# Umowa Powierzenia Przetwarzania Danych Osobowych (DPA)

**Załącznik nr 1 do Regulaminu świadczenia usługi BeautyAssist**

## Preambuła

Niniejsza Umowa Powierzenia Przetwarzania Danych Osobowych („**DPA**" lub „**Umowa**") zawierana jest pomiędzy:

- **Intelibyte sp. z o.o.** z siedzibą w Rybniku przy ul. Jabłoniowej 18, 44-270 Rybnik, woj. śląskie, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0001051332, NIP 6423246740, REGON 526034960, kapitał zakładowy 5 000,00 zł opłacony w całości (dalej: „**Procesor**" lub „**Intelibyte**") świadczącym usługę BeautyAssist;

a

- **Klientem** (dalej: „**Administrator**") — przedsiębiorcą wskazanym w procesie rejestracji Konta w usłudze BeautyAssist, który zaakceptował Regulamin i tym samym zawarł niniejszą Umowę.

DPA stanowi integralną część **Regulaminu świadczenia usługi BeautyAssist** i zostaje zawarta w chwili akceptacji Regulaminu przez Administratora.

Pojęcia użyte w DPA pisane wielką literą mają znaczenie nadane im w Regulaminie. Pojęcia zdefiniowane w RODO mają znaczenie nadane im w tym Rozporządzeniu.

**Mając na uwadze, że:**

1. Administrator korzysta z usługi BeautyAssist w celu wsparcia prowadzenia działalności gospodarczej w obszarze usług kosmetycznych (Salon beauty, klinika, gabinet);
2. W ramach korzystania z BeautyAssist Administrator wprowadza, przechowuje i przetwarza dane osobowe Klientów Końcowych (osób korzystających z usług kosmetycznych Administratora) oraz dane pracowników Administratora przypisanych do Stanowisk;
3. Administrator jest administratorem tych danych osobowych w rozumieniu art. 4 pkt 7 RODO, a Procesor — podmiotem przetwarzającym w rozumieniu art. 4 pkt 8 RODO;
4. Strony pragną określić warunki i zasady powierzenia przetwarzania danych osobowych zgodnie z art. 28 RODO,

**postanawia się, co następuje:**

---

## § 1. Przedmiot, charakter i czas trwania przetwarzania

1. Administrator powierza Procesorowi, a Procesor przyjmuje do przetwarzania dane osobowe w zakresie i celu określonym w niniejszej Umowie oraz w **Załączniku nr 1** (Specyfikacja

przetwarzania).

2. **Cel przetwarzania:** świadczenie przez Procesora na rzecz Administratora usługi BeautyAssist zgodnie z Regulaminem — w tym hosting kartoteki Klientów Końcowych, generowanie i archiwizacja cyfrowych ankiet i zgód, działanie modułu analizy składników INCI, działanie asystenta informacyjnego AI, generowanie eksportów i dokumentów RODO, obsługa powiadomień email i in-app, kopie zapasowe.
3. **Charakter przetwarzania:** zautomatyzowane przetwarzanie danych osobowych w infrastrukturze chmurowej Procesora i jego podprocesorów, w tym przechowywanie, organizowanie, indeksowanie, wyszukiwanie, modyfikowanie, eksportowanie i udostępnianie uprawnionym użytkownikom Administratora.
4. **Czas trwania:** Umowa obowiązuje przez okres trwania głównej umowy o korzystanie z usługi BeautyAssist zawartej na podstawie Regulaminu, z zastrzeżeniem postanowień § 11 (Zwrot lub usunięcie danych po zakończeniu).
5. **Procesor nie określa celów ani sposobów przetwarzania danych osobowych** wprowadzanych przez Administratora do BeautyAssist — pełni wyłącznie funkcję techniczną wykonawcy poleceń Administratora.

---

## § 2. Oświadczenia Administratora

1. Administrator oświadcza, że: - jest administratorem danych osobowych przetwarzanych w BeautyAssist i posiada zgodne z prawem podstawy przetwarzania tych danych (w tym przetwarzania danych szczególnych kategorii, jeżeli takie wprowadza do Usługi — np. danych dotyczących zdrowia Klientów Końcowych w ankietach przedzabiegowych); - posiada wymagane RODO zgody lub inne podstawy prawne do powierzenia danych osobowych Procesorowi; - jest uprawniony do zawarcia niniejszej Umowy oraz reprezentuje organizację Administratora.
2. Administrator zobowiązuje się: - korzystać z BeautyAssist zgodnie z Regulaminem i przepisami o ochronie danych osobowych; - skonfigurować dostęp do Konta i poszczególnych Stanowisk w sposób minimalizujący ryzyko nieuprawnionego dostępu (silne hasła, MFA, nieudostępnianie loginów); - niezwłocznie aktualizować dane kontaktowe Administratora w panelu Konta; - poinformować Procesora bez zbędnej zwłoki o każdej kontroli, postępowaniu lub korespondencji Prezesa Urzędu Ochrony Danych Osobowych (Prezesa UODO) lub innego organu nadzorczego dotyczącej powierzonych danych osobowych, w zakresie, w jakim Procesor jest zobowiązany do współpracy lub udzielenia informacji.

---

## § 3. Polecenia Administratora

1. Procesor przetwarza dane osobowe wyłącznie na **udokumentowane polecenie Administratora**, chyba że obowiązek przetwarzania nakłada na Procesora prawo Unii Europejskiej lub prawo państwa członkowskiego — w takim przypadku Procesor poinformuje o tym Administratora przed

rozpoczęciem przetwarzania, chyba że prawo zakazuje takiego poinformowania ze względu na ważny interes publiczny.

2. Za udokumentowane polecenia Administratora uznaje się: - postanowienia niniejszej DPA i Regulaminu, - czynności konfiguracyjne i operacje wykonywane przez Administratora w panelu BeautyAssist (np. dodanie Klienta Końcowego, wysłanie ankiety, eksport, usunięcie rekordu), - dodatkowe polecenia wysłane przez Administratora w formie elektronicznej na adres **hello@beautyassist.pl** z adresu kontaktowego Konta.
3. Jeżeli Procesor uzna, że polecenie Administratora narusza RODO lub inne przepisy o ochronie danych osobowych, Procesor niezwłocznie poinformuje o tym Administratora i ma prawo wstrzymać wykonanie polecenia do czasu jego potwierdzenia, zmiany lub wycofania.

---

## § 4. Obowiązki Procesora

Procesor zobowiązuje się:

1. **Przetwarzać dane osobowe wyłącznie w celu i zakresie określonym w § 1 i Załączniku nr 1** oraz na podstawie udokumentowanych poleceń Administratora.
2. **Zapewnić, że osoby upoważnione przez Procesora** do przetwarzania danych osobowych zobowiązały się do zachowania ich w tajemnicy lub podlegają ustawowemu obowiązkowi zachowania tajemnicy. Procesor utrzymuje rejestr osób upoważnionych.
3. **Wdrożyć i utrzymywać środki techniczne i organizacyjne** (TOM) odpowiadające ryzyku, opisane w **Załączniku nr 3**, zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą, zgodnie z art. 32 RODO.
4. **Pomagać Administratorowi** poprzez odpowiednie środki techniczne i organizacyjne w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO (bezpieczeństwo, notyfikacja naruszeń, ocena skutków DPIA, konsultacje z organem nadzorczym), w zakresie, w jakim Procesor dysponuje informacjami niezbędnymi do tej pomocy.
5. **Pomagać Administratorowi** w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą (art. 12-22 RODO — prawo dostępu, sprostowania, usunięcia, ograniczenia, przenoszenia, sprzeciwu) — poprzez udostępnienie odpowiednich funkcji w panelu BeautyAssist (eksport danych, usuwanie rekordów Klientów Końcowych, anonimizacja) oraz, na wniosek Administratora, dodatkową pomoc techniczną realizowaną w terminie odpowiadającym charakterowi żądania.
6. **Po zakończeniu świadczenia usługi** dokonać zwrotu lub usunięcia danych osobowych zgodnie z § 11.
7. **Udostępnić Administratorowi** wszelkie informacje niezbędne do wykazania spełnienia obowiązków wynikających z art. 28 RODO oraz umożliwić Administratorowi (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów na zasadach określonych w § 10.

---

## § 5. Poufność

1. Procesor zobowiązuje się do zachowania w tajemnicy danych osobowych powierzonych mu przez Administratora oraz wszelkich informacji o sposobie ich zabezpieczania, zarówno w trakcie obowiązywania Umowy, jak i po jej zakończeniu — bezterminowo.
2. Obowiązek zachowania tajemnicy nie ma zastosowania w przypadku obowiązku ujawnienia informacji wynikającego z bezwzględnie obowiązujących przepisów prawa; w takiej sytuacji Procesor poinformuje Administratora przed ujawnieniem (chyba że prawo to zakazuje).

---

## § 6. Środki techniczne i organizacyjne (TOM)

1. Procesor stosuje środki techniczne i organizacyjne opisane szczegółowo w **Załączniku nr 3** do Umowy, obejmujące m.in.: - **Szyfrowanie w spoczynku** — wszystkie dane osobowe przechowywane w bazie Firestore i Cloud Storage są szyfrowane przy użyciu kluczy zarządzanych Cloud KMS (CMEK) Procesora. - **Szyfrowanie w transmisji** — komunikacja między urządzeniem Administratora a infrastrukturą Procesora odbywa się wyłącznie po protokole TLS 1.3. - **Kontrolę dostępu** — uwierzytelnianie wieloskładnikowe (MFA) dla pracowników Procesora; autoryzacja oparta o ścisły model uprawnień IAM; logowanie i audyt każdego dostępu do danych. - **Segmentację sieciową** — odseparowane środowiska produkcyjne, testowe i developerskie; zasoby chmurowe w prywatnych VPC. - **Kopie zapasowe** — codzienne snapshoty bazy danych z deklarowanym czasem odtworzenia (RTO) ≤ 4 godziny i maksymalną utratą danych (RPO) ≤ 1 godzina. - **Monitorowanie i wykrywanie incydentów** — logi bezpieczeństwa, alerty, monitoring podatności (SBOM, skanowanie zależności). - **Zarządzanie podatnościami** — regularne aktualizacje, testowanie penetracyjne, polityka patch managementu. - **Polityki organizacyjne** — polityka bezpieczeństwa informacji, polityka czystego biurka, regulamin pracy zdalnej, szkolenia okresowe pracowników.
2. Procesor ma prawo aktualizować TOM przy zachowaniu poziomu zabezpieczeń nie gorszego niż dotychczasowy. Istotne zmiany TOM Procesor publikuje w panelu Administratora.

---

## § 7. Podprzetwarzający (Subprocessors)

1. Administrator wyraża **ogólną zgodę** na korzystanie przez Procesora z podprzetwarzających (subprocessors) w zakresie niezbędnym do świadczenia usługi BeautyAssist.
2. Aktualna lista podprzetwarzających jest dostępna w **Załączniku nr 2** do Umowy oraz w panelu Administratora.
3. Procesor zapewnia, że każdy podprzetwarzający został zobowiązany umownie do przestrzegania wymogów ochrony danych nie niższych niż określone w niniejszej Umowie (w tym podpisał z Procesorem umowę powierzenia spełniającą art. 28 ust. 3 RODO).
4. Procesor zobowiązuje się informować Administratora o **planowanych zmianach** dotyczących dodania lub zastąpienia podprzetwarzających z **wyprzedzeniem co najmniej 30 dni**, publikując

informację w panelu Administratora oraz wysyłając powiadomienie email na adres kontaktowy Konta.

5. Administrator ma prawo wyrazić **uzasadniony sprzeciw** wobec planowanej zmiany podprzetwarzającego w terminie 14 dni od powiadomienia. W przypadku sprzeciwu strony podejmą rozmowy w celu znalezienia rozwiązania. Jeżeli rozwiązanie nie będzie możliwe, Administrator ma prawo wypowiedzieć główną umowę o korzystanie z BeautyAssist zgodnie z postanowieniami Regulaminu.
6. Procesor pozostaje **w pełni odpowiedzialny** wobec Administratora za działania i zaniechania każdego podprzetwarzającego, jak za swoje własne.

---

## § 8. Transfer danych poza Europejski Obszar Gospodarczy (EOG)

1. Dane osobowe powierzone Procesorowi są przetwarzane w infrastrukturze zlokalizowanej **w granicach Europejskiego Obszaru Gospodarczego** (region GCP Frankfurt, Niemcy).
2. **Procesor nie przekazuje danych osobowych poza EOG** w ramach świadczenia podstawowej usługi BeautyAssist.
3. W przypadku, w którym konieczne stanie się przetwarzanie danych osobowych poza EOG (np. wsparcie techniczne podprocesora z poza UE, awaria infrastruktury regionalnej), Procesor zapewni odpowiednie zabezpieczenia transferu zgodnie z art. 46 RODO — w szczególności poprzez **Standardowe Klauzule Umowne** (SCC) zatwierdzone decyzją Komisji Europejskiej (Decyzja 2021/914) oraz, w razie potrzeby, dodatkowe środki bezpieczeństwa (Transfer Impact Assessment, dodatkowe szyfrowanie, ograniczenie zakresu danych).
4. Administrator zostanie poinformowany o każdym takim transferze przed jego rozpoczęciem.

---

## § 9. Naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia **naruszenia ochrony danych osobowych** w rozumieniu art. 4 pkt 12 RODO, Procesor zobowiązuje się powiadomić Administratora **bez zbędnej zwłoki, nie później niż w terminie 48 godzin** od stwierdzenia naruszenia, drogą elektroniczną na adres kontaktowy przypisany do Konta Administratora.
2. Powiadomienie zawiera co najmniej: - opis charakteru naruszenia, w tym, jeżeli jest to możliwe, kategorie i przybliżoną liczbę osób oraz wpisów, których dane dotyczą, - imię i nazwisko oraz dane kontaktowe osoby kontaktowej w sprawie naruszenia (IOD lub osoby pełniącej tę funkcję), - opis możliwych konsekwencji naruszenia, - opis środków zastosowanych lub proponowanych przez Procesora w celu zaradzenia naruszeniu, w tym, w stosownych przypadkach, środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Wzór formularza powiadomienia stanowi **Załącznik nr 4** do Umowy.
4. Procesor zachowuje dokumentację każdego naruszenia obejmującą okoliczności, skutki i podjęte działania zaradcze, oraz udostępnia ją Administratorowi na żądanie.

5. Zgłoszenie naruszenia organowi nadzorczemu (Prezesowi UODO) oraz zawiadomienie osób, których dane dotyczą — w zakresie wymaganym art. 33 i 34 RODO — leży po stronie Administratora jako administratora danych. Procesor pomaga Administratorowi w wywiązaniu się z tych obowiązków poprzez udzielenie wszelkich niezbędnych informacji.

---

## § 10. Audyt

1. Administrator ma prawo do przeprowadzenia audytu sposobu przetwarzania danych osobowych przez Procesora, w zakresie zgodności z postanowieniami Umowy i RODO.
2. Audyt realizowany jest na następujących zasadach: - **Pisemne zawiadomienie** z wyprzedzeniem co najmniej **30 dni** roboczych. - Audyt prowadzony przez Administratora **osobiście** lub przez **niezależnego audytora** związanego umową o zachowaniu poufności i niebędącego konkurentem Procesora. - Audyt nie może powodować nieproporcjonalnego zakłócenia działalności operacyjnej Procesora; szczegółowy zakres, czas i metodologia są uzgadniane przez Strony przed audytem. - **Częstotliwość:** nie częściej niż raz na 12 miesięcy, chyba że wystąpią uzasadnione okoliczności (np. zgłoszone naruszenie, wniosek organu nadzorczego). - **Koszty:** każda Strona ponosi swoje koszty. W przypadku, gdy audyt wykaże poważne naruszenia po stronie Procesora, koszty Administratora pokrywa Procesor.
3. W zastępstwie audytu osobistego Administrator może akceptować jako wystarczający dowód zgodności: - aktualne certyfikaty zgodności Procesora i jego podprocesorów (np. ISO 27001, SOC 2 Type II — w zakresie dostępnym), - raporty audytów zewnętrznych przeprowadzonych przez akredytowane podmioty, - wypełnione kwestionariusze bezpieczeństwa udostępniane przez Procesora na żądanie.

---

## § 11. Zwrot lub usunięcie danych po zakończeniu

1. Po rozwiązaniu lub wygaśnięciu głównej umowy o korzystanie z usługi BeautyAssist Procesor: - przez okres **90 dni** od dnia zakończenia umowy zachowuje dane osobowe w trybie „archiwalnym" (Konto zablokowane, dostęp tylko po ponownym zalogowaniu Administratora w celu pobrania eksportu); - udostępnia Administratorowi możliwość pobrania pełnego eksportu danych (PDF, Excel) z poziomu panelu; - po upływie 90 dni dokonuje **nieodwracalnego usunięcia** danych osobowych z aktywnych systemów (w tym kopii zapasowych — zgodnie z polityką rotacji kopii) i przesyła Administratorowi potwierdzenie usunięcia na żądanie.
2. Administrator może w dowolnym momencie przed upływem 90-dniowego okresu archiwalnego zażądać natychmiastowego usunięcia powierzonych danych — Procesor wykona to żądanie w terminie do **7 dni** od jego otrzymania.
3. Zachowanie danych po zakończeniu Umowy w zakresie wymaganym **bezwzględnie obowiązującymi przepisami prawa** (np. dokumenty księgowe, faktury — Ordynacja podatkowa, 5 lat) odbywa się na podstawie odrębnych obowiązków prawnych, niezależnie od niniejszej Umowy. Procesor stosuje wówczas zasadę minimalizacji danych.

## § 12. Odpowiedzialność

1. Każda ze Stron ponosi odpowiedzialność za niewykonanie lub nienależyte wykonanie niniejszej Umowy na zasadach ogólnych Kodeksu cywilnego, z uwzględnieniem przepisów RODO i bezwzględnie obowiązujących przepisów prawa.
2. **Odpowiedzialność Procesora** wobec Administratora z tytułu niniejszej Umowy podlega ograniczeniu odpowiedzialności określonemu w głównej umowie o korzystanie z BeautyAssist (Regulamin § 13), z zastrzeżeniem przypadków, w których ograniczenie odpowiedzialności jest niedopuszczalne na mocy bezwzględnie obowiązujących przepisów (w tym przepisów RODO o odpowiedzialności podmiotu przetwarzającego).
3. Strony ponoszą wobec osób, których dane dotyczą, odpowiedzialność określoną w art. 82 RODO. Wewnętrzne rozliczenie odpowiedzialności między Stronami następuje zgodnie z zasadami winy określonymi w art. 82 ust. 5 RODO.

## § 13. Postanowienia końcowe

1. Niniejsza Umowa wchodzi w życie z chwilą akceptacji Regulaminu przez Administratora.
2. Zmiany Umowy mogą być wprowadzane przez Procesora w trybie analogicznym do zmian Regulaminu (powiadomienie 14-dniowe, prawo Administratora do wypowiedzenia w przypadku braku akceptacji).
3. W sprawach nieuregulowanych w niniejszej Umowie mają zastosowanie postanowienia Regulaminu, RODO oraz powszechnie obowiązujące przepisy prawa polskiego.
4. Prawem właściwym dla Umowy jest prawo polskie. Spory wynikające z Umowy podlegają jurysdykcji sądu powszechnego właściwego miejscowo dla siedziby Procesora (Rybnik).
5. Jeżeli którekolwiek z postanowień Umowy okaże się nieważne lub niewykonalne, pozostałe postanowienia zachowują moc, a Strony zobowiązują się zastąpić nieważne postanowienie postanowieniem najbardziej zbliżonym do celu nieważnego.

# ZAŁĄCZNIKI

## Załącznik nr 1 — Specyfikacja przetwarzania

### A. Przedmiot przetwarzania

Przetwarzanie danych osobowych Klientów Końcowych Administratora (osób fizycznych korzystających z usług kosmetycznych Salonu Administratora) oraz pracowników Administratora (użytkowników

Stanowisk) w celu świadczenia przez Procesora usługi BeautyAssist zgodnie z Regulaminem.

### B. Charakter i cel przetwarzania

| Cel | Charakter |
|---|---|
| Prowadzenie kartoteki Klientów Końcowych | Zbieranie, przechowywanie, organizowanie, modyfikowanie, wyszukiwanie, eksportowanie |
| Zbieranie ankiet zdrowotnych i zgód cyfrowych | Zbieranie, przechowywanie, generowanie dokumentów PDF, podpis elektroniczny |
| Analiza składników INCI produktów stosowanych przez Administratora | Przetwarzanie informacji o składnikach (nie danych osobowych), z podświetlaniem podobieństw do deklarowanych alergii Klientów Końcowych |
| Asystent informacyjny AI (chat dla kosmetologa) | Generowanie odpowiedzi językowych w oparciu o pytania użytkownika; dane Klientów Końcowych mogą być przetwarzane w kontekście pytań |
| Powiadomienia (email, push) o stanie konta, ankietach, wizytach | Wysyłka komunikacji elektronicznej do pracowników Administratora i Klientów Końcowych |
| Archiwizacja i kopie zapasowe | Automatyczne kopie zapasowe, retencja zgodnie z § 11 |

### C. Czas trwania przetwarzania

Przez okres obowiązywania głównej umowy o korzystanie z BeautyAssist + 90 dni okresu archiwalnego po jej zakończeniu (zob. § 11), z wyjątkiem danych zachowywanych na podstawie obowiązków ustawowych (np. dokumenty księgowe).

### D. Rodzaje danych osobowych

**Kategorie podstawowe (wprowadzane obligatoryjnie):** - Imię i nazwisko Klienta Końcowego - Dane kontaktowe Klienta Końcowego (numer telefonu, adres email) - Imię i nazwisko, adres email pracowników Administratora (użytkowników Stanowisk)

**Kategorie opcjonalne (wprowadzane przez Administratora w razie potrzeby):** - Data urodzenia / wiek Klienta Końcowego - Notatki kosmetologa dotyczące Klienta Końcowego - Zdjęcia z zabiegów (twarz, fragment ciała poddany zabiegowi) - Historia wizyt i zabiegów

**Dane szczególnych kategorii (art. 9 RODO) — przetwarzane na podstawie zgody Klienta Końcowego zebranej przez Administratora:** - Dane dotyczące zdrowia (deklaracje z ankiety zdrowotnej: alergie, choroby, ciąża, przyjmowane leki, przeciwwskazania zabiegowe) - Dane biometryczne (zdjęcia twarzy / części ciała poddanych zabiegowi) — o ile zdjęcia umożliwiają jednoznaczną identyfikację

### E. Kategorie osób, których dane dotyczą

- **Klienci Końcowi** — osoby fizyczne korzystające z usług kosmetycznych Administratora

- **Pracownicy Administratora** — osoby fizyczne przypisane do Stanowisk Konta Administratora (kosmetolożki, recepcjonistki, kierownicy salonu)
- **Osoba kontaktowa Administratora** — osoba fizyczna reprezentująca Administratora w procesie rejestracji i komunikacji z Procesorem (jej dane przetwarzane są przez Procesora w roli administratora, na podstawie Polityki Prywatności, nie w ramach niniejszej DPA)

---

## Załącznik nr 2 — Lista podprzetwarzających (Subprocessors)

Stan na: 2026-05-26.

| # | Podprzetwarzający | Zakres danych | Lokalizacja przetwarzania | Podstawa DPA |
|---|---|---|---|---|
| 1 | **Google Cloud Platform (Google Ireland Ltd.)** | Wszystkie powierzone dane osobowe (Firestore, Cloud Storage, Cloud Run, Cloud KMS) | Region GCP `europe-west3` (Frankfurt, Niemcy, EOG) | Standardowe Klauzule Umowne Google Cloud Data Processing Addendum |
| 2 | **Google Vertex AI** (część GCP) | Pseudonimizowane dane wejściowe do modeli AI (treść pytań do asystenta, fragmenty kartoteki w kontekście zapytania) | Region GCP `europe-west3` (Frankfurt) | Pokryte umową DPA Google Cloud Platform |
| 3 | **Firebase (część GCP)** | Identyfikatory użytkowników, tokeny uwierzytelniające, tokeny FCM dla powiadomień push | Region GCP `europe-west3` (Frankfurt) | Pokryte umową DPA Google Cloud Platform |
| 4 | **Stripe Payments Europe Ltd.** | Dane rozliczeniowe Administratora (nazwa firmy, NIP, email, identyfikatory subskrypcji); nie obejmuje danych Klientów Końcowych | Irlandia (EOG) + USA (SCC) | Stripe Data Processing Agreement |
| 5 | **Resend (Resend Inc.)** | Adresy email odbiorców powiadomień (Administratorzy, Klienci Końcowi w wysyłce ankiet), treść wiadomości email | USA + EOG; transfer poza EOG zabezpieczony SCC | Resend Data Processing Agreement |

**Procesor aktualizuje listę podprzetwarzających w panelu Administratora oraz powiadamia o zmianach zgodnie z § 7 DPA.**

---

# Załącznik nr 3 — Środki techniczne i organizacyjne (TOM)

Stan na: 2026-05-26. Lista nie jest wyczerpująca — pełen opis polityki bezpieczeństwa udostępniany na żądanie zgodnie z § 10.

## A. Środki techniczne

| Obszar | Zastosowane środki |
|---|---|
| Szyfrowanie w spoczynku | Cloud KMS z kluczami zarządzanymi przez Klienta (CMEK); szyfrowanie AES-256 |
| Szyfrowanie w transmisji | TLS 1.3 dla całej komunikacji; HSTS preload; certyfikaty wydawane przez akredytowane CA |
| Kontrola dostępu | Firebase Authentication z obowiązkiem MFA dla pracowników Procesora; uwierzytelnianie JWT dla użytkowników; model uprawnień RBAC |
| Segmentacja sieciowa | Prywatne VPC; segregacja środowisk produkcyjnego, testowego, developerskiego; private endpoints dla Firestore i Cloud Storage |
| Kopie zapasowe i odtworzenie | Codzienne snapshoty bazy; RTO ≤ 4 godziny; RPO ≤ 1 godzina; geo-redundantne przechowywanie kopii |
| Anonimizacja i pseudonimizacja | Pseudonimizacja danych w pipeline'ach analitycznych; anonimizacja IP w analityce strony |
| Monitorowanie i wykrywanie incydentów | Logi bezpieczeństwa Cloud Audit Logs; alerty na anomalne wzorce dostępu; integracja z systemem zgłoszeń |
| Zarządzanie podatnościami | Automatyczne skanowanie zależności (SCA); rejestr komponentów oprogramowania (SBOM); polityka patch management |
| Ochrona aplikacyjna | Walidacja danych wejściowych; ochrona przed XSS, CSRF, SQL injection; rate limiting endpointów publicznych |
| Bezpieczeństwo poczty | SPF, DKIM, DMARC skonfigurowane dla domeny beautyassist.pl |

### B. Środki organizacyjne

| Obszar | Zastosowane środki |
|---|---|
| Polityki | Polityka Bezpieczeństwa Informacji; Polityka Zarządzania Dostępem; Polityka Czystego Biurka; Procedura Obsługi Incydentów |
| Szkolenia | Obowiązkowe coroczne szkolenia RODO i cyberbezpieczeństwa dla wszystkich pracowników; szkolenie przed dopuszczeniem do danych |
| Klauzule poufności | Każdy pracownik Procesora podpisuje klauzulę poufności obejmującą okres zatrudnienia i okres po jego zakończeniu |
| Audyty | Wewnętrzne przeglądy bezpieczeństwa co 6 miesięcy; gotowość do audytu zewnętrznego na żądanie Administratora |
| Zarządzanie dostawcami | Procedura weryfikacji DPA przed integracją nowego podprzetwarzającego (zob. `docs/compliance/dpa-checklist.md` ) |
| Zarządzanie incydentami | Procedura `incident-response-plan.md` ; dyżury inżynierów dla incydentów krytycznych |
| Plan ciągłości działania | Procedura `disaster-recovery.md` ; coroczne ćwiczenia odtworzeniowe |
| Inspektor Ochrony Danych | Wyznaczona osoba odpowiedzialna za nadzór nad RODO (kontakt: hello@beautyassist.pl z dopiskiem „IOD") |

---

## Załącznik nr 4 — Wzór powiadomienia o naruszeniu

Procesor zgłasza naruszenie ochrony danych osobowych Administratorowi drogą elektroniczną zgodnie z § 9 DPA. Powiadomienie zawiera co najmniej:

```
TEMAT: [BeautyAssist] Powiadomienie o naruszeniu ochrony danych osobowych — [Identyfikator zgłosz

1. Identyfikator zgłoszenia:           [INC-RRRR-MM-DD-NNNN]
2. Data i godzina stwierdzenia:        [data + godzina, strefa CET]
3. Data i godzina wystąpienia:         [jeżeli znane]
4. Charakter naruszenia:               [opis: poufność / integralność / dostępność]
5. Kategorie danych objęte naruszeniem: [imię/nazwisko, kontakt, ankieta, dane zdrowotne…]
6. Przybliżona liczba osób:            [N]
7. Przybliżona liczba rekordów:        [N]
8. Możliwe konsekwencje:               [opis ryzyka dla osób, których dane dotyczą]
9. Środki podjęte przez Procesora:     [działania zaradcze, izolacja, powiadomienia]
10. Środki proponowane:                [następne kroki, w tym wsparcie Administratora]
11. Osoba kontaktowa:                  [imię, nazwisko, stanowisko, email, telefon]
12. Załączniki:                        [logi, raporty, jeżeli dostępne]
```

Administrator po otrzymaniu powiadomienia jest odpowiedzialny za ewentualne zgłoszenie naruszenia Prezesowi UODO (w terminie 72 godzin od stwierdzenia) oraz zawiadomienie osób, których dane dotyczą, jeżeli wymaga tego art. 33-34 RODO.