

NEGOTIVO — Polityka Prywatności / Privacy Policy

Table of Contents

NEGOTIVO — POLITYKA PRYWATNOŚCI / PRIVACY POLICY	1
CZĘŚĆ I — WERSJA POLSKA (WIAŻĄCA)	1
PART II — ENGLISH VERSION (FOR REFERENCE ONLY).....	12

NEGOTIVO — POLITYKA PRYWATNOŚCI / PRIVACY POLICY

Dokument dwujęzyczny — Wersja polska jest wersją wiążącą. W razie rozbieżności pierwszeństwo ma wersja polska.

Bilingual document — The Polish version is the binding version. In case of discrepancies, the Polish version prevails.

CZĘŚĆ I — WERSJA POLSKA (WIAŻĄCA)

POLITYKA PRYWATNOŚCI APLIKACJI NEGOTIVO

1. WSTĘP I POSTANOWIENIA OGÓLNE

Język i wersja wiążąca:

Niniejsza Polityka Prywatności Aplikacji Negotivo została sporządzona w wielu wersjach językowych. W celu uniknięcia wątpliwości:

- w przypadku Konsumentów zamieszkałych w Polsce, wersja polska jest > wiążąca w pełnym zakresie wymaganym przez bezwzględnie > obowiązujące przepisy polskiego prawa;
- w przypadku Użytkowników, nie będących Konsumentami, w razie > rozbieżności wersją nadrzędną i wiążącą jest wersja polska.

Zastrzeżenie: *Negotivo jest platformą technologiczną do rozwiązywania sporów. Administrator nie jest podmiotem ADR (Alternative Dispute Resolution) i nie działa w ramach systemu licencjonowanych podmiotów ADR. Świadczymy usługi automatyzacji i wsparcia procesów negocjacji przedsądowych na potrzeby działalności gospodarczej oraz wsparcia Konsumentów.*

2. DEFINICJE

- 1) **Administrator** - spółka pod firmą NEGOTIVO Prosta Spółka Akcyjna > z siedzibą w Puławach przy ul. Ignacego Mościckiego 1, 24-110 > Puławy, wpisana do Rejestru

Przedsiębiorców Krajowego Rejestru > Sądowego pod nr KRS: 0001197501, NIP: 7162849640, REGON: > 542861449;

- 2) **Aplikacja** – oprogramowanie udostępniane przez Administratora > (aplikacja mobilna, panel webowy), służące do zarządzania sporami, > analizy luk i generowania projektów dokumentów prawnych;
- 3) **Zewnętrzna Platforma Sprzedażowa** – zewnętrzny system e-commerce > lub marketplace (np. Shopify, WooCommerce, Amazon), z którym > zintegrowana jest Aplikacja;
- 4) **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub > możliwej do zidentyfikowania osobie fizycznej.
- 5) **Podmiot danych** - osoba fizyczna, której dotyczą Dane osobowe, w > szczególności Użytkownik, Składający Skargę, Odpowiadający (w tym > przedstawiciel Przedsiębiorcy/Merchanta) oraz Kurator.
- 6) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) > 2016/679 z dnia 27 kwietnia 2016 r.
- 7) **CCPA / CPRA** – California Consumer Privacy Act oraz California > Privacy Rights Act (przepisy o ochronie prywatności obowiązujące w > stanie Kalifornia, USA).

3. **ROLA ADMINISTRATORA I PROCESORA**

Z uwagi na specyfikę Aplikacji, Administrator może występować w dwóch rolach:

- 1) **jako Administrator** - w odniesieniu do Danych osobowych > Użytkowników zakładających Konto w Aplikacji (np. Konsumentów > rozwiązujących spór C2C, Przedsiębiorców, personelu sklepów, > Kuratorów) oraz w zakresie realizacji własnych obowiązków > prawnych, podatkowych, księgowych, zapewnienia bezpieczeństwa > systemu oraz ustalenia, dochodzenia lub obrony roszczeń.
- 2) **jako Podmiot Przetwarzający (procesor)** – w odniesieniu do > Danych osobowych Konsumentów wprowadzanych do Aplikacji przez > Przedsiębiorców (lub pobieranych za pośrednictwem API Zewnętrznych > Platform Sprzedażowych, np. Shopify) w ramach obsługi spraw B2B. > Administratorem danych pozostaje wtedy Przedsiębiorca, a > Administrator przetwarza dane wyłącznie na jego polecenie, na > podstawie odrębnej umowy powierzenia przetwarzania danych.

4. **OCHRONA DZIECI (PRYWATNOŚĆ MAŁOLETNICH)**

Usługi świadczone przez Administratora nie są skierowane do osób poniżej 18. roku życia. Świadomie nie zbieramy Danych osobowych od małoletnich. W przypadku powzięcia informacji o zgromadzeniu danych osoby niepełnoletniej, niezwłocznie podejmiemy kroki w celu ich usunięcia i zamknięcia powiązanego Konta. Jeśli rodzic lub opiekun prawny uważa, że zgromadziliśmy dane dziecka, prosimy o pilny kontakt pod adresem privacy@negotivo.com.

5. **SZCZEGÓŁOWY ZAKRES ZBIERANYCH DANYCH**

W zależności od roli Użytkownika, zbieramy następujące kategorie danych:

1) Dane Przedsiębiorców i ich personelu:

- a. informacje o prowadzonym przedsiębiorstwie: nazwa, domena, ID > Sklepu (z platformy zewnętrznej), plan subskrypcji, dane > rozliczeniowe (jeżeli dotyczy);
- b. dane administracyjne: imiona, nazwiska, służbowe adresy e-mail i > numery telefonów członków zespołu posiadających dostęp do > Aplikacji;
- c. dane konfiguracyjne: reguły automatycznego rozstrzygania sporów, > preferencje powiadomień, progi kwotowe dla ugód;
- d. dane o wydajności i analityka: zagregowane wskaźniki sporów, > wskaźniki sukcesu ugód, czasy reakcji.

2) dane Użytkowników innych niż Przedsiębiorców (w tym Konsumentów):

- a. informacje o tożsamości: imię i nazwisko, adres e-mail, numer > telefonu;
- b. informacje o przedmiocie sporu, np.: identyfikatory zamówień, > opisy produktów, daty transakcji, kwoty, ograniczone > informacje o metodzie płatności (wyłącznie np. 4 ostatnie > cyfry karty; nie przechowujemy pełnych danych kart > płatniczych);
- c. dane komunikacyjne i dowodowe: wiadomości, zdjęcia, zrzuty > ekranu, korespondencja ze sprzedawcą, dokumentacja techniczna > wgrana w ramach sporu. Dokumenty te są przetwarzane także z > użyciem technologii OCR (w celu ekstrakcji tekstu.
- d. informacje o Koncie: dane z systemów autoryzacji OAuth (Google, > Apple);
- e. dane z urządzeń i dane techniczne: adresy IP, typ urządzenia, > system operacyjny;
- f. historia sporów: pełne rejestry zgłoszonych roszczeń, wyniki > ugód, komunikacja z mediatorem (kuratorem).

3) Dane pobierane z Zewnętrznych Platform Sprzedażowych

- a) w przypadku integracji (np. poprzez autoryzację OAuth z Shopify), > uzyskujemy dostęp (za zgodą Przedsiębiorcy) do: danych > kontaktowych klienta powiązanych z zamówieniem, historii > transakcji, statusu realizacji i śledzenia przesyłek. Aplikacja > żąda wyłącznie minimalnych uprawnień API (tzw. *scopes*) > niezbędnych do obsługi sporu.

6. **CELE ORAZ PODSTAWY PRAWNE PRZETWARZANIA**

W zależności od tego, w jakiej roli korzystasz z naszej Aplikacji, przetwarzamy Twoje dane osobowe w różnych celach. Poniżej przedstawiamy szczegółowe cele przetwarzania oraz odpowiadające im podstawy prawne:

1. **Rejestracja i obsługa Konta Użytkownika**

Zakres: Rejestracja konta Użytkownika wymaga podania niezbędnych w tym celu danych określonych w formularzu rejestracyjnym. W ramach edycji danych konta możesz podać swoje dalej idące dane. Ponadto nasz system wykorzystywany do obsługi kont zapisuje Twój numer IP użyty podczas rejestracji. Dane przetwarzane są w celu świadczenia na Twoją rzecz usługi konta Użytkownika. Po usunięciu konta dane trafiają do archiwum na potrzeby ewentualnego ustalenia, dochodzenia lub obrony roszczeń. Podanie tych danych jest warunkiem korzystania z Aplikacji.

Podstawa prawna: Niezbędność do wykonania umowy o świadczenie usług drogą elektroniczną (art. 6 ust. 1 lit. b RODO).

2. **Świadczenie usług dla Przedsiębiorców i integracje**

Zakres: Obsługa konta Przedsiębiorcy, w tym integracja z Zewnętrznymi Platformami Sprzedażowymi, pozyskiwanie danych o zamówieniach i sporach, konfiguracja zasad rozstrzygania sporów, obsługa subskrypcji i płatności (poprzez systemy płatności Zewnętrznej Platformy Sprzedażowej, np. Shopify Billing API), komunikacja z zespołem Przedsiębiorcy oraz generowanie raportów. Po wykonaniu umowy, dane trafiają do archiwum oraz do dokumentacji księgowej na potrzeby wywiązywania się z obowiązków podatkowych.

Podstawa prawna: Niezbędność do wykonania umowy (art. 6 ust. 1 lit. b RODO) oraz prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO).

3. **Obsługa sporów, reklamacji i obciążeń zwrotnych (dla Kupujących / > Konsumentów)**

Zakres: Przyjmowanie i obsługa sporów (reklamacji, obciążeń zwrotnych), komunikacja za pośrednictwem Aplikacji, gromadzenie dowodów (w tym przetwarzanie obrazów za pomocą technologii OCR), analiza sporu z wykorzystaniem sztucznej inteligencji (AI), generowanie propozycji ugód, dokumentowanie wyniku sporu. Jeżeli składasz reklamację lub odstępujesz od umowy, przekazujesz dane osobowe zawarte w treści oświadczeń. Podanie danych jest warunkiem przeprowadzenia procesu reklamacyjnego.

Podstawa prawna: Niezbędność do wykonania umowy (art. 6 ust. 1 lit. b RODO), wypełnienie obowiązku prawnego w zakresie praw konsumenta (art. 6 ust. 1 lit. c RODO) oraz prawnie uzasadniony interes Administratora i Stron (art. 6 ust. 1 lit. f RODO).

4. **Certyfikacja Porozumień (ChainProof)**

Zakres: W celu zapewnienia niezaprzeczalności i autentyczności osiągniętych ugód lub wygenerowanych dokumentów, Aplikacja wykorzystuje technologię blockchain. Przetwarzanie ogranicza się do generowania i zapisu

kryptograficznych skrótów (tzw. hash) z dokumentów w sieci Hyperledger, bez ujawniania na zewnątrz samych Danych osobowych Użytkowników.

Podstawa prawna: Prawnie uzasadniony interes Administratora oraz stron sporu, polegający na zapewnieniu niepodważalności zawartych porozumień i bezpieczeństwa obrotu (art. 6 ust. 1 lit. f RODO).

5. **Kontakt i obsługa korespondencji**

Zakres: Kontaktując się z nami za pośrednictwem dostępnych środków komunikacji (np. poczty elektronicznej, komunikatora, infolinii), przekazujesz swoje dane osobowe zawarte w treści korespondencji. Podanie danych jest warunkiem nawiązania kontaktu. System komunikacji zapisuje także Twój adres IP. Dane przetwarzane są w celu prowadzenia komunikacji. Po jej zakończeniu trafiają do archiwum.

Podstawa prawna: Prawnie uzasadniony interes Administratora polegający na prowadzeniu korespondencji i obsłudze zapytań (art. 6 ust. 1 lit. f RODO).

6. **Realizacja obowiązków podatkowych i księgowych**

Zakres: Realizujemy obowiązki podatkowe i księgowe, w szczególności w postaci wystawienia faktury, włączenia jej do naszej dokumentacji księgowej oraz przechowywania dokumentacji rozliczeniowej. Przetwarzamy m.in. imię i nazwisko, firmę, adres działalności, numer NIP. Podanie tych danych jest konieczne, by zachować zgodność z prawem.

Podstawa prawna: Niezbędność do wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO w zw. z właściwymi przepisami prawa podatkowego).

7. **Tworzenie archiwum**

Zakres: Na potrzeby naszej działalności tworzymy archiwa cyfrowe. Do archiwów trafiają dane osobowe, które przetwarzaliśmy w związku z Tobą, a ich zakres może się różnić w zależności od rodzaju sprawy (np. zakończone spory, dokumentacja wygenerowana z systemu).

Podstawa prawna: Prawnie uzasadniony interes polegający na porządkowaniu, organizowaniu i archiwizowaniu nośników danych (art. 6 ust. 1 lit. f RODO).

8. **Obrona, ustalenie lub dochodzenie roszczeń**

Zakres: Korzystanie z Aplikacji oraz zawieranie z nami umów może rodzić w przyszłości roszczenia po naszej lub Twojej stronie. W związku z tym jesteśmy uprawnieni do przetwarzania wszelkich Danych osobowych, które wiążą się z danym roszczeniem, w tym logów aktywności, zapisów czatów i dokumentacji dowodowej.

Podstawa prawna: Prawnie uzasadniony interes polegający na ochronie naszych interesów, dochodzeniu praw oraz obronie w postępowaniach przed sądami i organami (art. 6 ust. 1 lit. f RODO).

9. **Analiza i statystyka**

Zakres: Prowadzimy działania analityczne z wykorzystaniem narzędzi zewnętrznych dostawców (np. Google Analytics). Analizujemy, w jaki sposób Użytkownicy korzystają z platformy, wykrywamy błędy UX oraz badamy skuteczność argumentacji prawnych generowanych przez AI. Z poziomu narzędzi mamy wgląd w zasadzie wyłącznie do Informacji Anonimowych lub wysoce zagregowanych statystyk.

Podstawa prawna: Prawnie uzasadniony interes polegający na optymalizacji Aplikacji, poprawie jakości usług i wyciąganiu wniosków biznesowych (art. 6 ust. 1 lit. f RODO).

10. **Marketing własny (w tym Newsletter)**

Zakres: Prowadzimy działania marketingowe polegające na przesyłaniu informacji handlowych, nowości o platformie (Newsletter) oraz ewentualnym dopasowywaniu treści reklamowych z wykorzystaniem odpowiednich plików cookies. Działania te oparte są zawsze o Twoją wyraźną zgodę.

Podstawa prawna: Dobrowolna zgoda osoby, której dotyczą dane (art. 6 ust. 1 lit. a RODO).

11. **Realizacja obowiązków związanych z ochroną danych (RODO) oraz > bezpieczeństwem (DSA)**

Zakres: Jako administrator jesteśmy zobowiązani do udowodnienia przestrzegania RODO (zasada rozliczalności), rozpatrywania Twoich żądań dotyczących prywatności, a także do reagowania na zgłoszenia nielegalnych treści zgodnie z Aktem o usługach cyfrowych (Digital Services Act). W tym celu przetwarzamy dane zgłaszającego oraz logi systemowe.

Podstawa prawna: Wypełnienie obowiązku prawnego (art. 6 ust. 1 lit. c RODO) oraz prawnie uzasadniony interes w postaci zabezpieczenia dowodów realizacji wniosków (art. 6 ust. 1 lit. f RODO).

12. **Profile na portalach społecznościowych**

Zakres: Administrator posiada profile na portalach Facebook i LinkedIn. Przetwarza Dane osobowe osób odwiedzających te profile (komentarze, polubienia) w celu promowania własnej marki i komunikacji.

Podstawa prawna: Prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO).

7. **SZTUCZNA INTELIGENCJA (AI) I ZAUTOMATYZOWANE DECYZJE**

Aplikacja wykorzystuje systemy AI (m.in. Google Gemini, sieci Bayesowskie, mechanizm *Negative Exclusion*) do analizy spraw i generowania rekomendacji ugód.

- Analiza sentymentu: System dokonuje analizy tonu wypowiedzi (np. > pilny, sfrustrowany, neutralny) w celu kategoryzacji i > priorytetyzacji zgłoszeń (nie w celu dyskryminacji lub odmowy > usług).

- Brak wyłącznej decyzyjności maszyn (poza zdefiniowanymi regułami): > Ostateczna decyzja zawsze należy do człowieka. Wyjątkiem są progi > *Auto-Settlement* (np. zwrot środków przy sporach poniżej > określonej kwoty), które Przedsiębiorca sam, świadomie i z góry > skonfigurował – jest to realizacja woli Przedsiębiorcy, a nie > autonomiczna decyzja maszyny.
- Prawa Konsumenta: Konsument ma prawo zakwestionować decyzję > wygenerowaną przez system i zażądać interwencji człowieka.
- Trening modeli: kategorycznie zabrania się wykorzystywania Danych > osobowych Użytkowników do trenowania publicznych modeli AI. Modele > środowiska testowego korzystają z danych syntetycznych lub > zanonimizowanych.

8. ODBIORCY DANYCH I TRANSFER MIĘDZYNARODOWY

Starannie dobieramy podmioty, z którymi współpracujemy. Odbiorcami danych mogą być:

- **Dostawca infrastruktury chmurowej:** Google Cloud Platform > (przechowywanie danych, bazy danych - serwery w Europie).
- **Dostawca usług AI:** Google Vertex AI (jako procesor analizujący > spory w wyizolowanym środowisku).
- **Dostawcy komunikacyjni:** Mailgun (e-mail), SMSAPI (SMS).
- **Dostawcy platform zewnętrznych:** Shopify, itp. (w zakresie > wymiany danych przez API).
- **Dostawcy płatności:** systemy bilingowe platform lub zewnętrzni > operatorzy płatności.

Transfery poza EOG:

Administrator przechowuje dane na serwerach GCP zlokalizowanych w UE (np. Belgia, Frankfurt, Holandia). W przypadku, gdy dostawcy narzędzi analitycznych lub wspierających transferują dane poza Europejski Obszar Gospodarczy (EOG), opieramy się na decyzjach Komisji Europejskiej stwierdzających odpowiedni stopień ochrony (np. *EU-U.S. Data Privacy Framework*) oraz na wiążących Standardowych Klauzulach Umownych (SCC).

9. OKRES RETENCJI (PRZECZOWYWANIA) I USUWANIE DANYCH

- 1) Dane Użytkowników: przechowywane przez czas aktywności konta oraz > minimalnie przez 1 rok po jego zamknięciu w celach prawnych i > rozliczeniowych.
- 2) Historia sporów i dowody: Przechowywane przez okres 7 lat od momentu > zamknięcia lub rozwiązania sporu. Okres ten jest niezbędny do > zabezpieczenia przed opóźnionymi roszczeniami typu chargeback z > instytucji płatniczych oraz do obrony przed roszczeniami prawnymi. > Po tym czasie dokumentacja jest trwale usuwana.

- 3) Logi systemowe (dane zautomatyzowane): przechowywane przez 90 dni, a > następnie usuwane lub całkowicie zagregowane.
- 4) Wymogi Zewnętrznych Platform Zakupowych (np. Shopify webhooks): > Administrator w pełni obsługuje obowiązkowe mechanizmy > prywatności. W przypadku otrzymania z platformy żądania > (customers/data_request, customers/redact, shop/redact), dane są > lokalizowane i usuwane w wymaganym czasie, chyba że nadrzędne > prawo nakazuje ich dłuższą retencję dla celów dowodowych.
- 5) Odinstalowanie Aplikacji – odinstalowanie Aplikacji \z systemu > zewnętrznego (np. Shopify) automatycznie inicjuje proces usuwania > danych powiązanych z danym Przedsiębiorcą z naszych systemów, poza > danymi wymaganymi przez prawo do archiwizacji.

10. PRAWA PODMIOTÓW DANYCH – RODO (DLA MIESZKAŃCÓW EUROPY)

Zgodnie z RODO (oraz prawem polskim), przysługują Ci następujące prawa:

- Prawo dostępu do danych i otrzymania ich kopii;
- Prawo do sprostowania (poprawienia) niedokładnych lub niekompletnych > informacji;
- Prawo do usunięcia danych (prawo do bycia zapomnianym) z > zastrzeżeniem wymogów retencji wynikających z obrony roszczeń;
- Prawo do ograniczenia przetwarzania;
- Prawo do przenoszenia danych w powszechnie używanym formacie;
- Prawo do sprzeciwu wobec przetwarzania opartego na uzasadnionym > interesie (w tym sprzeciwu wobec określonego profilowania);
- Prawo cofnięcia zgody, jeżeli uprzednio taką wyraziłeś;
- Prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych > (PUODO) w Polsce lub innego właściwego organu nadzorczego w Twoim > kraju.

Żądania należy kierować na adres: privacy@negotivo.com lub office@negotivo.com. Czas reakcji wynosi do 30 dni kalendarzowych.

11. DODATKOWE PRAWA DLA MIESZKAŃCÓW KALIFORNII (USA) – CCPA / CPRA

Jeżeli jesteś mieszkańcem stanu Kalifornia, przepisy CCPA (California Consumer Privacy Act) oraz CPRA (California Privacy Rights Act) przyznają Ci dodatkowe i specyficzne prawa dotyczące Twoich danych.

1. Prawa na mocy CCPA i CPRA:
 - Prawo do wiedzy (Right to Know): masz prawo zażądać informacji o > tym, jakie kategorie danych osobowych zbieramy, wykorzystujemy i > ujawniamy na Twój temat.

- Prawo do usunięcia (Right to Delete): masz prawo zażądać usunięcia > swoich danych osobowych, z zastrzeżeniem wyjątków prawnych (np. > sfinalizowanie transakcji, spory prawne).
- Prawo do rezygnacji ze sprzedaży i udostępniania (Right to Opt-Out): > masz prawo zabronić "sprzedaży" lub "udostępniania" Twoich > danych. Zaznaczamy, że nie sprzedajemy Twoich danych osobowych w > tradycyjnym rozumieniu tego słowa. Udostępniamy je wyłącznie > naszym dostawcom usług (Service Providers). Możesz zrezygnować z > udostępniania kontaktując się z nami.
- Prawo do sprostowania (Right to Correct): prawo do żądania > poprawienia nieścisłych danych.
- Prawo do ograniczenia użycia danych wrażliwych (Right to Limit Use): > prawo do zażądania ograniczenia użycia wrażliwych danych osobowych > wyłącznie do celów niezbędnych do świadczenia usług.
- Prawo do rezygnacji z zautomatyzowanego podejmowania decyzji (Right > to Opt-Out of Automated Decision-Making): prawo do rezygnacji z > profilowania, które wywołuje wobec Ciebie istotne skutki prawne (z > zastrzeżeniem niezbędności algorytmów do działania samej platformy > w przypadku dobrowolnego korzystania z niej).
- Prawo do niedyskryminacji (Right to Non-Discrimination): zapewniamy, > że nie będziemy Cię dyskryminować (np. poprzez odmowę usług, > zmiany cen) za skorzystanie z przysługujących Ci praw CCPA/CPRA.
- Prawo do odwołania (Right to Appeal): Jeśli odrzucimy Twoje żądanie, > masz prawo odwołać się od tej decyzji.

1. Jak złożyć wniosek CCPA:

Wnioski prosimy kierować na adres e-mail: privacy@negotivo.com z dopiskiem w tytule: *"CCPA Data Request"*. Zastrzegamy sobie prawo do weryfikacji Twojej tożsamości przed realizacją żądania.

2. Prawo „Shine the Light” (California Civil Code Section 1798.83):

Mieszkańcy Kalifornii mają prawo zażądać informacji o kategoriach danych osobowych udostępnionych stronom trzecim do ich własnych celów marketingu bezpośredniego. Wnioski te należy zgłaszać pod ww. adres e-mail z tematem *"California Shine the Light Request"*.

12. **PLIKI COOKIES I TECHNOLOGIE ŚLEDZĄCE**

W ramach Aplikacji (zarówno w aplikacji mobilnej, jak i panelu webowym) korzystamy z plików „cookies” (tymczasowych plików sesyjnych oraz plików stałych) oraz podobnych technologii śledzących (np. JWT - JSON Web Tokens, Local Storage) w celach:

1. Niezbędnych (Essential): umożliwienie logowania, uwierzytelnianie > Użytkownika za pomocą bezpiecznych tokenów (np. za pośrednictwem > Firebase Auth), utrzymanie

aktywnej sesji, zabezpieczenie > formularzy (ochrona CSRF) oraz podtrzymanie stanu rozmowy i > kontekstu dla modułu AI (system RAG). Bez tych technologii > Aplikacja nie będzie funkcjonować poprawnie.

2. Analitycznych i wydajnościowych (Performance & Analytics): > gromadzenie zbiorczych statystyk odwiedzin, śledzenie ścieżek > nawigacji, identyfikacja typu urządzenia oraz przeglądarki, w celu > bieżącego ulepszania interfejsu i wykrywania błędów UX. W tym celu > wykorzystujemy narzędzia zewnętrzne, w szczególności Google > Analytics (dostawca: Google Ireland Ltd.). Dane pozyskiwane za > pomocą tych plików stanowią co do zasady Informacje Anonimowe, > które nie pozwalają na bezpośrednią identyfikację osoby.
3. Funkcjonalnych i Marketingowych: zapamiętywanie indywidualnych > preferencji Użytkownika (np. wybór języka, motywu wizualnego > jasny/ciemny). Ponadto, wyłącznie na stronach promocyjnych i typu > *landing page* (poza głównym panelem rozstrzygania sporów), możemy > używać narzędzi takich jak Google Ads oraz Meta Pixel (dostawca: > Meta Platforms Ireland Ltd.) w celu mierzenia skuteczności naszych > kampanii i dopasowywania treści reklamowych.

Dane o lokalizacji:

W przypadku korzystania z Aplikacji mobilnej, za uprzednią i wyraźną zgodą Użytkownika udzieloną na poziomie ustawień systemu operacyjnego, możemy zbierać precyzyjne dane o lokalizacji. Służą one wyłącznie do obsługi określonych funkcjonalności Aplikacji (np. osadzania widgetów dowodowych lub precyzowania miejsca zdarzenia w ramach toczzonego sporu).

Zarządzanie preferencjami:

Możesz zarządzać plikami cookies poprzez odpowiednie ustawienia swojej przeglądarki internetowej (np. Chrome, Safari, Firefox, Opera), w tym włączyć funkcję blokowania lub opcji "opt-out". Należy jednak pamiętać, że zablokowanie plików *sesyjnych* (niezbędnych) uniemożliwi Ci zalogowanie się do panelu i korzystanie z funkcjonalności Aplikacji. W przypadku instalacji specjalnego pliku "opt-out", pamiętaj, że działa on wyłącznie w przeglądarce, w której został zapisany.

13. KONTAKT W SPRAWACH PRYWATNOŚCI

Z pytaniami dotyczącymi niniejszej Polityki Prywatności, żądaniami dostępu do danych oraz skargami prosimy zwracać się na:

- e-mail: **privacy@negotivo.com** lub **office@negotivo.com**
- adres korespondencyjny: NEGOTIVO Prosta Spółka Akcyjna, ul. Ignacego > Mościckiego 1, 24-110 Puławy, Polska.

W razie nierozwiązania sporu na linii Użytkownik-Administrator, przysługuje prawo skargi do organów:

- w Polsce: Urząd Ochrony Danych Osobowych (UODO) - > <https://uodo.gov.pl/>

- w Kalifornii: California Attorney General, Office of Privacy > Protection - <https://oag.ca.gov/privacy>
- w innych krajach UE: Właściwy krajowy organ nadzorczy ochrony > danych.

14. ZMIANY W POLITYCE PRYWATNOŚCI

Z uwagi na fakt, że Aplikacja znajduje się obecnie w fazie wczesnego uruchomienia (wersja Beta / MVP) i podlega intensywnemu rozwojowi, a także ze względu na dynamiczne zmiany w przepisach (np. RODO, AI Act, DSA, regulacje w USA), niniejsza Polityka może ulegać modyfikacjom. W przypadku wprowadzenia istotnych zmian, Administrator poinformuje zarejestrowanych Użytkowników za pośrednictwem poczty elektronicznej lub poprzez wyraźny komunikat wewnątrz panelu Aplikacji. Dalsze korzystanie z Aplikacji po otrzymaniu zawiadomienia oznacza akceptację zaktualizowanych zasad.

PART II — ENGLISH VERSION (FOR REFERENCE ONLY)

NEGOTIVO PRIVACY POLICY

1. INTRODUCTION AND GENERAL PROVISIONS

Language and binding version:

This Privacy Policy of the Negotivo App has been drafted in multiple language versions. For the avoidance of doubt:

- in the case of Consumers residing in Poland, the Polish version is > binding to the full extent required by the mandatory provisions of > Polish law;
- in the case of Users who are not Consumers, in the event of > discrepancies, the Polish version is the superior and binding > version.

***Disclaimer:** Negotivo is a technology platform for dispute resolution. The Administrator is not an ADR (Alternative Dispute Resolution) entity and does not operate within the ADR Licensed Entity System. We provide automation and support services for pre-litigation negotiations for business and consumer support.*

2. DEFINITIONS

- 1) **Administrator** – a company under the name of NEGOTIVO Prosta > Spółka Akcyjna with its registered office in Puławy at Ignacego > Mościckiego 1 Street, 24-110 Puławy, entered into the Register of > Entrepreneurs of the National Court Register under KRS number: > 0001197501, NIP: 7162849640, REGON: 542861449;
- 2) **Application** – software made available by the Administrator > (mobile application, web panel), used for dispute management, gap > analysis and generation of draft legal documents;
- 3) **External Sales Platform** – an external e-commerce system or > marketplace (e.g. Shopify, WooCommerce, Amazon) with which the > Application is integrated;
- 4) **Personal data** – any information about an identified or > identifiable natural person.
- 5) **Data Subject** – a natural person to whom the Personal Data > relates, in particular the User, the Complainant, the Responder > (including the Entrepreneur's/Merchant's representative) and the > Curator.
- 6) **GDPR** – Regulation (EU) 2016/679 of the European Parliament and > of the Council of 27 April 2016
- 7) **CCPA/CPRA** – California Consumer Privacy Act and California > Privacy Rights Act.

3. ADMINISTRATOR AND PROCESSOR ROLE

Due to the specificity of the Application, the Administrator may act in two roles:

- 1) **as the Administrator** - in relation to the Personal Data of Users > creating an Account in the Application (e.g. Consumers resolving a > C2C dispute, Entrepreneurs, store

staff, curators) and in the > scope of fulfilling their own legal, tax and accounting > obligations, ensuring system security and establishing, pursuing > or defending claims.

- 2) **as a Processor** – in relation to Consumer Personal Data entered > into the Application by Entrepreneurs (or downloaded via the API > of Third-Party Sales Platforms, e.g. Shopify) as part of B2B > matters. The Entrepreneur then remains the data controller, and > the Administrator processes the data only at his instruction, on > the basis of a separate data processing entrustment agreement.

4. **PROTECTION OF CHILDREN (PRIVACY OF MINORS)**

The services provided by the Administrator are not addressed to persons under 18 years of age. We do not knowingly collect Personal Data from minors. If we become aware of the collection of information about a minor, we will immediately take steps to delete it and close the linked Account. If a parent or legal guardian believes that we have collected your child's information, please contact us urgently at privacy@negotivo.com.

5. **DETAILED SCOPE OF DATA COLLECTED**

Depending on your role, we collect the following categories of data:

- 1) Data of Entrepreneurs and their staff:
 - a. information about the company: name, domain, Store ID (from an > external platform), subscription plan, billing data (if > applicable);
 - b. Administrative data: names, business email addresses, and phone > numbers of team members who have access to the App;
 - c. configuration data: rules for automatic dispute resolution, > notification preferences, amount thresholds for settlements;
 - d. Performance data and analytics: aggregated dispute rates, > settlement success rates, response times.
- 2) data of Users other than Entrepreneurs (including Consumers):
 - a. identity information: name, email address, phone number;
 - b. information about the subject of the dispute, e.g.: order IDs, > product descriptions, transaction dates, amounts, limited > information about the payment method (only e.g. the last 4 > digits of the card; we do not store full payment card > details);
 - c. Communication and evidence data: messages, photos, screenshots, > correspondence with the seller, technical documentation > uploaded as part of the dispute. These documents are also > processed using OCR technology (text extraction.
 - d. Account information: data from OAuth authorization systems > (Google, Apple);

- e. device data and technical data: IP addresses, device type, > operating system;
 - f. Dispute history: full records of claims filed, settlement > results, communication with the mediator (curator).
- 3) Data Retrieved from Third-Party Sales Platforms
- a) in the case of integrations (e.g., through OAuth authorization with > Shopify), we gain access (with the Merchant's consent) to: the > customer's contact information associated with the order, > transaction history, fulfillment status, and shipment tracking. > The application only requests the minimum API permissions > (so-called *scopes*) necessary to handle the dispute.

6. PURPOSES AND LEGAL BASES OF PROCESSING

Depending on the role in which you use our App, we process your personal data for different purposes. Below we present the detailed purposes of the processing and the corresponding legal bases:

1. Registration and Maintenance of the User Account

Scope: Registration of the User account requires the provision of the necessary data specified in the registration form. As part of the account data editing, you can provide your further details. In addition, our system used for account management saves your IP number used during registration. The data is processed in order to provide you with the User account service. After deleting the account, the data is archived for the purpose of possible determination, pursuit or defense of claims. Providing this data is a condition for using the Application.

Legal basis: Necessity for the performance of a contract for the provision of services by electronic means (Article 6(1)(b) of the GDPR).

2. Provision of services for Entrepreneurs and integrations

Scope: Handling the Entrepreneur's account, including integration with External Sales Platforms, obtaining data on orders and disputes, configuring dispute resolution rules, handling subscriptions and payments (through the payment systems of the External Sales Platform, e.g. Shopify Billing API), communicating with the Entrepreneur's team and generating reports. After the contract is performed, the data goes to the archive and accounting documentation for the purposes of fulfilling tax obligations.

Legal basis: Necessity for the performance of the contract (Article 6(1)(b) of the GDPR) and the legitimate interest of the Administrator (Article 6(1)(f) of the GDPR).

3. Handling disputes, complaints and chargebacks (for > Buyers/Consumers)

Scope: Receiving and handling disputes (complaints, chargebacks), communication through the Application, collecting evidence (including image processing using OCR technology), analyzing the dispute using artificial intelligence (AI), generating settlement proposals, documenting the outcome of

the dispute. If you file a complaint or withdraw from the contract, you provide the personal data contained in the content of the statements. Providing data is a condition for conducting the complaint process.

Legal basis: Necessity for the performance of the contract (Article 6(1)(b) of the GDPR), fulfilment of a legal obligation in the field of consumer rights (Article 6(1)(c) of the GDPR) and the legitimate interest of the Administrator and the Parties (Article 6(1)(f) of the GDPR).

4. **Certification of Agreements (ChainProof)**

Scope: In order to ensure the non-repudiation and authenticity of the settlements reached or the documents generated, the App uses blockchain technology. The processing is limited to generating and storing cryptographic hashes from documents in the Hyperledger network, without revealing the Users' Personal Data to the outside of the User.

Legal basis: Legitimate interest of the Administrator and the parties to the dispute, consisting in ensuring the indisputability of concluded agreements and security of trading (Article 6(1)(f) of the GDPR).

5. **Contact and handling of correspondence**

Scope: By contacting us via available means of communication (e.g. e-mail, messenger, hotline), you provide your personal data contained in the content of the correspondence. Providing data is a condition for establishing contact. The communication system also stores your IP address. The data is processed for the purpose of communication. After its completion, they go to the archive.

Legal basis: The Controller's legitimate interest in conducting correspondence and handling inquiries (Article 6(1)(f) of the GDPR).

6. **Fulfilment of tax and accounting obligations**

Scope: We fulfil tax and accounting obligations, in particular in the form of issuing an invoice, including it in our accounting documentation and storing settlement documentation. We process, m.in, name and surname, company, business address, tax identification number. Providing this data is necessary to comply with the law.

Legal basis: Necessity to comply with a legal obligation incumbent on the Controller (Article 6(1)(c) of the GDPR in conjunction with the relevant provisions of tax law).

7. **Creating an archive**

Scope: We create digital archives for the needs of our business. The personal data that we have processed in connection with you are sent to the archives, and their scope may vary depending on the type of case (e.g. completed disputes, documentation generated from the system).

Legal basis: Legitimate interest in organizing, organizing and archiving data carriers (Art. 6 para. 1 lit. f GDPR).

8. **Defending, establishing or pursuing claims**

Scope: Your use of the App and entering into contracts with us may give rise to claims on our part or on your part in the future. As such, we are entitled to process any Personal Data that is related to a claim, including activity logs, chat logs, and evidentiary documentation.

Legal basis: Legitimate interest in protecting our interests, asserting rights and defending ourselves in proceedings before courts and authorities (Art. 6 (1) (f) GDPR).

9. **Analysis and statistics**

Scope: We conduct analytical activities using tools from external providers (e.g. Google Analytics). We analyze how Users use the platform, detect UX errors, and examine the effectiveness of AI-generated legal arguments. From the level of tools, we have access to basically only Anonymous Information or highly aggregated statistics.

Legal basis: Legitimate interest in optimizing the Application, improving the quality of services and drawing business conclusions (Article 6(1)(f) of the GDPR).

10. **Own marketing (including Newsletter)**

Scope: We carry out marketing activities consisting in sending commercial information, news about the platform (Newsletter) and possible adjustment of advertising content with the use of appropriate cookies. These actions are always based on your explicit consent.

Legal basis: Voluntary consent of the data subject (Art. 6 (1) (a) GDPR).

11. **Compliance with data protection obligations (GDPR) and security > (DSA)**

Scope: As a controller, we are required to demonstrate compliance with the GDPR (accountability principle), to deal with your privacy requests, and to respond to reports of illegal content in accordance with the Digital Services Act. For this purpose, we process the whistleblower's data and system logs.

Legal basis: Fulfilment of a legal obligation (Article 6(1)(c) of the GDPR) and a legitimate interest in the form of securing evidence of the implementation of requests (Article 6(1)(f) of the GDPR).

12. **Social media profiles**

Scope: The Administrator has profiles on Facebook and LinkedIn. It processes the Personal Data of visitors to these profiles (comments, likes) in order to promote its own brand and communication.

Legal basis: Legitimate interest of the Administrator (Article 6(1)(f) of the GDPR).

7. **ARTIFICIAL INTELLIGENCE (AI) AND AUTOMATED DECISIONS**

The application uses AI systems (m.in. Google Gemini, Bayesian networks, *Negative Exclusion mechanism*) to analyze cases and generate settlement recommendations.

- Sentiment analysis: The system analyzes the tone of speech (e.g., > urgent, frustrated, neutral) to categorize and prioritize reports > (not to discriminate or deny services).
- No exclusive decision-making power of machines (outside of defined > rules): The final decision always belongs to humans. The exception > is *the Auto-Settlement thresholds* (e.g. reimbursement of funds > in disputes below a certain amount), which the Entrepreneur has > configured himself, consciously and in advance – this is the > implementation of the Entrepreneur's will, not an autonomous > decision of the machine.
- Consumer rights: The consumer has the right to challenge the > decision generated by the system and request human intervention.
- Model training: It is strictly prohibited to use your Personal Data > to train public AI models. Test environment models use synthetic > or anonymized data.

8. DATA RECIPIENTS AND INTERNATIONAL TRANSFER

We carefully select the entities with which we cooperate. The recipients of the data may be:

- **Cloud infrastructure provider:** Google Cloud Platform (data > storage, databases - servers in Europe).
- **AI service provider:** Google Vertex AI (as a processor that > analyzes disputes in an isolated environment).
- **Communication providers:** Mailgun (email), SMSAPI (SMS).
- **Third-party platform providers:** Shopify, etc. (in terms of data > exchange via API).
- **Payment providers:** platform billing systems or third-party > payment operators.

Transfers outside the EEA:

The Administrator stores data on GCP servers located in the EU (e.g. Belgium, Frankfurt, the Netherlands). Where providers of analytics or support tools transfer data outside of the European Economic Area (EEA), we rely on adequacy decisions of the European Commission (e.g. *EU-U.S. Data Privacy Framework*) and binding Standard Contractual Clauses (SCCs).

9. RETENTION PERIOD AND DELETION OF DATA

- 1) User data: stored for the duration of the account activity and for > at least 1 year after its closure for legal and billing purposes.
- 2) Dispute history and evidence: Retained for a period of 7 years from > the time the dispute was closed or resolved. This period is > necessary to protect against late chargebacks from payment > institutions and to defend against legal claims. After this time, > the documentation is permanently deleted.

- 3) System logs (automated data): Retained for 90 days and then deleted > or completely aggregated.
- 4) Third-Party Shopping Platform Requirements (e.g., Shopify webhooks): > The administrator fully supports mandatory privacy mechanisms. In > the event of a request from the platform (customers/data_request, > customers/redact, shop/redact), the data is located and deleted > within the required time, unless the overriding law requires a > longer retention for evidentiary purposes.
- 5) Uninstall the App – Uninstalling the App \from an external system > (e.g., Shopify) automatically initiates the process of deleting > data associated with a given Business Owner from our systems, in > addition to the data required by the archiving law.

10. DATA SUBJECT RIGHTS – GDPR (FOR EUROPEAN RESIDENTS)

In accordance with the GDPR (and Polish law), you have the following rights:

- The right to access and receive a copy of the data;
- The right to rectify (correct) inaccurate or incomplete information;
- The right to erasure (right to be forgotten), subject to the > retention requirements of the defence of claims;
- Right to restriction of processing;
- The right to portability data in a commonly used format;
- The right to object to processing based on legitimate interest > (including objecting to certain profiling);
- The right to withdraw your consent, if you have previously given > such consent;
- The right to lodge a complaint with the President of the Office for > Personal Data Protection (PUODO) in Poland or another competent > supervisory authority in your country.

Requests should be sent to the following address: privacy@negotivo.com or office@negotivo.com. The response time is up to 30 calendar days.

11. ADDITIONAL RIGHTS FOR CALIFORNIA (USA) RESIDENTS – CCPA/CPRA

If you are a California resident, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) grant you additional and specific rights regarding your information.

1. Rights under the CCPA and CPRA:
 - Right to Know: You have the right to request information about the > categories of personal information we collect, use, and disclose > about you.
 - Right to Delete: You have the right to request the deletion of your > personal data, subject to legal exceptions (e.g. closing a > transaction, legal disputes).

- Right to Opt-Out: You have the right to prohibit the "sale" or "sharing" of your data. Please note that we do not sell your personal information in the traditional sense of the word. We only share it with our Service Providers. You can opt out of sharing by contacting us.
- Right to rectification: the right to request the rectification of inaccurate data.
- Right to Limit Use: The right to request the restriction of the use of sensitive personal data only for the purposes necessary to provide the services.
- Right to Opt-Out of Automated Decision-Making: the right to opt-out of profiling that produces significant legal effects for you (subject to the necessity of algorithms for the operation of the platform itself in the case of voluntary use of the platform).
- Right to Non-Discrimination: We ensure that we will not discriminate against you (e.g., by denying services, changing prices) for exercising your CCPA/CPRA rights.
- Right to Appeal: If we deny your request, you have the right to appeal the decision.

1. How to File a CCPA:

Please send your requests to the e-mail address: privacy@negotivo.com with a note in the title: *"CCPA Data Request"*. We reserve the right to verify your identity before fulfilling your request.

2. "Shine the Light" Law (California Civil Code Section 1798.83):

California residents have the right to request information about the categories of personal information shared with third parties for their own direct marketing purposes. These requests should be submitted to the above email address with the subject *"California Shine the Light Request"*.

12. COOKIES AND TRACKING TECHNOLOGIES

As part of the Application (both in the mobile application and in the web panel) we use "cookies" (temporary session files and permanent files) and similar tracking technologies (e.g. JWT - JSON Web Tokens, Local Storage) for the following purposes:

1. Essential: enabling login, authenticating the User with secure tokens (e.g. via Firebase Auth), maintaining an active session, securing forms (CSRF protection), and maintaining the state of the conversation and context for the AI module (RAG system). Without these technologies, the App will not function properly.
2. Performance & Analytics: collecting aggregate visitor statistics, tracking navigation paths, identifying device and browser type in order to improve the interface on an ongoing basis and detect UX errors. For this purpose, we use external tools, in particular Google Analytics (provider: Google Ireland Ltd.). The data obtained with the help of these files are generally Anonymous Information, which do not allow for direct identification of a person.

3. Functional and Marketing: remembering the User's individual > preferences (e.g. choice of language, light/dark visual theme). In > addition, only on promotional pages and *landing pages* (other > than the main dispute resolution panel), we may use tools such as > Google Ads and Meta Pixel (provider: Meta Platforms Ireland Ltd.) > to measure the effectiveness of our campaigns and tailor > advertising content.

Location data:

When you use the Mobile Application, we may collect precise location data with your prior and explicit consent at the operating system settings level. They are used only to support certain functionalities of the Application (e.g. embedding evidence widgets or specifying the location of an event as part of an ongoing dispute).

Managing Preferences:

You can manage cookies through the appropriate settings of your web browser (e.g. Chrome, Safari, Firefox, Opera), including enabling the blocking or "opt-out" function. However, it should be remembered that blocking *session* files (necessary) will prevent you from logging in to the panel and using the functionality of the Application. If you install a special "opt-out" file, please note that it only works in the browser in which it was saved.

13. CONTACT FOR PRIVACY

If you have any questions about this Privacy Policy, data access requests and complaints, please contact:

- Email: **privacy@negotivo.com** or **office@negotivo.com**
- correspondence address: NEGOTIVO Prosta Spółka Akcyjna, 1 Ignacego > Mościckiego Street, 24-110 Puławy, Poland.

If the dispute between the User and the Administrator is not resolved, the right to complain to the following authorities:

- in Poland: Office for Personal Data Protection (UODO) - > <https://uodo.gov.pl/>
- in California: California Attorney General, Office of Privacy > Protection - <https://oag.ca.gov/privacy>
- in other EU countries: The competent national data protection > supervisory authority.

14. CHANGES TO THE PRIVACY POLICY

Due to the fact that the Application is currently in the early launch phase (Beta / MVP version) and is subject to intensive development, as well as due to dynamic changes in regulations (e.g. GDPR, AI Act, DSA, regulations in the USA), this Policy may be modified. In the event of significant changes, the Administrator will inform registered Users via e-mail or by means of a clear message inside the

Application panel. Your continued use of the App after receiving notice constitutes your acceptance of the updated policy.