

Rejestr Technologii i Dostawców AutoLert

DEVSTY Bartłomiej Hudecki · Wersja 1.0 · Obowiązuje od 12 sierpnia 2026

1. Zakres i zasady Rejestru

Rejestr uzupełnia Regulamin, Politykę Prywatności oraz Politykę Cookies i podobnych technologii AutoLert. Wskazuje aktualnie używane technologie urządzenia, dostawców przetwarzających dane, typowe kategorie danych, cele, regiony, mechanizmy transferowe i okresy retencji.

Zmiana narzędzia w ramach wcześniej opisanego celu i kategorii danych może zostać odzwierciedlona przez zmianę Rejestru. Nowy cel, nowa kategoria danych, istotnie szersze profilowanie lub technologia bardziej ingerująca w prywatność wymagają wcześniejszej oceny, odpowiedniej aktualizacji dokumentów i – gdy jest to wymagane – ponownego uzyskania zgody.

Okresy wskazane w Rejestrze są okresami typowymi albo maksymalnymi dla aktywnej konfiguracji. Dane mogą być przechowywane dłużej, jeżeli jest to wymagane prawem, konieczne dla bezpieczeństwa, rozpatrzenia reklamacji lub ustalenia, dochodzenia bądź obrony roszczeń.

2. Technologie zapisywane lub odczytywane na urządzeniu

Technologie oznaczone jako niezbędne są używane w zakresie koniecznym do działania Serwisu lub funkcji wyraźnie żądanej przez Użytkownika. PostHog jest uruchamiany dopiero po zgodzie na kategorię analityczną.

Technologie zapisywane lub odczytywane na urządzeniu

Identyfikator	Dostawca / domena	Kategoria i cel	Typowe dane	Okres
al_consent	AutoLert / .autolert.pl	Niezbędna · zapis i dowód wyboru zgód	wybrane kategorie, identyfikator i czas zgody, wersja/revision	182 dni
__session, __client_uat	Clerk / clerk.autolert.pl	Niezbędna · logowanie, sesja i bezpieczeństwo Konta	identyfikator sesji/Konta, stan uwierzytelnienia, czas aktywności	sesja lub okres technicznie wymagany przez Clerk
__cf_bm	Cloudflare / challenges.cloudflare.com	Niezbędna · ochrona przed botami i nadużyciami	sygnały urządzenia i przeglądarki, adres IP, wynik kontroli bezpieczeństwa	około 30 minut
NEXT_LOCALE	AutoLert / next-intl	Niezbędna lub funkcjonalna · preferencja języka	wybrany język PL/EN	1 rok
ph_* / __ph_*	PostHog / eu.i.posthog.com	Analityczna · odsłony, zdarzenia, lejki, atrybucja i badanie produktu; tylko po zgodzie	identyfikator analityczny, URL, źródło wejścia, kampania, zdarzenia, elementy interfejsu, urządzenie, przybliżona lokalizacja; identyfikator Konta, jeżeli został świadomie powiązany	do 1 roku; dane analityczne zgodnie z konfiguracją i zasadami retencji AutoLert

Aktualna konfiguracja PostHog: autocapture i pomiar odsłon są aktywne po uzyskaniu zgody, nagrywanie sesji jest wyłączone. Przechowywanie wykorzystuje first-party cookie i local storage w domenie .autolert.pl.

3. Dostawcy infrastruktury, aplikacji i obsługi

3.1. Vercel Inc.

Status w AutoLert: aktywny i potwierdzony publicznie

Rola: podmiot przetwarzający w zakresie danych klienta, niezależny administrator dla własnych danych usługowych i rozliczeniowych

Usługa i cel: hosting stron autolert.pl i app.autolert.pl, sieć dostarczania treści, wykonanie aplikacji Next.js, bezpieczeństwo, cache i logi techniczne

Typowe dane: adres IP, identyfikatory żądań, nagłówki i parametry techniczne, URL, dane urządzenia i przeglądarki, ograniczone logi błędów, dane przesyłane przez funkcje frontendowe w zakresie niezbędnym do obsługi żądania

Region przetwarzania: infrastruktura globalna, w tym EOG i USA, bieżące odpowiedzi są obsługiwane przez infrastrukturę Vercel

Transfer poza EOG: DPF wobec certyfikowanych podmiotów lub Standardowe Klauzule Umowne i środki uzupełniające zgodnie z DPA

Retencja: przez okres świadczenia usługi i według konfiguracji, dane usługowe do czasu ustania celu, z możliwością dłuższej retencji prawnej i bezpieczeństwa

Informacje szczególne: Vercel może przetwarzać dane generowane przez usługę dla utrzymania, bezpieczeństwa, analityki, benchmarków i raportowania na zasadach DPA, nie należy przysyłać danych szczególnych.

Prywatność: <https://vercel.com/legal/privacy-notice>

DPA: <https://vercel.com/legal/dpa>

3.2. Railway Corporation

Status w AutoLert: aktywny i potwierdzony publicznie dla api.autolert.pl, zakres bazy danych i kopii wymaga potwierdzenia administracyjnego

Rola: podmiot przetwarzający, niezależny administrator dla danych konta Railway i danych użycia infrastruktury

Usługa i cel: hosting backendu API, komunikacja aplikacji z backendem, wykonanie usług, logi, diagnostyka i bezpieczeństwo, może obejmować bazę danych, wolumeny i kopie, jeżeli są skonfigurowane w projekcie Railway

Typowe dane: dane Konta i umowy, adresy URL i treść Ogłoszeń, obrazy i metadane, Raporty, identyfikatory transakcji, logi, adres IP, diagnostyka i dane bezpieczeństwa – zależnie od endpointu

Region przetwarzania: region wybrany w projekcie Railway, publiczny endpoint jest obsługiwany przez węzeł w Warszawie, ale przetwarzanie lub wsparcie może obejmować USA i inne regiony

Transfer poza EOG: DPF, gdy znajduje zastosowanie, albo Standardowe Klauzule Umowne zgodnie z DPA Railway

Retencja: według okresów określonych w Polityce Prywatności i konfiguracji projektu, po zakończeniu usługi dane są zwracane lub usuwane, chyba że dalsze przechowywanie jest wymagane prawem

Informacje szczególne: Railway może przetwarzać dane użycia i logi jako niezależny administrator dla bezpieczeństwa, zapobiegania nadużyciom oraz utrzymania usługi.

Prywatność: <https://railway.com/legal/privacy>

DPA: <https://railway.com/legal/dpa>

3.3. Clerk, Inc.

Status w AutoLert: aktywny i potwierdzony publicznie

Rola: podmiot przetwarzający dane uwierzytelniania, niezależny administrator dla danych własnego konta i telemetrii dostawcy

Usługa i cel: rejestracja, logowanie hasłem lub kodem e-mail, logowanie przez Google, utrzymanie sesji, zarządzanie Kontem i przeciwdziałanie nadużyciom

Typowe dane: adres e-mail, nazwa wyświetlana, identyfikator Konta, hash/sekret uwierzytelniający, identyfikatory sesji i urządzenia, adres IP, dane bezpieczeństwa, przy logowaniu Google – identyfikator i dane profilu objęte zgodą użytkownika

Region przetwarzania: USA i inne lokalizacje dostawcy lub jego podwykonawców, zależnie od konfiguracji Clerk

Transfer poza EOG: EU-US Data Privacy Framework, a gdy nie może być zastosowany – Standardowe Klauzule Umowne zgodnie z DPA Clerk

Retencja: przez czas korzystania z Konta i świadczenia usługi, zgodnie z DPA pozostałe kopie danych klienta są usuwane zasadniczo w ciągu 90 dni od zakończenia umowy

Informacje szczególne: Clerk może prowadzić telemetrię, monitoring bezpieczeństwa i ochronę przed nadużyciami. Hasła nie są przechowywane przez Operatora w postaci jawnej.

Prywatność: <https://clerk.com/legal/privacy>

DPA: <https://clerk.com/legal/dpa>

Telemetria: <https://clerk.com/legal/telemetry>

3.4. Google Ireland Limited / Google LLC

Status w AutoLert: aktywny dla logowania Google, Google Fonts jest publicznie ładowany w aplikacji

Rola: niezależny administrator w zakresie konta Google i procesu logowania, dostawca zasobów czcionek w zakresie żądania sieciowego

Usługa i cel: OAuth/OpenID Connect dla opcjonalnego logowania przez Google oraz dostarczenie plików Google Fonts w app.autolert.pl

Typowe dane: przy logowaniu: identyfikator Google, adres e-mail, nazwa i inne dane profilu objęte zakresem zgody, przy pobraniu czcionki: adres IP, dane urządzenia i przeglądarki, czas i żądany zasób

Region przetwarzania: EOG, USA i infrastruktura globalna Google

Transfer poza EOG: decyzje stwierdzające odpowiedni poziom ochrony, DPF wobec certyfikowanych podmiotów lub Standardowe Klauzule Umowne – zależnie od usługi i przepływu

Retencja: według ustawień konta Google i polityk Google, dane przekazane do AutoLert – zgodnie z retencją Konta w Polityce Prywatności

Informacje szczególne: Logowanie przez Google jest dobrowolne. AutoLert powinien żądać wyłącznie minimalnego zakresu danych potrzebnego do utworzenia i obsługi Konta.

Prywatność: <https://policies.google.com/privacy>

OAuth: <https://developers.google.com/identity/protocols/oauth2>

3.5. PostHog Inc.

Status w AutoLert: aktywny po zgodzie analitycznej, potwierdzony publicznie, chmura UE

Rola: podmiot przetwarzający dla danych analitycznych, niezależny administrator dla danych konta PostHog i części danych usługowych dostawcy

Usługa i cel: analityka produktu i marketingu, odsłony, zdarzenia, lejki, atrybucja, kohorty, testy i badanie sposobu korzystania z funkcji

Typowe dane: identyfikator analityczny, adres IP, przybliżona lokalizacja, źródło wejścia, URL, parametry kampanii, typ urządzenia i przeglądarki, zdarzenia i elementy interfejsu, identyfikator Konta, jeśli zostanie powiązany. Autocapture może obejmować tekst lub atrybuty elementu, dlatego pola i obszary z treścią Raportu, danymi kontaktowymi, hasłami i płatnościami muszą być wyłączone lub maskowane

Region przetwarzania: chmura UE – Niemcy/Frankfurt, ograniczone operacje wsparcia lub korporacyjne mogą obejmować USA

Transfer poza EOG: DPF wobec certyfikowanego podmiotu i/lub Standardowe Klauzule Umowne zgodnie z DPA PostHog

Retencja: identyfikatory na urządzeniu do 1 roku, dane analityczne przez okres skonfigurowany w projekcie, nie dłużej niż jest to potrzebne do analityki i badania produktu

Informacje szczególne: Nagrywanie sesji jest obecnie wyłączone. Polityka PostHog przewiduje możliwość używania zagregowanych lub zdeidentyfikowanych treści klienta do rozwoju produktów i modeli, chyba że klient zrezygnuje lub uzgodni inaczej. Status opt-out AutoLert wymaga potwierdzenia administracyjnego.

Prywatność: <https://posthog.com/privacy>

DPA: <https://posthog.com/dpa>

3.6. Plus Five Five, Inc. (Resend)

Status w AutoLert: aktywny i potwierdzony w publicznym kodzie aplikacji

Rola: podmiot przetwarzający dla wiadomości wysyłanych przez AutoLert, niezależny administrator dla danych konta Resend i danych użycia

Usługa i cel: wysyłanie wiadomości transakcyjnych, kodów logowania, potwierdzeń, dokumentów, informacji o bezpieczeństwie oraz – po właściwej zgodzie – wiadomości marketingowych

Typowe dane: adres e-mail, identyfikator i nazwa odbiorcy, metadane wysyłki, temat, treść wiadomości i załączniki, jeżeli włączono pomiar otwarć lub kliknięć – także adres IP, urządzenie, klient pocztowy, czas otwarcia i kliknięcia

Region przetwarzania: USA, region wysyłki nie zmienia faktu, że dane konta, metadane, logi i zapisy API są przechowywane w USA

Transfer poza EOG: EU–US Data Privacy Framework i Standardowe Klauzule Umowne zgodnie z DPA Resend

Retencja: przez czas obowiązywania umowy, zgodnie z DPA dane klienta są usuwane w ciągu 90 dni od zakończenia konta, z wyjątkami prawnymi i bezpieczeństwa

Informacje szczególne: Resend może monitorować lub blokować wiadomości dla zapewnienia zgodności, przeciwdziałania spamowi, nadużyciom i naruszeniom prawa. Pomiar otwarć i kliknięć powinien być wyłączony dla wiadomości, gdy nie jest potrzebny.

Prywatność: <https://resend.com/legal/privacy-policy>

DPA: <https://resend.com/legal/dpa>

3.7. PayPro S.A. (Przelewy24)

Status w AutoLert: aktywny i potwierdzony publicznie

Rola: niezależny administrator danych płatnika w zakresie realizacji płatności, odbiorca danych transakcyjnych od AutoLert

Usługa i cel: obsługa jednorazowych płatności za Raporty i Pakiety, obsługa BLIK, przelewów, kart oraz dostępnych portfeli płatniczych, rozliczenia, bezpieczeństwo i przeciwdziałanie oszustwom

Typowe dane: identyfikator i kwota transakcji, waluta, opis i status płatności, dane płatnika i nabywcy wymagane do realizacji transakcji, adres IP i dane urządzenia, dane bezpieczeństwa, pełne dane karty są wprowadzane w środowisku dostawcy płatności i nie trafiają do Operatora

Region przetwarzania: Polska/EOG, dalsze transfery zależnie od wybranej metody płatności, organizacji kartowej lub portfela

Transfer poza EOG: odpowiednia podstawa dostawcy i właściwe zabezpieczenia transferowe wynikające z jego dokumentacji oraz dokumentacji wybranej metody płatności

Retencja: zgodnie z obowiązkami prawnymi dotyczącymi płatności, przeciwdziałania nadużyciom, rachunkowości, AML i roszczeń

Informacje szczególne: Przejście do środowiska Przelewy24 lub wybranego portfela powoduje stosowanie własnych technologii i dokumentacji danego dostawcy.

Prywatność: <https://www.przelewy24.pl/polityka-prywatnosci>

3.8. Cloudflare, Inc.

Status w AutoLert: aktywny warunkowo podczas kontroli bezpieczeństwa Clerk, potwierdzony publicznie

Rola: podmiot zapewniający techniczną ochronę przed botami i nadużyciami, w określonym zakresie niezależny administrator danych bezpieczeństwa

Usługa i cel: wyświetlanie i obsługa wyzwania bezpieczeństwa, ocena ruchu automatycznego, ochrona logowania i dostępności

Typowe dane: adres IP, identyfikatory żądania, parametry urządzenia i przeglądarki, dane sieciowe, czas, wynik wyzwania i cookie __cf_bm

Region przetwarzania: infrastruktura globalna, w tym EOG i USA

Transfer poza EOG: DPF wobec certyfikowanego podmiotu lub Standardowe Klauzule Umowne zgodnie z właściwym DPA

Retencja: cookie __cf_bm około 30 minut, logi bezpieczeństwa przez okres potrzebny do wykrywania nadużyć i ochrony usługi

Informacje szczególne: Technologia jest uruchamiana wyłącznie w zakresie potrzebnym do bezpieczeństwa i nie służy AutoLert do reklamy.

Prywatność: <https://www.cloudflare.com/privacypolicy/>

DPA: <https://www.cloudflare.com/cloudflare-customer-dpa/>

4. Dostawca sztucznej inteligencji

4.1. OpenAI Ireland Limited / OpenAI OpCo, LLC

Status w AutoLert: założony jako aktywny dostawca AI – wymaga potwierdzenia w konfiguracji backendu przed publikacją Rejestru

Rola: podmiot przetwarzający dane przekazywane przez API, OpenAI Ireland Limited jest właściwą stroną dla klienta z EOG, z możliwością dalszego przetwarzania przez podmioty powiązane i podwykonawców

Usługa i cel: generowanie i analiza tekstu, obrazów i danych potrzebnych do utworzenia Raportu AI, funkcje bezpieczeństwa, moderacji i monitorowania nadużyć

Typowe dane: adres URL i treść Ogłoszenia, fotografie, dane i cechy pojazdu, VIN oraz widoczne dane sprzedawcy, jeżeli są potrzebne do analizy, instrukcje systemowe i prompty, wyniki, identyfikatory żądań, metadane techniczne i wyniki klasyfikatorów bezpieczeństwa

Region przetwarzania: EOG i USA, zależnie od usługi, endpointu, konfiguracji i podwykonawców

Transfer poza EOG: przetwarzanie przez OpenAI Ireland Limited oraz – dla transferów poza EOG – decyzja o odpowiednim poziomie ochrony, Standardowe Klauzule Umowne i środki uzupełniające zgodnie z DPA

Retencja: domyślnie logi monitorowania nadużyć mogą zawierać treść wejściową, wynik i metadane i są przechowywane do 30 dni, dłużej, gdy wymaga tego prawo lub bezpieczeństwo. Niektóre endpointy przechowują stan aplikacyjny według własnych okresów. Zero Data Retention i Modified Abuse Monitoring nie są przyjmowane jako aktywne bez pisemnego potwierdzenia

Informacje szczególne: Dane przesyłane przez API nie są wykorzystywane do trenowania modeli OpenAI, chyba że klient wyraźnie zdecyduje się na udostępnianie danych. Automatyczne monitorowanie bezpieczeństwa jest standardowe, w sytuacjach wynikających z warunków dostawcy, bezpieczeństwa lub prawa może wystąpić przegląd przez upoważnioną osobę. AutoLert nie zakłada aktywnego zakazu human review ani ZDR bez potwierdzenia.

Kontrola i retencja danych API: <https://developers.openai.com/api/docs/guides/your-data>

DPA: <https://openai.com/policies/data-processing-addendum/>

Jeżeli backend korzysta z innego albo dodatkowego dostawcy AI, przed skierowaniem do niego danych należy dodać odrębny wpis wskazujący właściwy podmiot, typ danych, region, transfer, retencję, zasady używania danych do rozwoju modeli, monitoring nadużyć i możliwość przeglądu przez człowieka. Samo zastąpienie dostawcy w ramach tego samego celu nie wymaga zmiany Polityki Prywatności, ale wymaga aktualizacji Rejestru przed rozpoczęciem przetwarzania.

5. Zewnętrzne źródła treści – niebędące dostawcami AutoLert

Otomoto i OLX oraz ich sieci dostarczania obrazów są źródłami publicznych Ogłoszeń wskazywanych przez Użytkownika, a nie dostawcami AutoLert. AutoLert nie jest przez te portale sponsorowany ani wspierany. Podczas pobierania treści przez backend lub wyświetlania obrazu bezpośrednio z zewnętrznej domeny portal albo operator jego CDN może otrzymać adres IP, parametry żądania, czas, typ przeglądarki oraz ograniczoną informację o stronie odsyłającej.

Domeny technicznie dopuszczone do prezentacji obrazów mogą obejmować w szczególności: *.otomotoimg.pl, otomotoimg.pl, *.olxcdn.com, olxcdn.com, *.allegroimg.com i *.fsimg.pl. Zakres ten nie oznacza stałego przekazywania danych do każdej z tych domen, połączenie następuje wyłącznie, gdy odpowiedni zasób jest używany w konkretnym Ogłoszeniu lub Raporcie.

6. Funkcje nieaktywne lub wymagające odrębnej aktywacji

- Nagrywanie sesji PostHog – obecnie wyłączone. Włączenie wymaga uprzedniej zgody, wpisu w Rejestrze, maskowania lub wyłączenia pól haseł, płatności, danych kontaktowych, treści Ogłoszeń i Raportów oraz kontroli jakości maskowania.
- Retargeting, piksele reklamowe i budowanie odbiorców na platformach reklamowych – brak potwierdzonej aktywnej technologii w publicznej konfiguracji. Włączenie wymaga uprzedniej zgody i dodania dokładnego dostawcy, identyfikatorów, danych oraz okresu działania.
- Dodatkowi dostawcy AI, enrichment, purchased leads, telefonia lub SMS – nie są uznawani za aktywnych na podstawie obecnej konfiguracji. Każdy aktywowany dostawca musi zostać dodany przed rozpoczęciem przekazywania danych.

7. Wersjonowanie i archiwizacja

Aktualna wersja Rejestru jest publikowana pod stałym adresem w Serwisie i dostępna z panelu zarządzania zgodami. Operator zachowuje archiwalne wersje w sposób pozwalający wykazać, jaki zakres informacji obowiązywał w chwili wyboru Użytkownika, zawarcia umowy albo wykonania Raportu.

Wersjonowanie i archiwizacja

Wersja	Data	Status	Zakres zmiany
1.0	12.08.2026	pierwsza wersja	Utworzenie Rejestru, odzwierciedlenie publicznie potwierdzonej konfiguracji i przyjętych założeń ostrożnościowych.