

Umowa powierzenia przetwarzania danych osobowych

Załącznik do umowy abonamentowej dotty · art. 28 RODO
dotty sp. z o.o. jako podmiot przetwarzający · wersja v3, 2 września 2026 r.

Strony:
Administrator - Gabinet: [firma, adres, NIP - dane Gabinetu z formularza zamówienia] (klient dotty, administrator danych swoich klientów).
Podmiot przetwarzający - DOTTY spółka z ograniczoną odpowiedzialnością z siedzibą w Brzegu, ul. Księcia Jerzego II Piasta 11 lok. 3, 49-300 Brzeg, KRS 0001262238, NIP 7471938413, REGON 545534722, kapitał zakładowy 6 000,00 zł (dostawca aplikacji dotty).

§1. Przedmiot i cel

Administrator powierza dotty przetwarzanie danych osobowych **klientów Gabinetu** wyłącznie w celu i zakresie niezbędnym do świadczenia usługi aplikacji dotty (SaaS): umawianie wizyt, kalendarz, kartoteka i dokumentacja zabiegowa, diagnostyka, usługi/cennik/koszty, komunikacja z klientem. dotty przetwarza dane **wyłącznie na udokumentowane polecenie Administratora** (poleceniem jest korzystanie z funkcji aplikacji zgodnie z jej przeznaczeniem oraz niniejsza umowa).

§2. Charakter, czas, rodzaj danych i kategorie osób

Kategorie osób	Klienci Gabinetu (osoby korzystające z usług kosmetycznych)
Kategorie danych	Identyfikacyjne i kontaktowe (imię, nazwisko, telefon, e-mail); dane o wizytach/zabiegach; dane dotyczące zdrowia (diagnostyka, przeciwwskazania, alergie) - szczególna kategoria, art. 9 RODO [jeśli Gabinet je wprowadza]
Czas	Czas trwania umowy abonamentowej

Podstawę przetwarzania wobec osób zapewnia Administrator (Gabinet), w tym **wyraźną zgodę na dane o zdrowiu** (art. 9 ust. 2 lit. a) - patrz wzór klauzuli dla klienta Gabinetu.

§3. Obowiązki dotty (podmiotu przetwarzającego) - art. 28 ust. 3

- przetwarza dane wyłącznie na udokumentowane polecenie Administratora, także co do transferów poza EOG;
- zapewnia, że osoby upoważnione zobowiązały się do **poufności**;
- stosuje **środki bezpieczeństwa** wymagane art. 32 RODO (§4);
- korzysta z **podprzetwarzających** tylko na zasadach §5;
- w miarę możliwości **pomaga Administratorowi** realizować prawa osób (art. 12-23) oraz obowiązki z art. 32-36 (bezpieczeństwo, zgłaszanie naruszeń, DPIA);
- po zakończeniu - wedle wyboru Administratora **usuwa lub zwraca** dane i kasuje kopie (chyba że obowiązek dalszego przechowywania wynika z przepisów prawa);
- udostępnia informacje niezbędne do wykazania zgodności i umożliwia **audyty** (w tym inspekcje) - nie częściej niż raz w roku kalendarzowym, po uprzednim zawiadomieniu z 14-dniowym wyprzedzeniem, w godzinach pracy i bez zakłócania świadczenia usług; koszty audytu ponosi Administrator, chyba że audyt wykaże istotne naruszenie po stronie dotty;
- **zgłasza Administratorowi naruszenie** ochrony danych bez zbędnej zwłoki - nie później niż w ciągu 24 godzin od stwierdzenia.

§4. Bezpieczeństwo (art. 32)

dotty stosuje adekwatne środki techniczne i organizacyjne: **szyfrowanie** (transmisji i danych), kontrola i rejestrowanie dostępu, pseudonimizacja gdzie możliwe, kopie zapasowe i zdolność przywrócenia po incydencie, regularne testowanie zabezpieczeń, rozdział ról. Dostęp do danych mają wyłącznie osoby upoważnione, w zakresie niezbędnym do obsługi usługi; hasła i tokeny dostępu przechowywane są w postaci zaszyfrowanej.

§5. Podprzetwarzający (subprocesorzy)

Administrator udziela **ogólnej zgody** na korzystanie z podprzetwarzających niezbędnych do świadczenia usługi (hosting i infrastruktura, poczta i powiadomienia, operator płatności, dostawca usługi diagnostycznej opartej na modelu językowym) - aktualna lista stanowi **Załącznik nr 1** do niniejszej umowy i jest publikowana na dotty.pl. dotty informuje Administratora o zamierzonej zmianie podprzetwarzającego z co najmniej 30-dniowym wyprzedzeniem (e-mailem lub w Aplikacji); Administrator może w tym terminie wnieść

uzasadniony sprzeciw, a w razie braku rozwiązania - wypowiedzieć abonament bez skutków finansowych. dotty nakłada na podprzetwarzających te same obowiązki ochrony danych. dotty odpowiada wobec Administratora za działania podprzetwarzających.

§6. Wykorzystanie modelu językowego (AI) w diagnostyce

Funkcja diagnostyczna Aplikacji korzysta z modelu językowego udostępnianego przez dostawcę zewnętrznego, działającego jako podprzetwarzający. Do dostawcy przekazywane są wyłącznie dane dotyczące stanu skóry, wywiadu kosmetycznego i parametrów zabiegu, **bez danych identyfikujących klientkę**; powiązanie wyniku z konkretną osobą pozostaje wyłącznie w Aplikacji. Zdjęcia przekazywane są bez metadanych (EXIF). Dostawca nie wykorzystuje przekazanych treści do trenowania modeli, a dane wejściowe i wyjściowe usuwa w terminie do 30 dni.

§7. Transfery poza EOG

Dane przetwarzane w EOG. Ewentualny transfer poza EOG wyłącznie na podstawie mechanizmów z rozdz. V RODO (decyzja o adekwatności / standardowe klauzule umowne). Stan faktyczny: dane Aplikacji przechowywane są na serwerach w Niemczech (EOG). Poza EOG przekazywane są wyłącznie dane przetwarzane przez dostawcę modelu językowego, wykorzystywanego do generowania interpretacji diagnostycznej - na podstawie standardowych klauzul umownych (decyzja 2021/914) i wyłącznie w postaci pozbawionej danych identyfikujących klientkę (bez imienia, nazwiska, kontaktu i identyfikatorów umożliwiających powiązanie poza Aplikacją).

§8. Odpowiedzialność, czas, wypowiedzenie

Umowa obowiązuje przez czas trwania abonamentu. Każda ze stron odpowiada zgodnie z RODO i przepisami krajowymi. Rażące naruszenie obowiązków ochrony danych przez dotty uprawnia Administratora do rozwiązania. Po zakończeniu - postępowanie z danymi wg §3.

Załącznik nr 1 - lista podprzetwarzających (stan na 2 września 2026 r.)

Podmiot	Rola	Lokalizacja / podstawa transferu
Hetzner Online GmbH	hosting i infrastruktura Aplikacji	Niemcy (EOG)
Google Ireland Limited	poczta służbowa; synchronizacja kalendarza wizyt (na wyraźne polecenie Gabinetu)	Irlandia (EOG)
Anthropic PBC	model językowy generujący interpretację diagnostyczną (dane bez identyfikatorów - §6)	USA - standardowe klauzule umowne (2021/914)
PayU S.A. (Poznań, KRS 0000274399)	obsługa płatności za Abonament i Pakiety Diagnostyk (dane Gabinetu, nie Klientów Gabinetu; w zakresie transakcji odrębny administrator)	Polska (EOG)
LINK Mobility Poland sp. z o.o. (Gliwice, KRS 0000350201) - usługa SMSAPI	wysyłka przypomnień SMS o wizytach na polecenie Gabinetu (imię, numer telefonu i termin wizyty Klienta Gabinetu)	Polska (EOG)

Zmiany listy następują w trybie §5. Aktualna wersja: dotty.pl oraz na żądanie - rodo@dotty.pl.

Administrator (Gabinet)	dotty sp. z o.o.
-------------------------	------------------

Umowa powierzenia (art. 28 RODO). Gabinet = administrator, dotty = procesor. Akceptacja przy zakupie abonamentu.