UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Załącznik nr 1 do Regulaminu świadczenia usług SilkCRM („DPA”)

Niniejsza umowa powierzenia przetwarzania danych osobowych (dalej: „Umowa” lub „DPA”) stanowi integralną część Regulaminu świadczenia usług SilkCRM (dalej: „Umowa Główna”) i jest zawierana pomiędzy:

1) Usługobiorcą — podmiotem, który zaakceptował Regulamin i korzysta z Aplikacji SilkCRM — zwanym dalej „Administratorem”, a

2) SZEFFER.EXPERT Maciej Szeffer, Os. Dębowe 49B, 30-698 Lusina, NIP: PL6112368636, REGON: 161507926, e-mail: privacy@silkcrm.net — zwanym dalej „Podmiotem przetwarzającym”.

Umowa zostaje zawarta w formie elektronicznej z chwilą akceptacji Regulaminu, co spełnia wymóg formy określony w art. 28 ust. 9 RODO.

§ 1. Definicje

1. RODO — rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Aplikacja — oprogramowanie SilkCRM udostępniane w modelu SaaS na podstawie Umowy Głównej i Regulaminu świadczenia usług SilkCRM z dn. 1.06.2025.
3. Dane Powierzone — dane osobowe, których administratorem jest Administrator, przetwarzane przez Podmiot przetwarzający w jego imieniu w ramach Aplikacji, opisane w Załączniku A.
4. Podprocesor — inny podmiot przetwarzający, któremu Podmiot przetwarzający podpowierza przetwarzanie Danych Powierzonych.
5. EOG — Europejski Obszar Gospodarczy.
6. Recepcja SilkAI — moduł Aplikacji uruchamiany przez Administratora, w ramach którego asystent głosowy oparty na sztucznej inteligencji odbiera połączenia telefoniczne kierowane do Administratora, udziela informacji o jego ofercie oraz umawia, przekłada i odwołuje wizyty w kalendarzu Aplikacji.

§ 2. Przedmiot Umowy

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie Danych Powierzonych w trybie art. 28 RODO, w zakresie i na zasadach określonych w niniejszej Umowie.
2. Podmiot przetwarzający przetwarza Dane Powierzone wyłącznie w celu świadczenia usług określonych w Umowie Głównej.
3. W odniesieniu do danych osobowych Administratora, jego pracowników i współpracowników przetwarzanych w celu zawarcia i wykonania Umowy Głównej (dane konta, rozliczenia, logowanie) Podmiot przetwarzający działa jako samodzielny administrator — zasady tego przetwarzania określa Polityka Prywatności SilkCRM; przetwarzanie to nie jest objęte niniejszą Umową.

§ 3. Czas trwania

1. Umowa obowiązuje przez czas obowiązywania Umowy Głównej.
2. Rozwiązanie lub wygaśnięcie Umowy Głównej skutkuje rozwiązaniem niniejszej Umowy, z zastrzeżeniem obowiązków określonych w § 12.

§ 4. Charakter i cel przetwarzania, rodzaje danych i kategorie osób

1. Charakter i cel przetwarzania, rodzaje Danych Powierzonych oraz kategorie osób, których dane dotyczą, określa Załącznik A do Umowy.

2. Administrator zapewnia, że posiada odpowiednią podstawę prawną do przetwarzania Danych Powierzonych oraz do ich powierzenia Podmiotowi przetwarzającemu, w tym — w przypadku danych szczególnych kategorii (np. dane o zdrowiu: alergie, przeciwwskazania) — podstawę z art. 9 ust. 2 RODO.

3. Administrator odpowiada za zgodność z prawem treści Danych Powierzonych oraz treści komunikacji inicjowanej przez Administratora, w szczególności za istnienie odpowiednich podstaw prawnych ich przetwarzania i wysyłki. Postanowienie to nie ogranicza obowiązków i odpowiedzialności Podmiotu przetwarzającego wynikających z RODO i niniejszej Umowy.

4. Aplikacja nie jest przeznaczona do prowadzenia dokumentacji medycznej w rozumieniu przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a powierzenie nie obejmuje takiej dokumentacji. Administrator nie prowadzi w Aplikacji dokumentacji medycznej; pola dotyczące zdrowia służą wyłącznie odnotowaniu informacji niezbędnych do bezpiecznego wykonania usługi.

§ 5. Obowiązki i uprawnienia Administratora

1. Administrator wydaje Podmiotowi przetwarzającemu udokumentowane polecenia dotyczące przetwarzania; za udokumentowane polecenie uznaje się w szczególności postanowienia Umowy Głównej i niniejszej Umowy oraz działania Administratora i jego użytkowników wykonywane w Aplikacji (konfiguracja, uruchamianie kampanii, wysyłka wiadomości, uruchomienie i konfiguracja Recepcji SilkAI).

2. Administrator odpowiada za realizację obowiązku informacyjnego (art. 13–14 RODO) wobec swoich klientów oraz za obsługę ich zgód.

3. Administrator zarządza uprawnieniami swoich użytkowników w Aplikacji i odpowiada za zachowanie poufności ich danych logowania.

§ 6. Obowiązki Podmiotu przetwarzającego

Podmiot przetwarzający zobowiązuje się:

1. przetwarzać Dane Powierzone wyłącznie na udokumentowane polecenie Administratora przez aktywację usługi — chyba że obowiązek przetwarzania nakłada na niego prawo Unii lub prawo państwa członkowskiego; w takim przypadku poinformuje Administratora o tym obowiązku przed rozpoczęciem przetwarzania, o ile prawo to nie zabrania udzielenia takiej informacji (art. 28 ust. 3 lit. a RODO);

2. zapewnić, by osoby upoważnione do przetwarzania Danych Powierzonych zobowiązały się do zachowania tajemnicy lub podlegały ustawowemu obowiązkowi zachowania tajemnicy (art. 28 ust. 3 lit. b RODO);

3. wdrożyć i utrzymywać środki techniczne i organizacyjne wymagane na mocy art. 32 RODO, opisane w § 7 (art. 28 ust. 3 lit. c RODO);

4. przestrzegać warunków korzystania z usług Podprocesorów określonych w § 8 (art. 28 ust. 3 lit. d RODO);

5. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomagać Administratorowi — poprzez odpowiednie środki techniczne i organizacyjne, w tym funkcje Aplikacji (eksport, anonimizacja, usunięcie danych klienta, rejestr zgód) — wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO (art. 28 ust. 3 lit. e RODO);

6. pomagać Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO (bezpieczeństwo, zgłaszanie naruszeń, ocena skutków dla ochrony danych), uwzględniając charakter przetwarzania i dostępne mu informacje (art. 28 ust. 3 lit. f RODO);

7. po zakończeniu świadczenia usług usunąć lub zwrócić Dane Powierzone zgodnie z § 12 (art. 28 ust. 3 lit. g RODO);

8. udostępniać Administratorowi informacje niezbędne do wykazania spełnienia obowiązków z art. 28 RODO oraz umożliwiać audyty na zasadach określonych w § 11 (art. 28 ust. 3 lit. h RODO);

9. niezwłocznie poinformować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

§ 7. Środki techniczne i organizacyjne

Podmiot przetwarzający stosuje w szczególności następujące środki:

1. szyfrowanie transmisji danych (TLS) oraz szyfrowanie danych w spoczynku na poziomie infrastruktury;
2. kontrolę dostępu opartą na rolach (RBAC) oraz uwierzytelnianie wieloskładnikowe (MFA);
3. logiczną izolację danych poszczególnych Administratorów (architektura multi-tenant z separacją per tenant) i Użytkowników (poprzez reguły RLS);
4. rejestr operacji na danych klientów (audit log) obejmujący dostęp, modyfikacje i eksport danych;
5. regularne kopie zapasowe oraz procedury odtwarzania danych;
6. monitoring błędów i bezpieczeństwa aplikacji z filtrowaniem danych osobowych z logów technicznych;
7. ograniczenie dostępu personelu do Danych Powierzonych do niezbędnego minimum (zasada need-to-know);
8. w Recepcji SilkAI: informowanie rozmówcy na początku każdej rozmowy, że rozmawia z asystentem opartym na sztucznej inteligencji działającym w imieniu Administratora; nagrywanie rozmów domyślnie wyłączone; przekazywanie asystentowi wyłącznie informacji niezbędnych do obsługi rozmowy, bez historii wizyt i danych o zdrowiu; przetwarzanie danych z rozmów przez Podprocesora wyłącznie w celu obsługi rozmowy, z umownym wyłączeniem ich wykorzystywania do rozwijania produktów i modeli Podprocesora.

§ 8. Podpowierzenie (Podprocesorzy)

1. Administrator udziela Podmiotowi przetwarzającemu ogólnej zgody na korzystanie z usług Podprocesorów, w rozumieniu art. 28 ust. 2 RODO.
2. Aktualna lista zatwierdzonych Podprocesorów wraz z zakresem podpowierzanych danych i lokalizacją przetwarzania stanowi Załącznik B do Umowy i jest publikowana pod adresem: silkcrm.net/podprocesorzy.
3. O zamierzonej zmianie dotyczącej dodania lub zastąpienia Podprocesora Podmiot przetwarzający poinformuje Administratora (e-mailem na adres konta lub komunikatem w Aplikacji) z wyprzedzeniem co najmniej 14 dni, dając Administratorowi możliwość wyrażenia sprzeciwu.
4. W przypadku uzasadnionego sprzeciwu Strony podejmą w dobrej wierze rozmowy w celu znalezienia rozwiązania; jeżeli nie będzie ono możliwe, Administrator może wypowiedzieć Umowę Główną przed rozpoczęciem przetwarzania przez nowego Podprocesora, bez ponoszenia opłat za niewykorzystany okres.
5. Podmiot przetwarzający nakłada na każdego Podprocesora — na mocy umowy — te same obowiązki ochrony danych, jakie wynikają z niniejszej Umowy, w szczególności obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych; za działania i zaniechania Podprocesorów Podmiot przetwarzający odpowiada jak za własne.
6. Zakres danych przekazywanych poszczególnym Podprocesorom jest ograniczony do minimum niezbędnego do realizacji ich funkcji, zgodnie z Załącznikiem B.
7. Podprocesor wskazany w Załączniku B jako obsługujący Recepcję SilkAI przetwarza Dane Powierzone wyłącznie w odniesieniu do Administratorów, którzy uruchomili ten moduł.

§ 9. Przekazywanie danych poza EOG

1. Główna baza Danych Powierzonych jest utrzymywana na terenie EOG, w Irlandii. Niektóre Dane Powierzone mogą być przetwarzane lub przekazywane poza EOG wyłącznie w zakresie niezbędnym do świadczenia usług przez Podprocesorów wskazanych w Załączniku B i na zasadach określonych poniżej.
2. Przekazanie Danych Powierzonych do państwa trzeciego następuje wyłącznie w zakresie opisanym w Załączniku B i wyłącznie z zapewnieniem odpowiednich zabezpieczeń, o których mowa w rozdziale V RODO: decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (w tym EU-U.S. Data Privacy Framework dla certyfikowanych podmiotów w USA) lub standardowych klauzul umownych (SCC), wraz z — w razie potrzeby — środkami uzupełniającymi.

3. Na żądanie Administratora Podmiot przetwarzający udostępni informacje o zastosowanych mechanizmach transferu.

§ 10. Naruszenia ochrony danych

1. Podmiot przetwarzający dokonuje wstępnego zawiadomienia bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od powzięcia wiadomości o naruszeniu. Informacje niedostępne w chwili pierwszego zawiadomienia mogą być przekazywane sukcesywnie.
2. Zawiadomienie obejmuje, w miarę dostępności informacji: opis charakteru naruszenia, kategorie i przybliżoną liczbę osób oraz rekordów, możliwe konsekwencje, zastosowane i proponowane środki zaradcze oraz dane kontaktowe do dalszych informacji.
3. Podmiot przetwarzający dokumentuje naruszenia i współpracuje z Administratorem w zakresie zgłoszenia naruszenia Prezesowi UODO oraz zawiadomienia osób, których dane dotyczą, jeżeli obowiązki te powstaną po stronie Administratora.

§ 11. Prawo kontroli (audyt)

1. Administrator ma prawo do przeprowadzenia audytu zgodności przetwarzania Danych Powierzonych z Umową — nie częściej niż raz w roku, chyba że audyt jest wymagany przez organ nadzorczy, wynika z naruszenia lub incydentu bezpieczeństwa, istotnej zmiany sposobu przetwarzania albo Administrator posiada uzasadnione podstawy do podejrzenia naruszenia DPA lub przepisów ochrony danych.
2. Audyt wymaga zawiadomienia z wyprzedzeniem co najmniej 14 dni roboczych, jest przeprowadzany w godzinach pracy Podmiotu przetwarzającego, w sposób nienaruszający tajemnicy przedsiębiorstwa oraz danych innych administratorów, i nie może zakłócać bieżącej działalności.
3. Podmiot przetwarzający realizuje prawo kontroli poprzez udzielenie odpowiedzi na pisemne pytania (poprzez kwestionariusz) oraz ewentualnie udostępnienie posiadanej dokumentacji, raportów i certyfikacji dotyczących bezpieczeństwa (w tym dokumentacji Podprocesorów w zakresie, w jakim Podmiot przetwarzający posiada taką dokumentację i jest uprawniony do jej ujawnienia; w pozostałym zakresie może udostępnić raport, zaświadczenie, streszczenie lub inne równoważne dowody).
4. Koszty audytu ponosi Administrator, chyba że audyt wykaże istotne naruszenie Umowy przez Podmiot przetwarzający.

§ 12. Usunięcie danych po zakończeniu przetwarzania

1. Po zakończeniu świadczenia usług Podmiot przetwarzający, według wyboru Administratora:
   a) usuwa wszystkie Dane Powierzone i ich kopie, albo
   b) zwraca Administratorowi Dane Powierzone w powszechnie używanym formacie, a następnie usuwa pozostające w jego posiadaniu kopie, z zastrzeżeniem danych, których dalsze przechowywanie jest wymagane prawem.
2. Usunięcie Danych Powierzonych z systemów produkcyjnych następuje w terminie 30 dni od zakończenia Umowy Głównej lub od decyzji Administratora; dane w kopiach zapasowych są nadpisywane w cyklu rotacji kopii, nie dłużej niż w terminie 90 dni — w tym czasie dane nie podlegają modyfikacjom ani przetwarzaniu operacyjnemu poza ewentualnym odtworzeniem awaryjnym (disaster recovery).
3. Podmiot przetwarzający może zachować dane w zakresie i przez okres, w jakim obowiązek ich przechowywania wynika z prawa Unii lub prawa państwa członkowskiego.
4. Na żądanie Administratora Podmiot przetwarzający potwierdzi wykonanie usunięcia danych.

§ 13. Odpowiedzialność

1. Każda ze Stron odpowiada za szkody wyrządzone osobom, których dane dotyczą, na zasadach określonych w art. 82 RODO.

2. Odpowiedzialność Podmiotu przetwarzającego wobec Administratora z tytułu niniejszej Umowy podlega ograniczeniom odpowiedzialności przewidzianym w Umowie Głównej, w zakresie dopuszczalnym przez bezwzględnie obowiązujące przepisy prawa.

§ 14. Postanowienia końcowe

1. W sprawach nieuregulowanych stosuje się postanowienia Umowy Głównej, przepisy RODO oraz prawo polskie.
2. Zmiany niniejszej Umowy następują w trybie przewidzianym dla zmian Regulaminu, z zastrzeżeniem § 8 ust. 3–4 (zmiany listy Podprocesorów).
3. Jeżeli poszczególne postanowienia Umowy okażą się nieważne lub bezskuteczne, pozostałe postanowienia pozostają w mocy.
4. W przypadku sprzeczności pomiędzy postanowieniami niniejszej DPA a Umową Główną w zakresie przetwarzania Danych Powierzonych pierwszeństwo mają postanowienia DPA.
5. Kontakt w sprawach ochrony danych: privacy@silkcrm.net.

Załącznik A — Opis przetwarzania

Przedmiot przetwarzania	Dane osobowe klientów końcowych Administratora (klientów salonu) wprowadzone do Aplikacji SilkCRM, a także dane osób dzwoniących do Administratora, jeżeli Administrator uruchomi Recepcję SilkAI.
Czas trwania	Okres obowiązywania Umowy Głównej (Regulaminu), z uwzględnieniem § 12 Umowy (usunięcie danych po zakończeniu).
Charakter przetwarzania	Przetwarzanie w systemach informatycznych, w sposób zautomatyzowany: zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, przeglądanie, wykorzystywanie, przesyłanie (wysyłka komunikacji), usuwanie; w Recepcji SilkAI także przetwarzanie głosu w czasie rzeczywistym, transkrypcja i podsumowanie rozmowy.
Cel przetwarzania	Świadczenie usługi SilkCRM na rzecz Administratora, w szczególności: prowadzenie kartotek klientów, rezerwacje i kalendarz wizyt, historia usług, komunikacja z klientami (SMS, e-mail), kampanie marketingowe Administratora, segmentacja i analityka, obsługa zgód, kopie zapasowe, a w przypadku uruchomienia Recepcji SilkAI — odbieranie połączeń telefonicznych kierowanych do Administratora, udzielanie informacji o jego ofercie oraz umawianie, przekładanie i odwoływanie wizyt.
Kategorie osób	Klienci końcowi Administratora (osoby korzystające z usług salonu / kliniki), w tym potencjalni klienci (leady) wprowadzeni do Aplikacji; osoby dzwoniące do Administratora, jeżeli Administrator uruchomi Recepcję SilkAI; pracownicy, współpracownicy i inne osoby wykonujące usługi na rzecz Administratora.
Rodzaje danych osobowych	a) dane identyfikacyjne: imię, nazwisko, data urodzenia; b) dane kontaktowe: numer telefonu, adres e-mail, adres; c) dane dotyczące korzystania z usług: historia wizyt i zabiegów, rezerwacje, preferencje, notatki pracowników, zdjęcia efektów zabiegów (jeżeli Administrator je wprowadza), historia zakupów i płatności w salonie, przyznane rabaty i pakiety; d) dane dotyczące komunikacji: treść wysłanych wiadomości, zgody marketingowe wraz z historią ich zmian, adres IP przy wyrażeniu zgody; e) szczególne kategorie danych (art. 9 RODO) — dane dotyczące zdrowia, jeżeli Administrator je wprowadza: alergie i alergeny, przeciwwskazania do zabiegów, wyniki testów płatkowych, informacje o chorobach skóry. Do danych dotyczących zdrowia mogą należeć również zdjęcia, historia zabiegów oraz notatki, jeżeli ze względu na swoją treść ujawniają informacje dotyczące stanu zdrowia osoby. Za istnienie ważnej podstawy prawnej przetwarzania tych danych (art. 9 ust. 2 RODO) odpowiada Administrator. Aplikacja nie służy do prowadzenia dokumentacji medycznej (§ 4 ust. 4); f) dane identyfikacyjne, grafik i czas pracy, wykonane usługi, przypisane transakcje, informacje dotyczące wynagrodzeń, prowizji lub premii — pracowników, współpracowników i podwykonawców usług na rzecz Administratora, w zakresie wykorzystywanym przez Administratora; g) dane z rozmów obsługiwanych przez Recepcję SilkAI (jeżeli Administrator uruchomi moduł): numer telefonu rozmówcy, głos i treść rozmowy przetwarzane w czasie rzeczywistym, transkrypcja i podsumowanie rozmowy, dane podane w rozmowie (np. imię, wybrana usługa i termin), wynik rozmowy; nagranie dźwiękowe rozmowy — wyłącznie jeżeli Administrator włączy nagrywanie.

Załącznik B — Lista zatwierdzonych Podprocesorów

Stan na: 1.11.2026 r.

Zakres danych przekazywanych każdemu Podprocesorowi jest ograniczony do niezbędnego minimum.

Podprocesor	Cel / rola, nazwa usługi	Zakres powierzonych danych	Lokalizacja przetwarzania	Podstawa transferu
Supabase, Inc. (USA)	Hosting bazy danych; Supabase	Pełny zakres Danych Powierzonych określony w Załączniku A	EOG — Irlandia (AWS, region eu-west-1, Dublin)	Dane w EOG; na wypadek zdalnego dostępu spoza EOG: standardowe klauzule umowne (SCC) w DPA Supabase
Google Ireland Ltd. (Irlandia)	Infrastruktura aplikacji, load balancing; Google Cloud Platform	Dane przetwarzane w warstwie aplikacji (w ruchu); pełny zakres Danych Powierzonych	EOG — region UE: europe-west1 (Belgia)	Dane w EOG; Google certyfikowany w EU-U.S. DPF, SCC w Cloud Data Processing Addendum
Plus Five Five, Inc. (USA)	Wysyłka wiadomości e-mail (transakcyjnych i kampanii); Resend	Adres e-mail i imię odbiorcy oraz treść wysyłanej wiadomości (bez treści dot. danych o zdrowiu)	Wysyłka z regionu EOG (eu-west-1, Irlandia); dane konta, logi i metadane wiadomości przechowywane w USA	EU-U.S. Data Privacy Framework (Resend certyfikowany) oraz SCC
LINK Mobility Poland Sp. z o.o. (Polska)	Wysyłka wiadomości SMS; SMSAPI	Numer telefonu i imię odbiorcy oraz treść wysyłanej wiadomości (bez treści dot. danych o zdrowiu)	Polska / EOG (grupa LINK Mobility — podmioty w EOG i Norwegii, państwie EOG)	Przetwarzanie w EOG; umowa powierzenia (UPPDO) z LINK Mobility Poland
Functional Software, Inc (USA)	Diagnostyka działania aplikacji; Sentry	Ograniczony zakres technicznych danych osobowych związanych z działaniem aplikacji, takich jak identyfikatory techniczne lub sesyjne, dane urządzenia i informacje diagnostyczne. Dane identyfikacyjne klientów, treści wiadomości i dane szczególnych kategorii są filtrowane przed wysłaniem.	USA	Privacy Framework / SCC (DPA Sentry)
Telnyx LLC (USA)	Obsługa połączeń telefonicznych przez asystenta głosowego: telefonia, rozpoznawanie i synteza mowy, model językowy; Recepcja SilkAI — wyłącznie u Administratorów, którzy uruchomili moduł	Numer telefonu rozmówcy, głos i treść rozmowy przetwarzane w czasie rzeczywistym, transkrypcja; informacje o ofercie, usługach i wolnych terminach Administratora; imię klienta, jeżeli został rozpoznany po numerze telefonu; nagranie rozmowy wyłącznie po włączeniu nagrywania przez Administratora (bez historii wizyt i danych o zdrowiu)	Region UE (punkt obsługi połączeń we Frankfurcie, przetwarzanie mowy i modelu językowego na infrastrukturze Telnyx w UE, przechowywanie w UE); w razie awarii, obsługi technicznej lub przeciwdziałania nadużyciom możliwe przetwarzanie poza EOG	Standardowe klauzule umowne (SCC, moduł 3) w DPA Telnyx oraz EU-U.S. Data Privacy Framework

Nota — podmioty niebędące Podprocesorami Danych Powierzonych

Stripe, Inc. (USA — płatności za subskrypcję SilkCRM; certyfikowany w EU-U.S. Data Privacy Framework) oraz Clerk, Inc. (USA — uwierzytelnianie użytkowników Aplikacji; certyfikowany w EU-U.S. Data Privacy Framework) przetwarzają wyłącznie dane Administratora i jego personelu, dla których SilkCRM jest samodzielnym administratorem. W tym zakresie nie przetwarzają Danych Powierzonych (danych klientów końcowych salonu) i dlatego nie figurują na liście Podprocesorów.

Płatności online klientów Administratora (zadatki i przedpłaty) obsługuje Stripe na koncie połączonym (Stripe Connect), które Administrator prowadzi na podstawie własnej umowy ze Stripe. Na polecenie Administratora Aplikacja przekazuje do Stripe kwotę, opis płatności i adres e-mail klienta, jeżeli jest znany. W tym zakresie Stripe przetwarza dane na podstawie umowy z Administratorem, a nie jako Podprocesor SilkCRM.

Microsoft Corporation (USA — Microsoft Clarity, analityka korzystania z Aplikacji) otrzymuje nagrania sesji panelu, widgetu rezerwacji, portalu klienta i stron otwieranych z wiadomości do klientów z maskowaniem całej wyświetlanej treści. Nie otrzymuje Danych Powierzonych i dlatego nie figuruje na liście Podprocesorów. Zasady przetwarzania danych przez podmioty wskazane w nocie opisuje Polityka Prywatności SilkCRM.