji, zgłaszania naruszeń lub składania skarg – prosimy o kontakt:

Forma kontaktu	Dane kontaktowe / instrukcja
E-mail (preferowany)	kontakt@midar.rent – odpowiedź w terminie do 30 dni od weryfikacji tożsamości wnioskodawcy

Korespondencja pisemna	MIDAR Dariusz Gregorczyk, ul. Mleczna 33, 26-617 Radom, Polska – z dopiskiem "RODO/Prywatność"
Organ nadzorczy (skargi)	Prezes Urzędu Ochrony Danych Osobowych (UODO), ul. Stawki 2, 00-193 Warszawa, uodo.gov.pl

Weryfikacja tożsamości: Przy składaniu żądań dotyczących praw (dostęp, usunięcie, przenoszenie) MIDAR może poprosić o potwierdzenie tożsamości, aby zapobiec nieautoryzowanemu dostępowi do danych. Weryfikacja odbywa się poprzez potwierdzenie dostępu do adresu e-mail powiązanego z kontem lub – w uzasadnionych przypadkach – poprzez przesłanie skanu dokumentu tożsamości (skan jest niszczony bezpośrednio po weryfikacji).

11. Zmiany Polityki Prywatności

MIDAR zastrzega sobie prawo do aktualizacji niniejszej Polityki Prywatności w związku ze zmianami przepisów prawa, rozwojem platformy lub zmianami w stosowanych technologiach.

- **Istotne zmiany** (wpływające na prawa użytkownika, nowe kategorie danych, nowi odbiorcy, nowe cele przetwarzania): MIDAR poinformuje użytkowników drogą e-mail oraz wyświetli wyraźne powiadomienie na platformie z co najmniej **30-dniowym** wyprzedzeniem.
- **Zmiany redakcyjne** (korekty językowe, uszczegółowienia, aktualizacje danych kontaktowych): wejście w życie z dniem publikacji na platformie bez wcześniejszego powiadomienia.
- Aktualna wersja Polityki Prywatności jest zawsze dostępna pod adresem **midar.rent/privacy**.
- Daty kolejnych wersji dokumentu są archiwizowane i dostępne na życzenie.

Kontynuowanie korzystania z platformy po wejściu w życie zmienionej Polityki Prywatności jest równoznaczne z akceptacją zmian. Jeśli nie zgadzasz się ze zmianami, masz prawo do usunięcia konta i żądania realizacji przysługujących Ci praw – kontakt: **kontakt@midar.rent**.