

Umowa powierzenia przetwarzania danych osobowych

Wersja 0.2 z 19 października 2026 · obowiązuje od 19 października 2026

Załącznik nr 1 do Regulaminu usługi Osnovia. Zawierana w formie elektronicznej przy zakładaniu Konta (art. 28 ust. 9 RODO).

Strony:

- Klient** w rozumieniu Regulaminu — jako administrator danych („**Administrator**”),
- APOLLO15 sp. z o.o.** z siedzibą w Gdańsku, ul. Heweliusza 11 lok. 17, 80-890 Gdańsk, KRS 0000604696, NIP 5833196774 — jako podmiot przetwarzający („**Przetwarzający**”).

Pojęcia pisane wielką literą mają znaczenie nadane w Regulaminie albo w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 („**RODO**”).

§1. Przedmiot, charakter, cel i czas przetwarzania

- Administrator powierza Przetwarzającemu przetwarzanie danych osobowych zawartych w Danych Klienta w zakresie niezbędnym do świadczenia Usługi.
- Charakter przetwarzania: przechowywanie, porządkowanie, wyszukiwanie, przeglądanie, pobieranie z Platform Zewnętrznych, przesyłanie do Platform Zewnętrznych na polecenie Administratora, wykonywanie kopii zapasowych, usuwanie.
- Cel: obsługa zamówień Administratora, nadawanie przesyłek, wystawianie dokumentów sprzedaży, obsługa zwrotów i komunikacji z kupującymi, migracja danych, pomoc techniczna.
- Czas: przez okres obowiązywania umowy o świadczenie Usługi oraz okres na eksport i usunięcie danych z § 8.

§2. Rodzaje danych i kategorie osób

Kategoria osób	Rodzaje danych
Kupujący i odbiorcy przesyłek Administratora	imię i nazwisko, nazwa firmy, NIP, adresy dostawy i rozliczeniowy, telefon, e-mail, login w marketplace, treść i historia zamówień, dane przesyłek, status płatności, dane zwrotów i reklamacji, korespondencja

Użytkownicy Konta (pracownicy i współpracownicy Administratora)	dziennik działań w Koncie udostępniany Administratorowi
Osoby kontaktowe kontrahentów Administratora	imię i nazwisko, e-mail, telefon, stanowisko

Przetwarzający nie przetwarza celowo szczególnych kategorii danych (art. 9 RODO). Administrator nie wprowadza takich danych do Usługi.

Dane Użytkowników Konta potrzebne do zawarcia i wykonania umowy o świadczenie Usługi, bezpieczeństwa logowania i komunikacji o Usłudze Przetwarzający przetwarza jako administrator, na zasadach Polityki prywatności, a nie na podstawie niniejszej umowy.

§ 3. Obowiązki Przetwarzającego

1. Przetwarzający przetwarza dane wyłącznie na udokumentowane polecenie Administratora. Poleceniem są Regulamin, niniejsza umowa, konfiguracja Konta i Integracji dokonana przez Administratora oraz zgłoszenia Administratora, także przekazane e-mailem.
2. Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem polecenie narusza RODO lub inne przepisy.
3. Przetwarzający dopuszcza do danych wyłącznie osoby upoważnione, zobowiązane do zachowania tajemnicy.
4. Przetwarzający stosuje środki techniczne i organizacyjne z art. 32 RODO opisane w Załączniku A.
5. Przetwarzający pomaga Administratorowi w odpowiadaniu na żądania osób, których dane dotyczą, w szczególności udostępniając w Usłudze funkcje wyszukania, eksportu, poprawienia i usunięcia danych kupującego.
6. Przetwarzający pomaga Administratorowi w wywiązaniu się z obowiązków z art. 32–36 RODO, uwzględniając charakter przetwarzania i dostępne mu informacje.
7. Przetwarzający nie przetwarza danych w celach własnych, w szczególności marketingowych.

§ 4. Dalsze powierzenie

1. Administrator udziela ogólnej zgody na korzystanie przez Przetwarzającego z dalszych podmiotów przetwarzających. Aktualna lista stanowi Załącznik nr 3 do Regulaminu i jest dostępna na osnovia.com.
2. O zamiarze dodania lub zmiany dalszego podmiotu przetwarzającego Przetwarzający informuje Administratora e-mailem co najmniej 14 dni wcześniej. Administrator może w tym czasie zgłosić sprzeciw; jeśli Strony nie uzgodnią rozwiązania, Administrator może rozwiązać umowę o świadczenie Usługi ze skutkiem natychmiastowym.

3. Przetwarzający nakłada na dalsze podmioty przetwarzające obowiązki ochrony danych nie mniejsze niż w niniejszej umowie i odpowiada za ich działania jak za własne.
4. Platformy Zewnętrzne, z którymi Administrator uruchomił Integrację, nie są dalszymi podmiotami przetwarzającymi Przetwarzającego. Dane trafiają do nich na polecenie Administratora, w ramach jego relacji z tymi podmiotami.

§ 5. Przekazywanie danych poza EOG

1. Dane są przetwarzane w Europejskim Obszarze Gospodarczym.
2. Przekazanie danych do państwa trzeciego następuje wyłącznie, gdy Administrator włączy asystenta AI. Asystent korzysta z modeli Claude dostarczanych przez Anthropic Ireland, Limited. Dane mogą być przetwarzane w Stanach Zjednoczonych przez Anthropic, PBC, na podstawie standardowych klauzul umownych (rozdział V RODO) zawartych w umowie powierzenia Anthropic. Do modelu trafia wyłącznie treść rozmowy z kupującym i dane zamówienia potrzebne do odpowiedzi.
3. Według zasad Anthropic dane przesłane przez API są usuwane w ciągu 30 dni i nie są wykorzystywane do trenowania modeli; dłużej, do 2 lat, Anthropic może przechowywać dane oznaczone jako naruszające jego zasady korzystania.

§ 6. Naruszenia ochrony danych

1. Przetwarzający zawiadamia Administratora o stwierdzonym naruszeniu ochrony danych bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od jego stwierdzenia, na adres e-mail właściciela Konta.
2. Zawiadomienie zawiera informacje z art. 33 ust. 3 RODO dostępne w chwili zawiadomienia. Pozostałe informacje Przetwarzający przekazuje niezwłocznie po ich uzyskaniu.
3. Przetwarzający podejmuje działania ograniczające skutki naruszenia i dokumentuje naruszenie.
4. Przetwarzający utrzymuje procedurę przyjmowania i obsługi naruszeń, która zapewnia dotrzymanie terminu z ust. 1 także poza godzinami pracy.

§ 7. Kontrola

1. Przetwarzający udostępnia Administratorowi informacje niezbędne do wykazania spełnienia obowiązków z art. 28 RODO, w pierwszej kolejności w formie pisemnych odpowiedzi na pytania i dokumentacji, w tym raportów z testów bezpieczeństwa.

2. Administrator może przeprowadzić audyt nie częściej niż raz w roku, chyba że zaszło naruszenie ochrony danych, po zawiadomieniu z co najmniej 14-dniowym wyprzedzeniem, w dni robocze, na własny koszt, samodzielnie lub przez audytora zobowiązanego do poufności. Audyt nie może obejmować danych innych klientów Przetwarzającego ani zagrażać bezpieczeństwu Usługi.

§ 8. Zakończenie przetwarzania

1. Po rozwiązaniu umowy o świadczenie Usługi Administrator może pobrać eksport danych przez 30 dni.
2. Po tym czasie Przetwarzający usuwa dane w ciągu 30 dni, a z kopii zapasowych w cyklu ich nadpisywania, nie dłuższym niż 35 dni, chyba że prawo Unii lub prawo polskie nakazuje ich dalsze przechowywanie.
3. Na żądanie Administratora Przetwarzający potwierdza usunięcie danych e-mailem.

§ 9. Odpowiedzialność i postanowienia końcowe

1. Odpowiedzialność Stron wobec osób, których dane dotyczą, określa art. 82 RODO. W stosunkach między Stronami stosuje się postanowienia Regulaminu o odpowiedzialności w zakresie dopuszczalnym przez prawo.
 2. W sprawach nieuregulowanych stosuje się Regulamin i RODO. W razie sprzeczności z Regulaminem w zakresie ochrony danych pierwszeństwo ma niniejsza umowa.
 3. Umowa obowiązuje przez czas obowiązywania umowy o świadczenie Usługi i do zakończenia czynności z § 8.
-

Załącznik A. Środki techniczne i organizacyjne

1. **Lokalizacja:** serwery w centrum danych Hetzner Online GmbH w Finlandii, w Unii Europejskiej.
2. **Szyfrowanie:** połączenia przez TLS; szyfrowane dyski serwerów; kopie zapasowe szyfrowane kluczem przechowywanym poza serwerem produkcyjnym; dane dostępne do Platform Zewnętrznych szyfrowane w bazie danych.
3. **Izolacja klientów:** rozdzielenie danych klientów wymuszane na poziomie bazy danych (zabezpieczenia na poziomie wierszy), niezależnie od logiki aplikacji.
4. **Dostęp administracyjny:** wyłącznie przez prywatną, szyfrowaną sieć; brak logowania z internetu; brak pracy na koncie root; indywidualne konta administratorów z drugim składnikiem; rejestrowanie każdego dostępu.
5. **Dostęp do danych klientów:** wyłącznie na prośbę klienta, w celu rozwiązania zgłoszenia lub dla bezpieczeństwa; każdy dostęp rejestrowany i widoczny dla klienta.

6. **Uwierzytelnianie użytkowników:** hasła przechowywane jako skrót odporny na łamanie; logowanie dwuskładnikowe; blokada po nieudanych próbach; dziennik logowań.
7. **Kopie zapasowe:** co najmniej raz na 24 godziny, poza serwerem produkcyjnym; próbne odtworzenie co najmniej raz w miesiącu.
8. **Ciągłość działania:** cel odtworzenia po awarii poniżej 8 godzin, utrata danych poniżej 24 godzin.
9. **Monitoring i aktualizacje:** całodobowy automatyczny monitoring z alarmami; krytyczne poprawki bezpieczeństwa wdrażane w ciągu 24 godzin od ich publikacji.
10. **Dziennik zdarzeń:** rejestr zmian zamówień, faktur i ustawień, dostępny dla klienta.
11. **Testy:** audyt bezpieczeństwa przed udostępnieniem Usługi i zewnętrzne testy penetracyjne, następnie co najmniej raz w roku.
12. **Organizacja:** upoważnienia i zobowiązania do poufności osób z dostępem; zasada najmniejszych uprawnień; procedura obsługi naruszeń z terminem z § 6.

Usługodawca: APOLLO15 sp. z o.o., ul. Jana Heweliusza 11 lok. 17, 80-890 Gdańsk, KRS 0000604696, NIP 5833196774. Poprzednie wersje: brak, to pierwsza opublikowana wersja.