

Polityka prywatności

Wersja z 27 października 2026

1. Administrator danych i kontakt

1. Administratorem danych osobowych w związku z prowadzeniem MarketDrones jest **SentioLab sp. z o.o., Nowy Kiełbów 32, 26-806 Stara Błotnica, Polska**, KRS 0000495860, NIP 7010410720, REGON 147082076 („Administrator”). Adres do korespondencji: **ul. Nowoursynowska 161 L, 02-787 Warszawa, Polska**.
2. Pytania i żądania dotyczące prywatności należy kierować na info@marketdrones.net. Serwis: <https://marketdrones.net/>.
3. Polityka obejmuje dane związane z użytkowaniem strony, rejestracją i kontami, rolami w Organizacji, monitorowaniem publicznych źródeł, obsługą płatności, bezpieczeństwem i komunikacją. Tam, gdzie dane osób z Organizacji są przetwarzane przez nią na własny rachunek poza systemem, Organizacja może występować jako odrębny administrator.

2. Kategorie osób i danych

Osoby	Kategorie danych
Użytkownicy, administratorzy i osoby zapraszane	Adres e-mail, imię lub oznaczenie użytkownika, Organizacja, rola, uprawnienia, status konta, zaproszenia, ustawienia raportów i alertów, obserwowane marki, potwierdzenia akceptacji dokumentów i preferencje marketingowe
Przedstawiciele i osoby kontaktowe Organizacji	Dane służbowe, treść korespondencji, dane zgłoszeń, informacje potrzebne do obsługi umowy
Osoby powiązane z rozliczeniami	Dane do faktury i identyfikacji przedsiębiorcy, dane osoby kontaktowej, płatności i rozliczeń, informacje o statusie płatności; nie gromadzimy pełnych danych karty ani CVV
Odwiedzający serwis i Użytkownicy Panelu	Adres IP, identyfikatory sesji, dane przeglądarki i urządzenia niezbędne do działania, informacje o błędach, zdarzenia techniczne i bezpieczeństwa

Osoby	Kategorie danych
Osoby występujące w monitorowanych materiałach	Incydentalne dane osobowe widoczne na publicznych stronach i w dokumentach, np. nazwiska, funkcje zawodowe, dane osób kontaktowych czy podpisujących dokumenty; celem nie jest monitorowanie osób fizycznych
Osoby objęte potwierdzonymi nadużyciami bezpłatnego dostępu	Minimalne identyfikatory niezbędne do rozpoznania powtórnego nadużycia, data potwierdzenia i podstawa blokady, ewentualnie skrótowy zapis wyniku weryfikacji

Nie prowadzimy marketingowego śledzenia zachowania Użytkowników ani historii ich wyszukiwań i przeglądania materiałów analitycznych. Wyjątkiem są techniczne rejestry niezbędne do bezpieczeństwa i realizacji istotnych operacji administracyjnych.

3. Cele i podstawy przetwarzania

Cel	Podstawa prawna
Rejestracja, logowanie, zarządzanie kontem, uprawnieniami i świadczenie Usługi B2B	Art. 6 ust. 1 lit. f RODO (prawnie uzasadniony interes w wykonaniu umowy z Organizacją i obsłudze jej przedstawicieli), a gdy osoba fizyczna jest stroną umowy – również lit. b
Zaproszenia, administracja Organizacją, historia istotnych operacji	Art. 6 ust. 1 lit. f RODO – prawidłowe zarządzanie i rozliczalność działań
Faktury, rachunkowość i podatki	Art. 6 ust. 1 lit. c RODO – obowiązki prawne; w razie potrzeby lit. b lub f dla realizacji umowy
Raporty tygodniowe, alerty, komunikaty systemowe i rozliczeniowe	Art. 6 ust. 1 lit. f RODO (świadczenie usługi na rzecz Organizacji) albo lit. b, jeżeli osoba fizyczna jest stroną umowy
Kontakt, wsparcie i reklamacje	Art. 6 ust. 1 lit. b lub f RODO; lit. c, gdy zastosowanie ma obowiązek prawny
Działanie serwisu, ochrona kont, wykrywanie incydentów i zapobieganie nadużyciom bezpłatnego dostępu	Art. 6 ust. 1 lit. f RODO – bezpieczeństwo, zapobieganie oszustwom i obchodzeniu uzgodnionych ograniczeń; po przeprowadzeniu testu niezbędności i równowagi interesów

Cel	Podstawa prawna
Dobrowolny marketing e-mail MarketDrones i SenticLab	Art. 6 ust. 1 lit. a RODO – zgoda, z uwzględnieniem art. 398 Prawa komunikacji elektronicznej
Tworzenie i prezentowanie analiz zmian na publicznie dostępnych stronach i w dokumentach	Art. 6 ust. 1 lit. f RODO – uzasadniony interes w analizie i dokumentowaniu zmian rynkowych, po ocenie proporcjonalności; dane osób fizycznych są ograniczane, gdy jest to możliwe
Ustalenie, dochodzenie i obrona roszczeń oraz wypełnienie żądań uprawnionych organów	Art. 6 ust. 1 lit. f lub c RODO, zależnie od celu

Zgoda marketingowa jest osobna, dobrowolna i domyślnie niezaznaczona. Jej wycofanie jest możliwe w ustawieniach konta albo przez link w wiadomości i powoduje zaprzestanie wysyłki marketingowej. Nie wpływa na zgodność z prawem wcześniejszego przetwarzania ani na wiadomości niezbędne do świadczenia Usługi.

4. Skąd mamy dane

Dane otrzymujemy od Użytkowników i przedstawicieli Organizacji, od jej administratorów (w szczególności przy zaproszeniu członka zespołu), z technicznych zdarzeń systemowych, od partnerów uczestniczących w realizacji rozliczeń oraz z **publicznie dostępnych witryn i dokumentów** objętych monitoringiem. Dostępność materiału w internecie nie oznacza braku ochrony danych osobowych ani dowolności jego dalszego wykorzystania.

W odniesieniu do osób wymienionych w monitorowanych źródłach Administrator powinien odrębnie ocenić obowiązki informacyjne wynikające z **art. 14 RODO**, w tym ewentualne wyjątki, oraz możliwość wykonania praw tych osób. Informacje o zasadach monitoringu są dostępne przez niniejszą Politykę i adres kontaktowy.

5. Odbiorcy danych i dostawcy

1. Dane kont mogą być dostępne uprawnionym Użytkownikom i Administratorom **tej samej Organizacji** w zakresie wynikającym z ich ról. Administrator widzi istotne operacje administracyjne, ale nie widzi logowań, adresów IP ani historii aktywności analitycznej pracowników.
2. Upoważnione osoby w SenticLab uzyskują dostęp tylko wtedy, gdy jest to uzasadnione obsługą zgłoszenia, usunięciem awarii, zapewnieniem bezpieczeństwa, rozliczeniem lub obowiązkiem prawnym. Zakres jest minimalizowany, a dostęp rejestrowany.
3. **Hosting głównej aplikacji:** MikrUs, infrastruktura wskazana przez Operatora jako zlokalizowana w **Finlandii**. Dane mogą być przetwarzane także przez dostawcę służbowej poczty i poczty transakcyjnej, podmioty świadczące obsługę księgową i rozliczeniową, dostawcę linków do płatności online oraz podmioty technicznego wsparcia.

4. **Usługa analizy AI:** płatne **Google Gemini API** uruchamiane z projektu z aktywnym Cloud Billing, bez zadeklarowanego ograniczenia regionu przetwarzania do EOG. Do modelu przekazujemy materiały z monitorowanych źródeł, **nie dane kont Użytkowników, informacje rozliczeniowe ani ich osobiste preferencje**. Dane osobowe przypadkowo obecne w treści źródeł minimalizujemy lub usuwamy przed przekazaniem, gdy jest to możliwe.
5. W przypadku płatnego Gemini API Google deklaruje niewykorzystywanie przesyłanych promptów i odpowiedzi do ulepszania swoich modeli/produktów na warunkach Paid Services. Google opisuje logowanie promptów, kontekstu i odpowiedzi **przez 55 dni** na potrzeby bezpieczeństwa i wykrywania nadużyć. Szczegóły wynikają z warunków dostawcy, które mogą ulec zmianie: <https://ai.google.dev/gemini-api/terms> oraz <https://ai.google.dev/gemini-api/docs/usage-policies>.
6. Dane mogą zostać udostępnione organom publicznym wyłącznie na właściwej podstawie prawnej. Nie sprzedajemy danych użytkowników reklamodawcom.

6. Przekazywanie danych poza EOG

Przetwarzanie w ramach **Gemini API może odbywać się poza Europejskim Obszarem Gospodarczym**, w krajach, gdzie Google lub jego podwykonawcy dysponują infrastrukturą. Dotyczy to wyłącznie zakresu danych przekazanego do API, który może incydentalnie zawierać dane osobowe z monitorowanych materiałów.

W przypadku transferów danych osobowych Administrator stosuje odpowiednią podstawę prawną przewidzianą w rozdziale V RODO, w szczególności decyzję o odpowiednim stopniu ochrony lub standardowe klauzule umowne wraz z odpowiednimi zabezpieczeniami. O informacje dotyczące zabezpieczeń można zwrócić się na adres kontaktowy.

7. Okresy przechowywania

Rodzaj danych	Reguła retencji
Aktywne konto, konfiguracja i dane Organizacji	Przez okres korzystania z Usługi; po zakończeniu Abonamentu w ograniczonym dostępie 90 dni , następnie usunięcie, z wyjątkami prawnymi
Żądanie usunięcia konta	Niezwłoczne usunięcie z aktywnych systemów po skutecznym żądaniu, z zachowaniem danych wymaganych prawem lub prawidłowo uzasadnionego wyjątku antynadużyciowego
Kopie bezpieczeństwa	Rotacja i usunięcie/automatyczne nadpisanie do 7 dni ; po odtworzeniu backupu wcześniejsze usunięcia są respektowane

Rodzaj danych	Reguła retencji
Logi techniczne, bezpieczeństwa i dostępu administracyjnych SentoLab	Standardowo 180 dni , z możliwością dłuższego przetwarzania tylko w odpowiednio udokumentowanej sprawie incydentu, roszczenia lub obowiązku prawnego
Historia istotnych operacji administracyjnych Organizacji	Standardowo 180 dni ; dostępna administratorom własnej Organizacji w ograniczonym zakresie
Zaproszenie do Organizacji	Link ważny 14 dni ; dane zaproszenia niezaakceptowanego, wygasłego albo anulowanego usuwane 30 dni po wygaśnięciu lub anulowaniu , o ile brak odrębnej podstawy prawnej
Historia akceptacji Regulaminu oraz zgód marketingowych	Do usunięcia konta; po usunięciu konta usuwana, z wyjątkiem danych, których dalsze zachowanie jest prawnie wymagane
Reklamacje	12 miesięcy od zakończenia sprawy , gdy konto nadal istnieje; po skutecznym żądaniu usunięcia konta usunięcie niezwłoczne, chyba że dalsza retencja jest wymagana prawem
Faktury i dokumentacja podatkowo-księgowa	Wyłącznie przez okres, którego wymagają właściwe przepisy podatkowe i rachunkowe
Potwierdzone nadużycia bezpłatnego dostępu	12 miesięcy od potwierdzenia nadużycia : minimalne identyfikatory, data i przyczyna blokady; oddzielnie od usuniętego konta, tylko gdy test równowagi potwierdza niezbędność dalszego przetwarzania
Treści z monitorowanych źródeł, w tym incydentalne dane osób fizycznych	Przez okres uzasadniony potrzebą dokumentowania historii zmian i świadczenia Usługi;

7.1. Minimalny rejestr potwierdzonych nadużyć — szczególna zasada

1. Rejestr służy **wyłącznie** rozpoznawaniu powtarzających się prób bezprawnego obchodzenia zasad bezpłatnego dostępu. Nie jest wykorzystywany do marketingu, analiz zachowania klientów ani komercyjnego profilowania.
2. **Samo podejrzenie nie skutkuje trwałym wpisem.** Wpis następuje po potwierdzeniu nadużycia w ramach weryfikacji przez upoważnioną osobę i zapisaniu związanego uzasadnienia.
3. Przetwarzamy tylko te identyfikatory Użytkownika lub Organizacji, które są rzeczywiście niezbędne do rozpoznania ponownego nadużycia; nie przechowujemy w tym celu pełnego profilu, historii przeglądania ani całej korespondencji. Skróty kryptograficzne identyfikatorów również mogą stanowić dane osobowe.

4. Okres przechowywania wynosi **12 miesięcy od potwierdzenia konkretnego nadużycia**. Uprawnienia dostępu są ograniczone, a po okresie retencji wpis jest usuwany, chyba że konkretna odrębna podstawa prawna wymaga zachowania określonych danych.
5. Wpis może pozostać po usunięciu konta tylko pod warunkiem, że Operator udokumentował podstawę przetwarzania, niezbędność i proporcjonalność. Użytkownik może zażądać ponownej oceny, skorzystać z prawa sprzeciwu oraz innych uprawnień na zasadach RODO.

8. Cookies, localStorage i statystyki

1. W serwisie i Panelu korzystamy wyłącznie z **technicznych cookies i/lub localStorage**, służących uwierzytelnieniu, utrzymaniu sesji, bezpieczeństwu, funkcjom wymaganych przez Użytkownika i ustawieniom interfejsu.
2. Nie stosujemy narzędzi śledzenia reklamowego ani analitycznych plików cookies, pikseli marketingowych i zewnętrznych systemów analizy zachowania użytkowników.
3. Przeglądarka może umożliwiać ograniczenie cookies, jednak zablokowanie niezbędnych mechanizmów może uniemożliwić korzystanie z konta.
4. Możemy tworzyć **rzeczywiście anonimowe, zbiorcze statystyki** na podstawie danych już przetwarzanych do realizacji Usługi, np. liczbę Organizacji, monitorowanych marek, wykrytych zmian lub raportów. Nie tworzymy w tym celu dodatkowej historii zachowania Użytkowników.

9. Uprawnienia i dostęp administracyjny

Administrator Organizacji może przeglądać historię istotnych operacji organizacyjnych wraz z datą i osobą wykonującą działanie. Nie widzi historii logowań, adresów IP, historii przeglądania treści ani wyszukiwań. Dostęp upoważnionych osób SentioLab do danych klienta jest ograniczony do uzasadnionych zadań (wsparcie, awarie, bezpieczeństwo, rozliczenia, obowiązki prawne) i odnotowywany w logach dostępu.

10. AI i decyzje zautomatyzowane

1. Gemini służy analizowaniu zmian rynkowych, a nie profilowaniu Użytkowników MarketDrones. Nie przekazujemy dostawcy AI danych kont, informacji o rozliczeniach ani preferencji Użytkowników.
2. Nie podejmujemy **wyłącznie w sposób zautomatyzowany** wobec Użytkowników decyzji wywołujących skutki prawne lub podobnie istotnie na nich wpływających w rozumieniu art. 22 RODO. Ocena i utrwalenie potwierdzonego nadużycia bezpłatnego dostępu wymaga odpowiedniej weryfikacji przez upoważnioną osobę.
3. Treści AI mogą zawierać błędy i nie powinny stanowić jedynej podstawy istotnych decyzji biznesowych.

11. Prawa osób, których dane dotyczą

Z zastrzeżeniem warunków określonych w RODO przysługuje prawo dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, wniesienia **sprzeciwu** wobec przetwarzania na podstawie uzasadnionego interesu (w tym danych antynadużyciowych) oraz wycofania zgody. Żądania można składać na info@marketdrones.net. Odpowiadamy bez zbędnej zwłoki, zasadniczo w ciągu **miesiąca**, z możliwością zgodnego z RODO przedłużenia tego terminu i poinformowania osoby.

Można złożyć skargę do **Prezesa Urzędu Ochrony Danych Osobowych**: <https://uodo.gov.pl/>. Zgłoszenie żądania nie oznacza automatycznego spełnienia go w całości, jeżeli istnieją zgodne z prawem podstawy ograniczenia danego prawa; w takim przypadku udzielimy wyjaśnienia.

12. Czy podanie danych jest obowiązkowe?

Dane wymagane do utworzenia konta, uwierzytelnienia i przypisania do Organizacji są niezbędne do korzystania z Usługi. Podanie danych do fakturowania jest konieczne do zawarcia odpłatnego Abonamentu. Zgoda na marketing jest **dobrowolna** i nie warunkuje uzyskania dostępu.

13. Zmiany Polityki

Polityka może być aktualizowana w związku ze zmianą prawa, infrastruktury, podwykonawców i sposobu świadczenia Usługi. Istotne zmiany przetwarzania danych będą komunikowane w sposób adekwatny do okoliczności i wymogów prawa. Wersje językowe PL/EN powinny być spójne; dla rozbieżności warunków umownych pierwszeństwo wersji polskiej określa Regulamin.