

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Załącznik nr 1 do Regulaminu Serwisu DocuWatcher
zawarta zgodnie z art. 28 Rozporządzenia RODO

§ 1. Strony Umowy

Administrator danych: Usługobiorca korzystający z Serwisu DocuWatcher - Przedsiębiorca, który zaakceptował Regulamin i dokonał rejestracji Konta (dalej: „Administrator”).

Procesor danych: Paweł Grabowski, ul. Krzywa 1H, 44-362 Rogów, NIP: 6472592040 - podmiot prowadzący Serwis DocuWatcher (dalej: „Procesor”).

Strony zawierają niniejszą Umowę Powierzenia Przetwarzania Danych (dalej: „UPPD” lub „Umowa”) z chwilą założenia Konta w Serwisie DocuWatcher poprzez akceptację Regulaminu wraz z niniejszą Umową stanowiącą jego Załącznik nr 1, co jest równoznaczne z akceptacją warunków niniejszej Umowy.

§ 2. Przedmiot i cel Umowy

Niniejsza Umowa określa zasady przetwarzania przez Procesora danych osobowych, których Administratorem jest Usługobiorca, w związku ze świadczeniem usług drogą elektroniczną za pośrednictwem Serwisu DocuWatcher.

Procesor przetwarza dane osobowe wyłącznie w celu świadczenia usług określonych w Regulaminie, w szczególności: analizy treści dokumentów (OCR), przechowywania dokumentów w cyfrowym archiwum, monitorowania terminów ważności oraz wysyłania powiadomień.

Przetwarzanie danych przez Procesora następuje wyłącznie na udokumentowane polecenie Administratora, którym jest w szczególności wgranie dokumentu do Systemu DocuWatcher.

§ 3. Zakres i charakter przetwarzanych danych

Kategorie osób, których dane dotyczą: pracownicy i współpracownicy Administratora, kontrahenci, kierowcy, operatorzy maszyn oraz inne osoby, których dane zawarte są w dokumentach wgrywanych przez Administratora do Systemu.

Kategorie danych osobowych: dane identyfikacyjne (imię, nazwisko, PESEL, numer dokumentu tożsamości), dane kontaktowe (adres, e-mail, telefon), dane zawodowe (stanowisko, uprawnienia, certyfikaty, wyniki badań lekarskich, daty szkoleń), dane pojazdów i maszyn (nr rejestracyjny, numer VIN) oraz inne dane zawarte w wgrywanych dokumentach.

Charakter przetwarzania: gromadzenie, utrwalanie, organizowanie, przechowywanie, przeglądanie, wykorzystywanie (analiza OCR), udostępnianie uprawnionym użytkownikom Administratora, usuwanie.

Czas trwania przetwarzania: przez okres obowiązywania Umowy, a po jej zakończeniu - do czasu usunięcia danych przez Administratora lub upływu 30 dni od rozwiązania umowy (po tym czasie dane są trwale usuwane).

§ 4. Obowiązki Procesora

Procesor zobowiązuje się do:

- a. przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora i w celach określonych w niniejszej Umowie - chyba że obowiązek taki nakłada na Procesora prawo Unii Europejskiej lub prawo państwa członkowskiego;

- b. zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- c. zastosowania środków bezpieczeństwa wymaganych na mocy art. 32 RODO, w tym w szczególności: szyfrowania danych w transmisji (TLS/HTTPS) i w spoczynku, regularnych kopii zapasowych, kontroli dostępu, izolacji danych klientów;
- d. przestrzegania warunków korzystania z usług podprocesorów, o których mowa w § 6 niniejszej Umowy;
- e. pomocy Administratorowi - w miarę możliwości - poprzez odpowiednie środki techniczne i organizacyjne w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą;
- f. pomocy Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32–36 RODO (bezpieczeństwo przetwarzania, zgłaszanie naruszeń, ocena skutków);
- g. po zakończeniu świadczenia usług - trwałego usunięcia wszystkich danych osobowych lub ich zwrotu Administratorowi, według wyboru Administratora, i usunięcia istniejących kopii, chyba że prawo UE lub państwa członkowskiego nakazuje przechowywanie danych;
- h. udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w niniejszej Umowie oraz umożliwienia przeprowadzania audytów i inspekcji.

§ 5. Obowiązki Administratora

Administrator zobowiązuje się do:

- i. wgrywania do Systemu wyłącznie tych dokumentów, do przetwarzania których posiada odpowiednią podstawę prawną w rozumieniu art. 6 lub art. 9 RODO;
- j. poinformowania osób, których dane zawarte są w wgrywanych dokumentach, o fakcie przetwarzania ich danych przez DocuWatcher jako procesora - w zakresie wymaganym przez art. 13 lub 14 RODO;
- k. niezwłocznego informowania Procesora o wszelkich okolicznościach mogących wpłynąć na spełnienie wymogów RODO w związku z korzystaniem z Serwisu;
- l. realizowania praw osób, których dane dotyczą, w tym żądań usunięcia danych z Systemu poprzez narzędzia dostępne w Koncie Usługobiorcy.

§ 6. Podprocesory

Administrator niniejszym wyraża ogólną zgodę na korzystanie przez Procesora z usług podprocesorów wymienionych w poniższej tabeli.

Podprocesor	Cel przetwarzania	Lokalizacja danych	Podstawa prawna	Status RODO
Railway Inc.	Hosting infrastruktury aplikacji, bazy danych, serwer backendowy	EU West – Amsterdam (europe-west4)	DPA Railway (railway.com/legal/dpa)	DPA dostępne
SMSAPI (LINK Mobility Poland Sp. z o.o.)	Wysyłanie powiadomień SMS o terminach ważności dokumentów	Polska / EOG	DPA dostępne; polska spółka	EOG, DPA dostępne
Google LLC (Vertex AI / Gemini)	Analiza OCR dokumentów, rozpoznawanie treści i dat	Warszawa, PL (europe-central 2)	Cloud Data Processing Addendum (CDPA)	Dane w EOG, nie służą do trenowania AI

Podprocesor	Cel przetwarzania	Lokalizacja danych	Podstawa prawna	Status RODO
Google LLC (Firebase Auth + Firestore)	Uwierzytelnianie użytkowników, baza danych czasu rzeczywistego	EOG (region konfigurowalny)	Firebase Data Processing & Security Terms + CDPA	DPA objęte warunkom i Google
Google LLC (Firebase Storage)	Przechowywanie plików dokumentów wgranych przez użytkowników	USA – US-EAST-1 (Karolina Północna)	Standard Contractual Clauses (SCC) zatwierdzone przez KE (art. 46 ust. 2 lit. c RODO) w ramach Firebase/Google Cloud DPA	Transfer do USA pokryty SCC
Postmark (ActiveCampaign Postmark)	Wysyłanie e-maili transakcyjnych (powiadomienia, reset hasła)	USA - serwery AWS Chicago	DPA z SCC (postmarkapp.com/dpa)	Serwery USA - pokryte SCC
Stripe, Inc.	Obsługa płatności kartą, subskrypcji i fakturowania (bramka płatnicza)	USA - serwery AWS; dane kart tokenizowane w EOG (Stripe Ireland Ltd.)	Stripe Data Processing Agreement (stripe.com/legal/dpa); SCC dla transferów do USA	DPA dostępne; dane kart w EOG przez Stripe Ireland
Fakturownia Sp. z o.o.	Generowanie i przechowywanie faktur VAT	Polska	UPPD zawarta przez akceptację regulaminu Fakturowni	Polska spółka, UPPD w regulaminie

W związku z korzystaniem z usług Firebase Storage firmy Google LLC, której serwery dla tej usługi zlokalizowane są w USA (region US-EAST-1), transfer danych osobowych poza Europejski Obszar Gospodarczy odbywa się na podstawie Standardowych Klauzul Umownych (SCC) zatwierdzonych przez Komisję Europejską decyzją z dnia 4 czerwca 2021 r. (art. 46 ust. 2 lit. c RODO), zawartych w ramach Firebase Data Processing and Security Terms oraz Google Cloud Data Processing Addendum. Dokumenty dostępne są pod adresem: firebase.google.com/terms/data-processing-terms.

Procesor poinformuje Administratora o planowanym dodaniu lub zastąpieniu podprocesora z co najmniej 14-dniowym wyprzedzeniem poprzez opublikowanie informacji w Serwisie lub przesłanie powiadomienia na adres e-mail przypisany do Konta. Administrator ma prawo wyrazić sprzeciw wobec zmian w terminie 14 dni od powiadomienia.

§ 7. Bezpieczeństwo przetwarzania (art. 32 RODO)

Procesor wdraża następujące środki techniczne i organizacyjne:

- m. szyfrowanie danych w transmisji (TLS 1.2+, HTTPS) i w spoczynku;
- n. izolacja danych - każdy Administrator ma dostęp wyłącznie do swoich danych;
- o. uwierzytelnianie - dostęp do danych wyłącznie po uwierzytelnieniu hasłem; zalecane uwierzytelnianie dwuskładnikowe;
- p. kontrola dostępu - dostęp do danych po stronie Procesora mają wyłącznie upoważnieni pracownicy i podwykonawcy;

- q. regularne kopie zapasowe danych (backup);
- r. monitoring bezpieczeństwa i reagowanie na incydenty;
- s. serwery infrastruktury głównej zlokalizowane na terenie Unii Europejskiej; pliki dokumentów przechowywane w Firebase Storage (Google LLC) na serwerach w USA na podstawie SCC - patrz § 6.

§ 8. Naruszenia ochrony danych

Procesor zobowiązuje się do niezwłocznego poinformowania Administratora o każdym naruszeniu ochrony danych osobowych dotyczącym danych przetwarzanych na jego polecenie - nie później niż w ciągu 36 godzin od wykrycia naruszenia.

Powiadomienie będzie zawierać: opis charakteru naruszenia, kategorie i przybliżoną liczbę osób i rekordów danych, możliwe konsekwencje, zastosowane lub proponowane środki zaradcze.

Powiadomienie nastąpi na adres e-mail powiązany z Kontem Administratora. Administrator odpowiada za terminowe zgłoszenie naruszenia do UODO (art. 33 RODO) w terminie 72 godzin od powzięcia informacji.

§ 9. Prawa osób, których dane dotyczą

W przypadku otrzymania przez Procesora żądania bezpośrednio od osoby, której dane dotyczą, Procesor niezwłocznie przekazuje to żądanie Administratorowi. Procesor nie jest upoważniony do samodzielnego odpowiadania na takie żądania.

Administrator realizuje prawa osób, których dane dotyczą (dostęp, sprostowanie, usunięcie, ograniczenie, przeniesienie) poprzez narzędzia dostępne w Koncie Usługobiorcy lub kontakt z Procesorem na adres kontakt@docuwatcher.com.

§ 10. Audyt i inspekcja

Administrator ma prawo do przeprowadzenia audytu zgodności przetwarzania danych z niniejszą Umową i RODO, nie częściej niż raz w roku kalendarzowym.

Audyt przeprowadzany jest po uprzednim pisemnym powiadomieniu Procesora z co najmniej 14-dniowym wyprzedzeniem. Procesor udostępni Administratorowi lub upoważnionemu przez niego audytorowi niezbędne informacje i dokumentację.

Koszty audytu ponosi Administrator, chyba że audyt ujawni naruszenia ze strony Procesora - w takim przypadku koszty ponosi Procesor.

§ 11. Odpowiedzialność

Procesor ponosi odpowiedzialność za szkody spowodowane przetwarzaniem, jeżeli nie wywiązał się z obowiązków RODO skierowanych bezpośrednio do procesorów lub działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew nim (art. 82 ust. 2 RODO).

Administrator ponosi odpowiedzialność za prawidłowość podstawy prawnej przetwarzania danych zawartych w wgrzanych dokumentach oraz za treść tych dokumentów.

Odpowiedzialność Procesora z tytułu niniejszej Umowy ograniczona jest do wysokości opłat abonamentowych uiszczonych przez Administratora w ciągu 12 miesięcy poprzedzających zdarzenie wywołujące szkodę, chyba że szkoda wynika z umyślnego działania lub rażącego niedbalstwa Procesora.

§ 12. Czas trwania i rozwiązanie Umowy

Niniejsza Umowa obowiązuje przez czas korzystania z Serwisu DocuWatcher, począwszy od chwili rejestracji Konta.

Umowa wygasa automatycznie z chwilą usunięcia Konta przez Administratora.

Po wygaśnięciu Umowy Procesor trwale usuwa wszystkie dane osobowe Administratora w terminie 30 dni, chyba że Administrator złoży wniosek o eksport danych przed upływem tego terminu.

§ 13. Postanowienia końcowe

Niniejsza Umowa stanowi Załącznik nr 1 do Regulaminu Serwisu DocuWatcher i podlega prawu polskiemu.

W sprawach nieuregulowanych niniejszą Umową zastosowanie mają przepisy RODO oraz powszechnie obowiązującego prawa polskiego.

Wszelkie zmiany niniejszej Umowy dokonywane będą w trybie i na zasadach określonych w Regulaminie (powiadomienie z 14-dniowym wyprzedzeniem).

Sądem właściwym do rozstrzygania sporów wynikających z niniejszej Umowy jest sąd powszechny właściwy dla siedziby Procesora.