

Umowa powierzenia przetwarzania danych osobowych

Załącznik nr 1 do Regulaminu świadczenia usług Brifli - wersja 2 - 26 października 2026 r.

Umowa jest zawierana razem z Regulaminem, przez akceptację w formularzu rejestracji. Można ją w każdej chwili pobrać i zapisać ze strony app.brifli.pl/umowa-powierzenia.

Strony:

1. Usługobiorca w rozumieniu Regulaminu - jako administrator danych (dalej: „Administrator”);
2. Social Dreams sp. z o.o. z siedzibą w Krakowie, ul. Szpakowa 10/143, 30-691 Kraków, KRS 0000910947, NIP 9372736564, REGON 389419750 - jako podmiot przetwarzający (dalej: „Procesor”).

Pojęcia pisane wielką literą mają znaczenie z Regulaminu. RODO oznacza rozporządzenie (UE) 2016/679.

§ 1. Przedmiot i czas przetwarzania

1. Administrator powierza Procesorowi przetwarzanie danych osobowych zawartych w Danych Spraw, w zakresie i celu opisanym w § 2, a Procesor zobowiązuje się przetwarzać je zgodnie z Umową powierzenia i RODO.
2. Przetwarzanie trwa przez czas obowiązywania Umowy i do usunięcia danych według § 11.

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

1. Cel: wyłącznie świadczenie usług opisanych w Regulaminie na rzecz Administratora: przechowywanie dokumentów, ich odczyt i analiza przez System z użyciem modelu AI, przygotowanie Analiz i Projektów pism, udostępnianie ich Użytkownikom Administratora.
2. Charakter: zautomatyzowane przetwarzanie w Systemie: zapisywanie, przechowywanie, przegląd przez skaner złośliwego oprogramowania, odczyt treści stron przez model AI, porządkowanie, zestawianie, udostępnianie Użytkownikom, pobieranie, usuwanie.
3. Rodzaje danych:
 - 1) dane zwykłe: imiona i nazwiska, numery PESEL, adresy, dane kontaktowe, numery spraw i szkód, dane o zatrudnieniu i dochodach, dane o zdarzeniu i jego skutkach, wszelkie inne dane zawarte we wgranych dokumentach lub wpisane przez Użytkowników do Spraw (np. notatki przy faktach, dane osób uprawnionych), a także dane kancelarii wpisywane do pism (imię i nazwisko pełnomocnika, tytuł, adres, telefon, e-mail);
 - 2) dane szczególnej kategorii - dane dotyczące zdrowia (art. 9 ust. 1 RODO): dokumentacja medyczna, rozpoznania i kody ICD-10, przebieg leczenia, koszty leczenia, opinie biegłych, także dane o zdrowiu osób uprawnionych po śmierci poszkodowanego i dane o zdrowiu wpisane w notatkach przy faktach;
 - 3) mogą występować dane dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO), np. w dokumentach postępowań karnych.
4. Kategorie osób: klienci Administratora (poszkodowani), w tym zmarli poszkodowani i ich bliscy jako osoby uprawnione; członkowie rodzin poszkodowanych; sprawcy zdarzeń; świadkowie; personel medyczny; biegli; pracownicy ubezpieczycieli i innych instytucji; pełnomocnicy i pracownicy Administratora wskazani w pismach; osoby, których dokumenty trafiły do Sprawy omyłkowo; Użytkownicy Administratora w zakresie, w jakim System zapisuje, kto sprawdził fakt, dodał notatkę lub zgłosił błąd.

§ 3. Oświadczenia Administratora

1. Administrator oświadcza, że ma podstawę prawną do przetwarzania powierzanych danych, w tym danych o zdrowiu (art. 6 ust. 1 i art. 9 ust. 2 RODO), i że wypełnił obowiązki informacyjne wobec osób, których dane dotyczą.

2. Administrator wgrywa do Systemu tylko dane potrzebne do prowadzenia sprawy.
3. Ocenę skutków dla ochrony danych (art. 35 RODO), jeżeli jest wymagana, przeprowadza Administrator; Procesor pomaga według § 9 ust. 2.
4. Administrator decyduje, czy Konto jest chronione drugim składnikiem logowania (§ 5 ust. 8 Regulaminu). Procesor udostępnia drugi składnik i zaleca jego włączenie. Brak włączenia go przez Administratora nie zwalnia Procesora z obowiązków z art. 32 RODO; Administrator uwzględnia tę decyzję w swojej ocenie ryzyka i w ocenie skutków.

§ 4. Polecenia Administratora

1. Procesor przetwarza dane wyłącznie na udokumentowane polecenie Administratora. Poleceniem jest: Umowa powierzenia, Regulamin, każda czynność Użytkownika w Systemie (np. wgranie dokumentu, uruchomienie Analizy, wygenerowanie Projektu pisma) oraz polecenie przesłane e-mailem z adresu Konta na kontakt@brifli.pl albo pismem podpisanym przez osobę uprawnioną do reprezentacji Administratora.
2. Polecenie obejmuje przekazanie danych do państw trzecich w zakresie opisanym w § 7 i Załączniku B.
3. Jeżeli prawo Unii lub prawo polskie nakłada na Procesora obowiązek innego przetwarzania, Procesor informuje o tym Administratora przed rozpoczęciem przetwarzania, chyba że prawo tego zabrania z uwagi na ważny interes publiczny.
4. Procesor niezwłocznie informuje Administratora, jeżeli jego zdaniem polecenie narusza RODO lub inne przepisy o ochronie danych.

§ 5. Zakaz przetwarzania do własnych celów

1. Procesor nie przetwarza Danych Spraw do żadnych własnych celów. W szczególności nie używa ich do trenowania, testowania ani ulepszania modeli AI lub Systemu, do tworzenia statystyk, zestawień, porównań ani baz danych, do celów marketingowych ani do sprzedaży.
2. Dostawca modelu AI (AWS Bedrock) nie wykorzystuje przesyłanych treści do trenowania modeli; zapisywanie wywołań modelu w logach dostawcy jest wyłączone.
3. Zakaz nie obejmuje danych o Koncie i korzystaniu z Systemu (np. liczby Stron, Spraw, Analiz, liczby i rodzaju zgłoszeń błędów bez ich treści), których administratorem jest Procesor (§ 11 Regulaminu).

§ 6. Poufność i osoby upoważnione

1. Dostęp do Danych Spraw mają wyłącznie osoby upoważnione przez Procesora na piśmie, zobowiązane do zachowania poufności, także po zakończeniu współpracy. Procesor prowadzi ewidencję upoważnień.
2. Osoby z zespołu Procesora nie przeglądają treści Danych Spraw. Wgląd w treść jest dopuszczalny wyłącznie na prośbę Administratora (np. przy reklamacji albo zgłoszeniu awarii - § 14 ust. 4 Regulaminu), tylko w zakresie wskazanej Sprawy i potrzebnym do jej obsługi, oraz gdy wymaga tego przepis prawa (§ 4 ust. 3) - wtedy Procesor informuje Administratora, chyba że przepis tego zabrania. Zgłoszenie nielegalnych treści dotyczące treści w Sprawie (§ 8 ust. 2 Regulaminu) Procesor najpierw przekazuje Administratorowi - bez danych zgłaszającego, chyba że są niezbędne - z prośbą o stanowisko w ciągu 5 dni roboczych, bez otwierania Danych Spraw; wgląd w treść następuje tylko wtedy, gdy bez niego nie da się rozpatrzyć zgłoszenia zgodnie z prawem, wyłącznie w zakresie wskazanym w zgłoszeniu i po poinformowaniu Administratora, chyba że przepis tego zabrania.
3. Każdy wgląd Procesor odnotowuje: data, osoba, Sprawa (identyfikator) i powód, bez danych osobowych z dokumentów. Na żądanie Administratora Procesor przekazuje wykaz wglądów w jego Sprawy.
4. Procesor wie, że Dane Spraw mogą być objęte tajemnicą adwokacką lub radcowską, i chroni je odpowiednio do wagi tej tajemnicy.

§ 7. Dalsze podmioty przetwarzające i przekazanie poza EOG

1. Administrator wyraża ogólną pisemną zgodę na korzystanie przez Procesora z dalszych podmiotów przetwarzających. Wykaz na dzień zawarcia Umowy powierzenia zawiera Załącznik B.
2. Procesor nakłada na każdy dalszy podmiot przetwarzający, umową, te same obowiązki ochrony danych co w Umowie powierzenia, w szczególności obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych. Procesor odpowiada wobec Administratora za wykonanie obowiązków przez dalszy podmiot przetwarzający jak za własne działania.
3. O zamiarze dodania lub zastąpienia dalszego podmiotu przetwarzającego Procesor informuje co najmniej 14 dni wcześniej, e-mailem na adres Konta i komunikatem w Systemie. Administrator może w tym terminie wyrazić sprzeciw na kontakt@brifli.pl. Zmianę Administrator akceptuje kliknięciem (§ 16 ust. 3 Regulaminu). Jeżeli Strony nie uzgodnią rozwiązania, Administrator może wypowiedzieć Umowę przed wejściem zmiany w życie, bez kosztów (§ 16 ust. 4 Regulaminu). Przy zmianie u dalszego podmiotu przetwarzającego dostawcy infrastruktury (np. nowy podwykonawca Supabase) Procesor przekazuje informację niezwłocznie po jej otrzymaniu; sprzeciw Administratora nie wstrzymuje takiej zmiany - Administrator może wtedy wypowiedzieć Umowę bez kosztów przed jej wejściem w życie.
4. Dane Spraw są przechowywane w Unii Europejskiej (baza danych i pliki - Frankfurt), model AI działa w regionach AWS w UE, a aplikacja - w Paryżu. Część dalszych podmiotów lub ich podwykonawców ma siedzibę albo personel poza Europejskim Obszarem Gospodarczym, a ruch sieciowy i pamięć podręczna sieci mogą przechodzić przez węzły poza EOG. W szczególności przy pobraniu pliku ze Sprawy kopia pliku trafia do pamięci podręcznej węzła sieci Cloudflare najbliższego pobierającemu, a przy pobraniu spoza EOG węzeł ten może być poza EOG; kopia jest wydawana tylko do końca ważności podpisanego linku (120-300 s), ale jej fizyczne usunięcie z węzła zależy od Cloudflare i Supabase go nie gwarantuje. Cloudflare działa jako podwykonawca Supabase - Supabase odpowiada za niego na podstawie umowy z nim, a narzędzia przekazania z rozdziału V RODO między nimi nie podaje (Załącznik B). Przy każdym dalszym podmiocie Załącznik B opisuje, czy dochodzi do przekazania poza EOG i na jakiej podstawie (dla Supabase - standardowe klauzule ochrony danych przyjęte przez Komisję Europejską, art. 46 ust. 2 lit. c RODO).
5. Procesor udostępnia Administratorowi na żądanie podsumowanie oceny skutków przekazania danych do Supabase Pte. Ltd.
6. Gdy dalszy podmiot przetwarzający działa na podstawie standardowych klauzul umownych, Procesor niezwłocznie, nie później niż w 2 dni robocze, przekazuje Administratorowi otrzymane od niego: zawiadomienie o prawnie wiążącym żądaniu organu publicznego państwa trzeciego ujawnienia Danych Spraw albo o bezpośrednim dostępie takiego organu do Danych Spraw, zawiadomienie, że dalszy podmiot podlega przepisom lub praktykom, które nie pozwalają mu wykonywać klauzul, okresowe informacje o otrzymanych żądaniach oraz wynik jego oceny legalności żądania - chyba że zabrania tego prawo Unii lub prawo polskie. Środki zaradcze Procesor uzgadnia z Administratorem. Na polecenie Administratora Procesor wstrzymuje przekazywanie: blokuje wgrywanie dokumentów i Analizy w jego Sprawach, a na żądanie przekazuje eksport i usuwa Dane Spraw według § 11 ust. 2-4; Administrator może wtedy wypowiedzieć Umowę bez kosztów.

§ 8. Bezpieczeństwo

1. Procesor stosuje środki techniczne i organizacyjne wymagane przez art. 32 RODO. Ich opis na dzień zawarcia Umowy powierzenia zawiera Załącznik A.
2. Procesor może zmieniać środki, jeżeli poziom ochrony nie spada. Istotną zmianę na niekorzyść Procesor zgłasza jak zmianę Umowy powierzenia (§ 16 Regulaminu).

§ 9. Pomoc Administratorowi

1. Prawa osób: biorąc pod uwagę charakter przetwarzania, Procesor pomaga Administratorowi odpowiadać na żądania osób, których dane dotyczą (rozdział III RODO). Na polecenie Administratora Procesor:

- 1) udostępnia eksport Danych Spraw w formacie nadającym się do odczytu maszynowego, razem z plikami - Administrator pobiera go sam w Systemie (Ustawienia, Eksport danych), w każdej chwili, także w trybie tylko do odczytu; gdy pobranie w Systemie nie jest możliwe, Procesor przekazuje eksport na zaszyfowanym nośniku, z hasłem przekazany osobno, bez wysyłania Danych Spraw e-mailem;
 - 2) usuwa wskazaną Sprawę wraz z jej kopiami w Systemie w ciągu 14 dni i potwierdza wykonanie. Zapis odczytu pliku, który Administrator wgrał także do innej swojej Sprawy, zostaje do usunięcia tamtej Sprawy. Żądanie, które osoba skieruje wprost do Procesora, Procesor niezwłocznie przekazuje Administratorowi i sam na nie nie odpowiada.
2. Bezpieczeństwo, naruszenia, ocena skutków: uwzględniając charakter przetwarzania i dostępne mu informacje, Procesor pomaga Administratorowi wywiązać się z obowiązków z art. 32-36 RODO, w szczególności przekazuje informacje o Systemie potrzebne do oceny skutków dla ochrony danych.

§ 10. Naruszenia ochrony danych

1. Po stwierdzeniu naruszenia ochrony Danych Spraw Procesor zgłasza je Administratorowi bez zbędnej zwłoki, nie później niż w ciągu 48 godzin, na adres e-mail Konta oraz na adres do spraw danych, jeżeli Administrator wskazał go w Systemie (Ustawienia).
2. Zgłoszenie zawiera co najmniej: opis charakteru naruszenia, w tym w miarę możliwości kategorie i przybliżoną liczbę osób oraz wpisów, możliwe konsekwencje, podjęte i proponowane środki zaradcze oraz kontakt do osoby, która udzieli dalszych informacji. Informacji, których nie da się podać od razu, Procesor udziela sukcesywnie, bez zbędnej zwłoki.
3. Procesor dokumentuje każde naruszenie Danych Spraw i współpracuje z Administratorem przy jego wyjaśnieniu.

§ 11. Usunięcie i zwrot danych

1. Po rozwiązaniu Umowy Administrator może przez 30 dni przeglądać Dane Spraw i pobierać ich eksport razem z plikami w Systemie, a gdy pobranie nie jest możliwe - zgłosić to według § 15 ust. 6 Regulaminu. Wygaśnięcie Umowy z braku aktywności (§ 15 ust. 7 Regulaminu) ma w tym paragrafie takie same skutki jak jej rozwiązanie; terminy z ust. 1 i 2 liczą się od dnia wygaśnięcia.
2. Po upływie 30 dni od rozwiązania Umowy, a jeżeli Administrator dokonał w tym terminie zgłoszenia z § 15 ust. 6 Regulaminu - po upływie 7 dni od przekazania eksportu, jeżeli to później, w każdym przypadku nie później niż 60 dni od rozwiązania Umowy, Procesor usuwa wszystkie Dane Spraw Administratora, łącznie ze wszystkimi ich kopiami (w tym zapisami odczytów stron), chyba że prawo Unii lub prawo polskie nakazuje ich przechowywanie.
3. Dane usunięte z bazy znikają z kopii zapasowych bazy w ciągu 8 dni (kopie są przechowywane 7 dni). Wgrane pliki nie są objęte kopiami zapasowymi.
4. Procesor potwierdza Administratorowi usunięcie e-mailem.
5. Usunięcie nie obejmuje rejestru zdarzeń Systemu, który Procesor prowadzi jako administrator w celu rozliczalności i bezpieczeństwa usługi i przechowuje 3 lata od wpisu, a wpis rejestracji (dowód akceptacji Regulaminu i Polityki prywatności) - do usunięcia danych Administratora jako klienta (3 lata od końca roku, w którym zakończyło się korzystanie z Systemu). Rejestr nie zawiera treści dokumentów ani danych z dokumentów.

§ 12. Kontrola (audyt)

1. Procesor udostępnia Administratorowi informacje niezbędne do wykazania, że spełnia obowiązki z art. 28 RODO, i umożliwia audyty, w tym inspekcje, przeprowadzane przez Administratora lub upoważnionego przez niego audytora.
2. Podstawową formą audytu jest kwestionariusz przesłany na kontakt@brifli.pl z co najmniej 14-dniowym

wyprzedzeniem, nie częściej niż raz na 12 miesięcy. Procesor odpowiada w ciągu 14 dni.

3. Audyt w innej formie, w tym inspekcja w siedzibie Procesora, oraz audyt dodatkowy są możliwe po naruszeniu ochrony Danych Spraw, na żądanie organu nadzorczego albo gdy Administrator uzna, z podaniem uzasadnienia, że odpowiedzi na kwestionariusz nie wystarczają do wykazania zgodności; zawiadomienie - co najmniej 14 dni wcześniej, chyba że sprawa jest pilna. Postanowienia tego paragrafu nie ograniczają uprawnień organu nadzorczego.
4. Audyt odbywa się w godzinach pracy, nie narusza tajemnic Procesora ani danych innych usługobiorców; audytor zewnętrzny zobowiązuje się do poufności. Koszty audytu ponosi Administrator.

§ 13. Odpowiedzialność

1. Strony odpowiadają wobec osób, których dane dotyczą, zgodnie z art. 82 RODO.
2. Odpowiedzialność Procesora wobec Administratora z tytułu Umowy powierzenia podlega ograniczeniom z § 13 Regulaminu.

§ 14. Postanowienia końcowe

1. Umowa powierzenia obowiązuje przez czas obowiązywania Umowy; obowiązki z § 6 ust. 1 i 4, § 11 i § 12 trwają do ich wykonania, a poufność - bezterminowo.
2. Zmiany Umowy powierzenia - według § 16 Regulaminu, z akceptacją kliknięciem.
3. W razie sprzeczności między Regulaminem a Umową powierzenia w sprawach ochrony danych osobowych pierwszeństwo ma Umowa powierzenia.
4. W sprawach nieuregulowanych stosuje się RODO i Kodeks cywilny.

Załącznik A. Środki techniczne i organizacyjne

Stan na 26 października 2026 r.

Lokalizacja i dostawcy

- Baza danych, pliki, logowanie i funkcje przetwarzające: Supabase, region Frankfurt (Niemcy).
- Model AI: AWS Bedrock, wywołanie z regionu Frankfurt, profil obejmujący wyłącznie regiony AWS w UE (Frankfurt, Sztokholm, Mediolan, Hiszpania, Irlandia, Paryż). Zapisywanie wywołań modelu wyłączone we wszystkich sześciu regionach.
- Hosting aplikacji: Clever Cloud, strefa Paryż (Francja).

Oddzielenie danych kancelarii

- Każda tabela z danymi kancelarii ma w bazie zasady dostępu na poziomie wierszy (Row Level Security) w trybie wymuszonym: Użytkownik widzi wyłącznie dane własnej kancelarii.
- Pliki leżą w prywatnym magazynie, w folderach kancelarii, z zasadami dostępu według folderu kancelarii; Użytkownik pobiera plik przez krótkotrwały podpisany link ważny 120-300 sekund.
- Oddzielenie danych między kancelariami jest sprawdzane testem uruchamianym przed włączeniem każdej zmiany kodu Systemu do wersji głównej.
- Po zakończeniu Umowy baza danych blokuje dodawanie i zmianę Spraw, dokumentów, Analiz i pism (tryb tylko do odczytu); przeglądanie, pobieranie i eksport działają. Eksport przekazywany poza Systemem - wyłącznie na zaszyfrowanym nośniku, doręczonym osobiście albo przesyłką, z hasłem przekazany osobno; kopia eksportu u Procesora usuwana najpóźniej 30 dni po przekazaniu, a po zakończeniu Umowy - razem z Danymi Spraw (§ 11 ust. 2). Komputery zespołu, na których powstaje eksport, mają zaszyfrowany dysk.

Wgrywanie i przetwarzanie

- Każdy plik jest sprawdzany skanerem złośliwego oprogramowania przed zapisaniem jako dokument; plik

niebezpieczny albo niesprawdzony jest odrzucany i usuwany.

- Funkcja analizy przyjmuje wyłącznie wywołanie z harmonogramu Systemu z sekretem i odmawia działania poza regionami AWS w UE.
- Klucze dające pełny dostęp do bazy i do modelu AI nie są przechowywane na serwerze aplikacji ani w kodzie i repozytorium.

Rozliczalność

- Rejestr zdarzeń tylko do dopisywania: aplikacja i skrypty administracyjne nie mogą zmieniać ani usuwać wpisów. Wpisy dotyczące Spraw zawierają identyfikatory, rodzaj czynności, czas, liczniki i wyniki, bez treści dokumentów.
- Drugi składnik logowania (kod jednorazowy z aplikacji w telefonie) dostępny dla Konta; przy Koncie z włączonym kodem baza danych nie udostępnia danych kancelarii sesji niepotwierdzonej kodem; o włączeniu decyduje Administrator (§ 3 ust. 4).
- Zespół Procesora ma osobny panel administracyjny, który nie pokazuje nazw Spraw, dokumentów ani wyników Analiz; dostęp administratora panelu wymaga drugiego składnika logowania (kod jednorazowy).

Ciągłość

- Kopia zapasowa bazy danych codziennie, przechowywana 7 dni; odtworzenie z kopii przetestowane. Wgrane pliki nie są objęte kopią zapasową.
- Eksport Danych Spraw w Systemie jest składany w chwili pobrania i przesyłany do przeglądarki Użytkownika, bez zapisywania kopii na serwerze.

Organizacja

- Pisemne upoważnienia i zobowiązania do poufności osób z dostępem do danych; ewidencja upoważnień.
- Wgląd zespołu w Dane Spraw tylko w przypadkach z § 6 ust. 2, z zapisem (§ 6 ust. 3).
- Zgłoszenia do wsparcia technicznego dostawców infrastruktury bez Danych Spraw; bez zgody na wgląd wsparcia dostawcy w Dane Spraw (wyjątek tylko decyzją członka zarządu, z zapisem jak w § 6 ust. 3).
- Drugi składnik logowania na kontach zespołu w Clever Cloud i AWS (konto główne); do Supabase zespół loguje się kontem GitHub z drugim składnikiem; w Google Workspace weryfikacja dwuetapowa jest włączona.
- Procedura postępowania z naruszeniem ochrony danych i rejestr naruszeń (zgłoszenie Administratorowi najpóźniej w 48 godzin - § 10).

Szyfrowanie

- Połączenia z Systemem oraz połączenia Systemu z bazą danych, modelem AI i skanerem plików są szyfrowane (HTTPS, TLS). Supabase szyfruje dyski i kopie zapasowe w spoczynku (AES-256, klucze chronione modułami HSM).
- AWS Bedrock nie zapisuje treści przesyłanych do modelu AI używanego w Systemie, poza automatycznym wykrywaniem materiałów przedstawiających seksualne wykorzystywanie dzieci w obrazach; dostawca modelu (Anthropic) nie ma do nich dostępu.

Załącznik B. Dalsze podmioty przetwarzające

Wersja 1 - 26 października 2026 r.

- Podmiot: Supabase Pte. Ltd., Singapur

Co robi z Danymi Spraw: baza danych, przechowywanie plików, logowanie, funkcje uruchamiające analizę

Gdzie: dane we Frankfurtzie (Niemcy)

Przekazanie poza EOG i podstawa: Supabase ma siedzibę w Singapurze, wsparcie techniczne i część podwykonawców w USA (lista: supabase.com/legal/customer-resources/subprocessor-list); ruch do Supabase przechodzi przez sieć Cloudflare (podwykonawca Supabase). Kopia pliku pobranego przez Użytkownika jest zapisywana w pamięci węzła sieci najbliższego pobierającemu i wydawana tylko do końca ważności podpisanego linku (120-300 s) - przy pobraniu spoza EOG węzeł może być poza EOG. Supabase nie pozwala wyłączyć tej pamięci podręcznej ani ograniczyć jej do węzłów w EOG; po wygaśnięciu linku kopia nie jest wydawana, ale jej fizyczne usunięcie z pamięci węzła zależy od Cloudflare i Supabase go nie gwarantuje. Podstawa przekazania do Supabase Pte. Ltd.: standardowe klauzule umowne w umowie powierzenia Supabase (moduł 3); podwykonawcy Supabase w USA - Supabase odpowiada za nich na podstawie umów z nimi, narzędzia przekazania z rozdziału V RODO nie podaje

- Podmiot: Cloudflare (podwykonawca Supabase)

Co robi z Danymi Spraw: przesyłanie ruchu między przeglądarką a Supabase: zapytania do bazy (w tym wyniki Analiz), logowanie, pobieranie i wgrywanie plików; kopia pobranego pliku w pamięci podręcznej węzła, wydawana do końca ważności podpisanego linku (fizyczne usunięcie zależy od Cloudflare)

Gdzie: węzeł sieci najbliższy Użytkownikowi (z Polski - Warszawa)

Przekazanie poza EOG i podstawa: przekazanie do Cloudflare, Inc. (USA) przy każdym węźle, także w UE; przy korzystaniu spoza EOG dodatkowo węzeł poza EOG; szyfrowanie połączenia kończy się na węźle Cloudflare; podstawa: Supabase odpowiada za swojego podwykonawcę na podstawie umowy z nim; narzędzia przekazania z rozdziału V RODO w tej umowie Supabase nie podaje; Cloudflare, Inc. deklaruje udział w programie EU-U.S. Data Privacy Framework (na liście programu oznaczona jako w trakcie ponownej certyfikacji), ale dane otrzymuje jako podwykonawca spółki z Singapuru

- Podmiot: Amazon Web Services EMEA SARL, Luksemburg - usługa AWS Bedrock

Co robi z Danymi Spraw: odczyt treści stron dokumentów i przygotowanie Analizy przez model AI (Claude, Anthropic)

Gdzie: wyłącznie regiony AWS w UE

Przekazanie poza EOG i podstawa: dane przetwarzane w UE; AWS nie zapisuje treści przesyłanych do modelu (poza automatycznym wykrywaniem materiałów przedstawiających seksualne wykorzystywanie dzieci w obrazach); dostawca modelu (Anthropic) nie ma dostępu do przesyłanych treści; umowa powierzenia AWS zawiera standardowe klauzule umowne

- Podmiot: Clever Cloud SAS, Nantes, Francja

Co robi z Danymi Spraw: hosting aplikacji: przez serwer aplikacji przechodzą m.in. nazwy Spraw, imię i nazwisko klienta Sprawy, nazwy plików, komentarze zgłoszeń i dane wpisywane do pism

Gdzie: Paryż (Francja)

Przekazanie poza EOG i podstawa: podwykonawcy wsparcia i obsługi klienta w USA; podstawa: standardowe klauzule umowne przyjęte przez Komisję Europejską (art. 46 ust. 2 lit. c RODO), zgodnie z umową powierzenia Clever Cloud

- Podmiot: widdix GmbH (attachmentAV), Niemcy

Co robi z Danymi Spraw: skanowanie każdego wgranego pliku pod kątem złośliwego oprogramowania; plik jest usuwany ze skanera po sprawdzeniu

Gdzie: serwery w UE

Przekazanie poza EOG i podstawa: plik jest przetwarzany w regionie UE; umowa powierzenia z widdix GmbH z 22.10.2026 obejmuje dane o zdrowiu; podwykonawcy: AWS EMEA SARL (UE) i Sophos Limited (Wielka Brytania - decyzja Komisji o odpowiednim stopniu ochrony); do usługi Sophos skaner przesyła wyłącznie skrót pliku - ciąg znaków obliczony z pliku, z którego nie da się odtworzyć jego treści; serwery Sophos przyjmujące skrót mogą być poza EOG

- Podmiot: Google Cloud Poland sp. z o.o., Warszawa (Google Workspace) - wyłącznie poczta kontakt@brifli.pl

Co robi z Danymi Spraw: korespondencja z Administratorem (polecenia, reklamacje); Dane Spraw nie są przyjmowane e-mailem, a otrzymane omyłkowo są usuwane (§ 7 ust. 2 Regulaminu)

Gdzie: bez wyboru regionu - możliwe przechowywanie w USA i innych państwach poza EOG

Przekazanie poza EOG i podstawa: USA: Google LLC deklaruje udział w programie EU-U.S. Data Privacy Framework (decyzja Komisji o odpowiednim stopniu ochrony, art. 45 RODO); inne państwa i na wypadek braku tej podstawy: standardowe klauzule ochrony danych w umowie Google (CDPA, art. 46 ust. 2 lit. c RODO)