Wersja: 1.0

Załącznik nr 1 do Regulaminu Aplikacji BROADCASTELLO

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Niniejsza umowa powierzenia przetwarzania danych osobowych (dalej: „Umowa Powierzenia" lub „Umowa") stanowi Załącznik nr 1 do Regulaminu Aplikacji BROADCASTELLO (dalej: „Regulamin") i jest zawierana pomiędzy:

Usługobiorcą w rozumieniu Regulaminu (dalej: „Administrator"),

a

Arturem Wilczkiem, prowadzącym działalność gospodarczą pod firmą AWFS Artur Wilczek (adres stałego miejsca wykonywania działalności gospodarczej: ul. Kopernika 6A, 43-190 Mikołów), wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, posiadającym NIP: 6511446527, numer REGON: 542878289 (dalej: „**Podmiot przetwarzający**"),

zwanymi dalej łącznie: „Stronami", a każdy z osobna: „Stroną".

Umowa Powierzenia zostaje zawarta z chwilą zawarcia umowy o dostarczanie Usługi na zasadach określonych w Regulaminie (dalej: „Umowa główna"), której wykonanie wymaga powierzenia Podmiotowi przetwarzającemu przetwarzania danych osobowych. Pojęcia pisane wielką literą, niezdefiniowane w Umowie Powierzenia, mają znaczenie nadane im w Regulaminie, z tym że ilekroć w Umowie Powierzenia jest mowa o „Umowie" – należy przez to rozumieć Umowę Powierzenia.

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w trybie art. 28 Rozporządzenia 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 (dalej: „Ogólne rozporządzenie o ochronie danych" lub „RODO").
2. Administrator oświadcza, że w rozumieniu przepisów RODO jest administratorem lub podmiotem przetwarzającym dane powierzane Podmiotowi przetwarzającemu na mocy Umowy Powierzenia. W przypadku, gdy dane osobowe powierzane Podmiotowi przetwarzającemu są danymi, w stosunku do których Administrator jest podmiotem przetwarzającym w rozumieniu przepisów RODO, niniejsza Umowa stanowi umowę podpowierzenia danych osobowych, a Podmiot przetwarzający jest na mocy jej postanowień podmiotem, wobec którego dokonuje się podpowierzenia.

3. Podmiot przetwarzający będzie przetwarzał powierzone mu dane osobowe wyłącznie na podstawie postanowień Umowy. Dopuszczalny zakres przetwarzania danych osobowych przez Podmiot przetwarzający, w szczególności:
   1) okres przetwarzania,
   2) charakter i cele przetwarzania,
   3) kategorie przetwarzanych danych osobowych,
   4) kategorie osób, których dane osobowe dotyczą,

   określa Załącznik nr 1 do Umowy.

§ 2
Przedmiot, charakter, cel i czas przetwarzania danych

1. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie na udokumentowane polecenie Administratora oraz wyłącznie w celu wykonywania Umowy głównej.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, przepisami RODO oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą. Strony potwierdzają, że niniejsza Umowa stanowi wydane przez Administratora polecenie przetwarzania danych osobowych na zasadach w niej określonych, w szczególności w zakresie wskazanym w Załączniku nr 1.
3. Udokumentowanymi poleceniami Administratora są także:
   1) czynności dokonywane przez Administratora lub Użytkowników w Aplikacji z wykorzystaniem jej funkcjonalności, w szczególności wprowadzanie, modyfikowanie i usuwanie Treści Usługobiorcy, tworzenie, modyfikowanie i usuwanie Kont Użytkowników, ustawienie okresu przechowywania wpisów dziennika zdarzeń Konta oraz parowanie i odłączanie Monitorów,
   2) polecenia przesłane przez Użytkownika posiadającego Rolę OWNER za pomocą poczty elektronicznej na adres: office@awfs.dev.
4. Podmiot przetwarzający realizuje polecenie, o którym mowa w ust. 3 pkt 2 powyżej, w terminie wskazanym przez Administratora, nie krótszym niż 7 dni, chyba że przepisy prawa wymagają niezwłocznej realizacji polecenia. Jeżeli realizacja polecenia wykracza poza funkcjonalności Aplikacji i wymagałaby jej zmiany, Podmiot przetwarzający niezwłocznie informuje o tym Administratora, a Strony uzgadniają sposób dalszego postępowania; w przypadku braku porozumienia Administrator może wypowiedzieć Umowę główną ze skutkiem natychmiastowym, a Podmiot przetwarzający zwraca Administratorowi część Opłaty Subskrypcyjnej odpowiadającą niewykorzystanej części opłaconego Okresu Subskrypcji, obliczoną proporcjonalnie do liczby dni pozostałych do jego zakończenia, w terminie 14 dni od dnia rozwiązania Umowy głównej.
5. Przedmiotem przetwarzania są dane osobowe przetwarzane w Koncie w związku ze świadczeniem Usługi, w zakresie określonym w Załączniku nr 1 do Umowy (dalej: „dane osobowe").
6. Administrator oświadcza i zobowiązuje się, że nie powierza Podmiotowi przetwarzającemu szczególnych kategorii danych osobowych ani danych dotyczących wyroków skazujących i czynów zabronionych, o których mowa odpowiednio w art. 9 i 10 RODO, w szczególności nie umieszcza ich w Treściach Usługobiorcy ani w Promptach.

7. Przetwarzanie powierzonych danych osobowych odbywa się wyłącznie przy wykorzystaniu systemów informatycznych (w sposób zautomatyzowany).

§ 3
Obowiązki, prawa i oświadczenia Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się do zabezpieczenia powierzonych danych osobowych poprzez wdrożenie, jeszcze przed przystąpieniem do przetwarzania, oraz utrzymywanie środków technicznych i organizacyjnych odpowiednich do charakteru, zakresu, kontekstu i celu przetwarzania, w tym środków wymaganych przez przepisy prawa powszechnie obowiązującego, by przetwarzanie spełniało wymogi RODO oraz innych przepisów. Środki stosowane przez Podmiot przetwarzający w dniu zawarcia Umowy opisuje Załącznik nr 3. Podmiot przetwarzający może zmieniać te środki, pod warunkiem zachowania co najmniej równoważnego poziomu bezpieczeństwa.
2. Podmiot przetwarzający zobowiązuje się zapewnić, aby osoby upoważnione do przetwarzania danych osobowych powierzonych na podstawie Umowy Powierzenia zobowiązane były do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Ponadto, Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały dane osobowe w celu realizacji niniejszej Umowy, zapoznania ich z obowiązkami wynikającymi z niniejszej Umowy oraz sprawowania kontroli nad ich realizacją.
3. Podmiot przetwarzający zobowiązany jest do prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych wymaganej przepisami o ochronie danych, w tym rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, o którym mowa w art. 30 ust. 2 RODO.
4. Podmiot przetwarzający zobowiązuje się, w zakresie uzasadnionym przedmiotem Umowy Powierzenia, w miarę możliwości, pomagać Administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO, w szczególności poprzez udostępnienie funkcjonalności Aplikacji umożliwiających dostęp do danych, ich sprostowanie i usunięcie, a także przygotowanie eksportu danych na zasadach określonych w § 10 ust. 4 Regulaminu.
5. Podmiot przetwarzający przetwarza dane osobowe w centrach danych zlokalizowanych na terytorium Europejskiego Obszaru Gospodarczego, wykorzystywanych przez podprocesorów wskazanych w Załączniku nr 2, a także – w zakresie niezbędnym do świadczenia Usługi, udzielania wsparcia i utrzymania Aplikacji – poprzez zdalny dostęp z miejsc wykonywania działalności Podmiotu przetwarzającego na terytorium Europejskiego Obszaru Gospodarczego. Przekazywanie danych osobowych do państw trzecich następuje wyłącznie na zasadach określonych w § 5 ust. 6.
6. Podmiot przetwarzający zobowiązuje się niezwłocznie zawiadomić Administratora o:
    1) każdym naruszeniu ochrony powierzonych danych osobowych, przy czym przez „naruszenie ochrony powierzonych danych" należy rozumieć w szczególności każde przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do powierzonych danych osobowych. Zawiadomienia, o którym mowa

w niniejszym punkcie, należy dokonać najpóźniej w ciągu 24 godzin od wykrycia naruszenia ochrony powierzonych danych;

2) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie, do czasu otrzymania opinii Administratora. Zawiadomienia, o którym mowa w niniejszym punkcie, należy dokonać najpóźniej w ciągu 24 godzin od otrzymania żądania;
3) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia;
4) przeprowadzeniu przez Prezesa Urzędu Ochrony Danych Osobowych lub inny organ nadzorczy kontroli zgodności przetwarzania danych osobowych i jej wynikach oraz o innych czynnościach organów władzy publicznej dotyczących tych danych.

7. Podmiot przetwarzający zobowiązuje się, w zakresie uzasadnionym przedmiotem Umowy Powierzenia i dostępnymi mu informacjami, pomagać Administratorowi w wywiązywaniu się przez niego z obowiązków wynikających z przepisów prawa powszechnie obowiązującego, w tym z art. 32-36 Ogólnego rozporządzenia o ochronie danych, i dotyczących bezpieczeństwa przetwarzania danych osobowych, zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu i osobie, której dane te dotyczą, oceny skutków dla ochrony danych i związanych z tą oceną konsultacji z organem nadzorczym.
8. Podmiot przetwarzający zobowiązuje się udostępniać Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwiać Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczyniać się do nich, na zasadach określonych w § 4.
9. Podmiot przetwarzający zobowiązuje się dostosować do zaleceń pokontrolnych Administratora, o których mowa w § 4 ust. 4 Umowy Powierzenia, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
10. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu danych osobowych.
11. W przypadku gdy zdaniem Podmiotu przetwarzającego, otrzymane przez niego instrukcje lub polecenia Administratora w sposób oczywisty naruszają powszechnie obowiązujące przepisy o ochronie danych osobowych, zobowiązany on jest niezwłocznie poinformować o tym Administratora.
12. Z tytułu zawarcia i wykonywania Umowy Powierzenia Podmiotowi przetwarzającemu nie przysługuje odrębne wynagrodzenie. Podmiot przetwarzający ponosi koszty przestrzegania obowiązków wynikających z Umowy oraz przepisów o ochronie danych, z zastrzeżeniem § 4 ust. 5.

§ 4
Obowiązki i prawa Administratora

1. Administrator ma prawo kontrolować zgodność przetwarzania powierzonych danych osobowych z Umową Powierzenia i RODO. Kontrola odbywa się w pierwszej kolejności poprzez żądanie informacji i dokumentów, w szczególności pisemnych wyjaśnień, odpowiedzi na kwestionariusze oraz

podsumowań wyników testów bezpieczeństwa. Podmiot przetwarzający udziela informacji i przekazuje dokumenty w terminie 14 dni od dnia otrzymania żądania.

2. Jeżeli informacje i dokumenty, o których mowa w ust. 1 powyżej, nie są wystarczające do wykazania zgodności przetwarzania z Umową Powierzenia, a także w przypadku naruszenia ochrony powierzonych danych osobowych lub żądania organu nadzorczego, Administrator może przeprowadzić audyt, w tym inspekcję, samodzielnie lub za pośrednictwem niezależnego audytora zobowiązanego do zachowania poufności. Audyt przeprowadza się po zawiadomieniu Podmiotu przetwarzającego z co najmniej 14-dniowym wyprzedzeniem (a w przypadku naruszenia ochrony powierzonych danych osobowych – z co najmniej 3-dniowym wyprzedzeniem), w Dni Robocze, w godzinach 9:00–17:00, nie częściej niż raz w roku kalendarzowym, z wyjątkiem audytu przeprowadzanego w związku z naruszeniem ochrony powierzonych danych osobowych lub na żądanie organu nadzorczego.
3. Audyt nie może obejmować dostępu do danych innych usługobiorców Podmiotu przetwarzającego ani do informacji stanowiących tajemnicę przedsiębiorstwa Podmiotu przetwarzającego w zakresie niezwiązanym z przetwarzaniem danych osobowych Administratora, ani zagrażać bezpieczeństwu Aplikacji. W odniesieniu do infrastruktury podprocesorów weryfikacja następuje na podstawie udostępnionych przez nich certyfikatów, raportów z audytów lub innych dokumentów.
4. Z przeprowadzonego audytu Administrator sporządza protokół w postaci elektronicznej, który przekazuje Podmiotowi przetwarzającemu. Podmiot przetwarzający może wnieść zastrzeżenia do protokołu w terminie 5 Dni Roboczych od dnia jego otrzymania. Zalecenia pokontrolne Podmiot przetwarzający wykonuje w terminie uzgodnionym przez Strony, nie krótszym niż 14 dni.
5. Koszty audytu, o którym mowa w ust. 2 powyżej, ponosi Administrator, chyba że audyt wykazał istotne naruszenie Umowy Powierzenia przez Podmiot przetwarzający.

§ 5
Dalsze powierzenie danych osobowych

1. Administrator udziela Podmiotowi przetwarzającemu ogólnej zgody na korzystanie z usług innych podmiotów przetwarzających (dalej: „podprocesorzy") w celu wykonania Umowy głównej. Wykaz podprocesorów, z których usług Podmiot przetwarzający korzysta w dniu zawarcia Umowy, stanowi Załącznik nr 2.
2. Podmiot przetwarzający korzysta wyłącznie z usług podprocesorów zapewniających wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, oraz nakłada na nich – w drodze umowy – te same obowiązki ochrony danych, jakie spoczywają na Podmiocie przetwarzającym na mocy Umowy Powierzenia.
3. Podmiot przetwarzający informuje Administratora o zamierzonych zmianach dotyczących dodania lub zastąpienia podprocesorów, za pomocą poczty elektronicznej na adres Użytkownika posiadającego Rolę OWNER lub komunikatu w Aplikacji, co najmniej 14 dni przed dniem wprowadzenia zmiany. Administrator może wyrazić sprzeciw wobec zmiany w terminie 14 dni od dnia otrzymania informacji, przesyłając go za pomocą poczty elektronicznej na adres office@awfs.dev, wraz ze wskazaniem przyczyn związanych z ochroną danych osobowych.

4. W przypadku zgłoszenia sprzeciwu Strony podejmą w dobrej wierze próbę uzgodnienia rozwiązania. Jeżeli Podmiot przetwarzający nie odstąpi od zmiany, Administrator może wypowiedzieć Umowę główną ze skutkiem natychmiastowym w terminie 30 dni od dnia otrzymania informacji, o której mowa w ust. 3 powyżej albo w ust. 5 poniżej. W takim przypadku Podmiot przetwarzający zwraca Administratorowi część Opłaty Subskrypcyjnej odpowiadającą niewykorzystanej części opłaconego Okresu Subskrypcji, obliczoną proporcjonalnie do liczby dni pozostałych do jego zakończenia, w terminie 14 dni od dnia rozwiązania Umowy głównej.
5. W przypadkach niecierpiących zwłoki, w szczególności w razie zagrożenia bezpieczeństwa danych lub nagłego zaprzestania świadczenia usług przez podprocesora, Podmiot przetwarzający może zastąpić podprocesora przed upływem terminu, o którym mowa w ust. 3 powyżej, informując o tym Administratora bez zbędnej zwłoki. Postanowienia ust. 3–4 powyżej stosuje się odpowiednio, przy czym termin na zgłoszenie sprzeciwu biegnie od dnia otrzymania informacji.
6. Administrator wyraża zgodę na przekazywanie danych osobowych do państw trzecich podprocesorom wskazanym w Załączniku nr 2, pod warunkiem zapewnienia przez Podmiot przetwarzający odpowiednich zabezpieczeń przewidzianych w rozdziale V RODO, w szczególności decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (w tym w ramach EU-US Data Privacy Framework – w odniesieniu do odbiorców uczestniczących w tym programie) albo standardowych klauzul umownych przyjętych przez Komisję Europejską. Inne przekazanie danych osobowych do państwa trzeciego może nastąpić wyłącznie na polecenie Administratora, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
7. Podmiot przetwarzający ponosi odpowiedzialność wobec Administratora za działania, zaniechania lub niewywiązanie się przez podprocesorów z obowiązków dotyczących ochrony danych osobowych jak za własne działania lub zaniechania, na zasadach określonych w § 9 ust. 3.

§ 6
Poufność

Strony zobowiązują się wykorzystać materiały, dane oraz wszelkie informacje pozyskane od drugiej Strony w celu wykonania Umowy Powierzenia wyłącznie do jej realizacji oraz zachować te materiały, dane oraz informacje w tajemnicy, zarówno w czasie trwania Umowy Powierzenia, jak i po jej rozwiązaniu.

§ 7
Czas obowiązywania Umowy i warunki wypowiedzenia

1. Umowa Powierzenia obowiązuje przez czas obowiązywania Umowy głównej, a po jej rozwiązaniu – do czasu usunięcia powierzonych danych osobowych zgodnie z § 8.
2. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający nie wykonuje lub w sposób nienależyty wykonuje postanowienia Umowy, w szczególności gdy:

1) pomimo wezwania nie usunie uchybień stwierdzonych podczas audytu w wyznaczonym terminie, nie krótszym niż 14 dni,
2) przetwarza dane osobowe w sposób niezgodny z Umową,
3) powierzył przetwarzanie danych osobowych innemu podmiotowi z naruszeniem § 5.

3. Mając na uwadze powiązanie niniejszej Umowy z Umową główną, Strony potwierdzają, że złożenie przez Administratora oświadczenia o rozwiązaniu niniejszej Umowy na podstawie ust. 2 powyżej jest równoznaczne ze złożeniem oświadczenia o rozwiązaniu Umowy głównej ze skutkiem natychmiastowym. W takim przypadku Podmiot przetwarzający zwraca Administratorowi część Opłaty Subskrypcyjnej odpowiadającą niewykorzystanej części opłaconego Okresu Subskrypcji, obliczoną proporcjonalnie do liczby dni pozostałych do jego zakończenia, w terminie 14 dni od dnia rozwiązania Umowy głównej.

§ 8
Skutki rozwiązania Umowy Powierzenia

1. Po rozwiązaniu Umowy głównej Podmiot przetwarzający udostępnia Administratorowi powierzone dane osobowe do pobrania na zasadach określonych w § 9 ust. 9 i § 10 Regulaminu, a następnie trwale usuwa powierzone dane osobowe, w tym ich kopie, w terminach określonych w § 9 ust. 9 albo § 10 ust. 6 Regulaminu, z zastrzeżeniem ust. 2–3 poniżej. Pobranie danych przez Administratora albo zaniechanie ich pobrania w tym okresie stanowi wybór Administratora w zakresie zwrotu lub usunięcia danych.
2. Dane osobowe zawarte w kopiach zapasowych są usuwane w zwykłym cyklu ich retencji – w przypadku kopii bazy danych w terminie do 14 dni, a w przypadku wcześniejszych wersji plików w terminie do 30 dni. Do czasu usunięcia dane te są zabezpieczone przed dostępem i nie są przetwarzane w innym celu niż odtworzenie systemu po awarii.
3. Obowiązek usunięcia danych osobowych nie dotyczy danych, których dalsze przechowywanie jest wymagane przez prawo Unii lub prawo państwa członkowskiego.
4. Na żądanie Administratora Podmiot przetwarzający potwierdza usunięcie powierzonych danych osobowych za pomocą poczty elektronicznej.

§ 9
Postanowienia końcowe

1. Postanowienia Umowy Powierzenia mają pierwszeństwo przed postanowieniami Regulaminu i Umowy głównej w sprawach dotyczących przetwarzania powierzonych danych osobowych.
2. Zmiany Umowy Powierzenia następują w trybie przewidzianym dla zmiany Regulaminu w § 23 Regulaminu, z wyjątkiem zmian Załącznika nr 2, które następują na zasadach określonych w § 5.
3. W sprawach nieuregulowanych w Umowie Powierzenia mają zastosowanie właściwe przepisy RODO, prawa polskiego oraz postanowienia Regulaminu, w tym – w relacjach między Stronami i z zastrzeżeniem bezwzględnie obowiązujących przepisów prawa – zasady odpowiedzialności określone w § 18 Regulaminu.
4. Załączniki nr 1–3 stanowią integralną część Umowy Powierzenia.

Załącznik nr 1 do Umowy Powierzenia – Zakres powierzenia

Element	Opis
Charakter przetwarzania	Przechowywanie, organizowanie, porządkowanie, przeglądanie, modyfikowanie, przesyłanie do Monitorów, wyświetlanie, przekazywanie Promptów dostawcom modeli sztucznej inteligencji w celu wygenerowania Materiałów AI, tworzenie kopii zapasowych, udostępnianie do eksportu oraz usuwanie danych – w sposób zautomatyzowany.
Cel przetwarzania	Świadczenie Usługi na rzecz Administratora zgodnie z Regulaminem, w tym zapewnienie dostępu Użytkowników do Konta, prowadzenie dziennika zdarzeń Konta, obsługa Monitorów, Funkcja AI, zapewnienie bezpieczeństwa i ciągłości działania Usługi oraz udzielanie wsparcia technicznego.
Okres przetwarzania	Czas obowiązywania Umowy głównej, a po jej rozwiązaniu – do czasu usunięcia danych zgodnie z § 8 Umowy Powierzenia.
Kategorie osób, których dane dotyczą	1) Użytkownicy – pracownicy, współpracownicy, zleceniobiorcy Administratora oraz inne osoby, którym Administrator udostępnił Konta Użytkowników; 2) osoby, których dane Administrator lub Użytkownicy umieszczają w Treściach Usługobiorcy (w szczególności pracownicy, współpracownicy, klienci, kontrahenci i goście Administratora); 3) osoby, których dotyczą wpisy dziennika zdarzeń Konta i zdarzenia parowania Monitorów.
Kategorie danych osobowych	1) dane Kont Użytkowników: imię i nazwisko, służbowy adres poczty elektronicznej, Rola, przynależność do grup Użytkowników, status Konta Użytkownika, dane uwierzytelniające (skrót kryptograficzny hasła, dane uwierzytelniania dwuskładnikowego), dane sesji; 2) dane dziennika zdarzeń Konta: identyfikator Użytkownika, adres IP, data i godzina, rodzaj i szczegóły zdarzenia, dozwolone adresy IP (jeżeli Administrator włączył ograniczenie dostępu według adresów IP); 3) dane parowania Monitorów: jednorazowy kod parowania, adres IP urządzenia, czas zgłoszenia i jego rozstrzygnięcia, identyfikator Użytkownika, który zatwierdził lub odrzucił parowanie; 4) dane osobowe zawarte w Treściach Usługobiorcy (Slajdach, Prezentacjach, Polach Dynamicznych, Promptach, Materiałach AI, zrzutach ekranu i adresach Slajdów URL), w szczególności imię i nazwisko, stanowisko, wizerunek oraz inne dane umieszczone przez Administratora lub Użytkowników – z wyłączeniem danych, o których mowa w art. 9 i 10 RODO.
Miejsce przetwarzania	Europejski Obszar Gospodarczy, z zastrzeżeniem przekazywania danych podprocesorom wskazanym w Załączniku nr 2 na zasadach § 5 ust. 6.

Załącznik nr 2 do Umowy Powierzenia – Wykaz podprocesorów

Podprocesor	Zakres i cel przetwarzania	Miejsce przetwarzania / podstawa przekazania
OVH SAS (OVHcloud), Francja	Hosting Aplikacji: serwery, baza danych, magazyn plików (Object Storage) wraz z wersjonowaniem	Warszawa, Polska (EOG)
Scaleway SAS, Francja	Zapasowa kopia plików (Object Storage) – zapewnienie ciągłości działania i odtworzenia danych po awarii	Amsterdam, Niderlandy (EOG)
Resend, Inc., Stany Zjednoczone	Doręczanie wiadomości poczty elektronicznej do Użytkowników (zaproszenia, linki aktywacyjne, resetowanie haseł, kody uwierzytelniania dwuskładnikowego, powiadomienia)	Stany Zjednoczone – decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony (EU-US Data Privacy Framework)
OpenRouter, Inc., Stany Zjednoczone	Pośrednictwo w przekazywaniu Promptów do dostawców modeli i generowaniu Materiałów AI (bez danych identyfikujących Użytkownika i Administratora)	Stany Zjednoczone – standardowe klauzule umowne przyjęte przez Komisję Europejską (umowa powierzenia OpenRouter, Inc.)
Google LLC, Stany Zjednoczone (modele Gemini, udostępniane za pośrednictwem OpenRouter, Inc.)	Generowanie Materiałów AI na podstawie Promptów (bez danych identyfikujących Użytkownika i Administratora)	Stany Zjednoczone – dalszy podmiot przetwarzający OpenRouter, Inc.; Google LLC uczestniczy w EU-US Data Privacy Framework

Załącznik nr 3 do Umowy Powierzenia – Środki techniczne i organizacyjne

Podmiot przetwarzający stosuje w szczególności następujące środki:

1. izolację danych poszczególnych Usługobiorców – dane jednego Usługobiorcy są niedostępne dla innych Usługobiorców, co jest weryfikowane automatycznymi testami izolacji danych,
2. szyfrowanie transmisji danych (HTTPS/TLS) wraz z wymuszaniem połączeń szyfrowanych (HSTS),
3. szyfrowanie danych w spoczynku na poziomie infrastruktury (szyfrowane wolumeny bazy danych, szyfrowanie po stronie serwera magazynu plików, szyfrowane kopie zapasowe),
4. przechowywanie haseł i Kluczy API wyłącznie w postaci skrótów kryptograficznych,
5. dobowe kopie zapasowe bazy danych przechowywane przez 14 dni oraz zapasową kopię plików u drugiego, niezależnego dostawcy na terytorium EOG, z wersjonowaniem (30 dni) i zabezpieczeniem kopii przed nadpisaniem i usunięciem,
6. nagłówki bezpieczeństwa HTTP zgodne z dobrymi praktykami (OWASP) oraz ograniczanie częstości żądań,
7. oczyszczanie danych wprowadzanych do Pól Dynamicznych (ochrona przed atakami XSS),
8. weryfikację rodzaju i zawartości plików wgrywanych do Aplikacji na podstawie ich zawartości, limity rozmiaru plików oraz ograniczenia zasobów przy ich przetwarzaniu,
9. minimalizację danych zwracanych przez interfejsy Aplikacji i zapisywanych w dzienniku zdarzeń – dane uwierzytelniające i inne wartości poufne nie opuszczają serwera,
10. dziennik zdarzeń Konta zapewniający rozliczalność operacji,
11. uwierzytelnianie dwuskładnikowe (domyślnie włączone dla nowych Kont) oraz możliwość ograniczenia dostępu do Konta według adresów IP,
12. natychmiastowe unieważnianie sesji wyłączonych lub usuniętych Kont Użytkowników,
13. parowanie Monitorów zatwierdzane przez uprawnionego Użytkownika, z odrębną, ograniczoną czasowo sesją urządzenia i natychmiastowym odcięciem urządzenia zastąpionego,
14. pseudonimizację danych przekazywanych dostawcom modeli sztucznej inteligencji oraz niezapisywanie treści Promptów w dzienniku zdarzeń,
15. okresowe testy bezpieczeństwa: testy penetracyjne interfejsów API, testy izolacji danych oraz automatyczne skanowanie kodu i zależności pod kątem podatności, wraz z dokumentowaniem ich wyników i usuwaniem wykrytych podatności,
16. ograniczenie dostępu do danych do osób upoważnionych, zobowiązanych do zachowania poufności.