

Umowa powierzenia przetwarzania danych osobowych

Zawierana zawsze, gdy w ramach obsługi informatycznej albo wdrożenia automatyzacji uzyskuję dostęp do danych osobowych, którymi administruje Twoja firma. Podstawa: art. 28 RODO. Umowa jest jawna, leży na stronie i nie trzeba o nią prosić mailem.

ADMINISTRATOR

NIP _____ · reprezentowany przez _____

PODMIOT PRZETWARZAJĄCY

SYSTEMBOX Sergiusz Siemak, Białystok
NIP 966-211-49-48 · kontakt@systembox.pl

Zawarta _____ w Białymstoku, jako załącznik do umowy głównej z dnia _____

§ 1. PRZEDMIOT, CHARAKTER I CEL PRZETWARZANIA

- Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i celu opisanym w **Załączniku nr 1**, wyłącznie w celu wykonania umowy głównej.
- Przetwarzanie obejmuje czynności niezbędne do świadczenia usług informatycznych: dostęp zdalny i lokalny do stacji roboczych i serwerów, administrowanie kontami poczty i uprawnieniami, nadzór nad kopiami zapasowymi, diagnostykę i usuwanie awarii oraz budowę i utrzymanie automatyzacji.
- Umowa obowiązuje przez czas trwania umowy głównej i wygasa razem z nią.
- Podmiot przetwarzający przetwarza dane wyłącznie na udokumentowane polecenie Administratora, którym jest także sama umowa główna i zgłoszenia serwisowe. Jeżeli obowiązek przetwarzania wynika z prawa Unii lub prawa polskiego, Podmiot przetwarzający informuje o tym Administratora przed przetwarzaniem, chyba że prawo tego zakazuje.

§ 2. OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO

- Dopuszcza do danych wyłącznie osoby z pisemnym upoważnieniem, zobowiązane do zachowania poufności. Lista osób jest prowadzona i udostępniana Administratorowi na żądanie.
- Stosuje środki techniczne i organizacyjne odpowiadające ryzyku (art. 32 RODO), w szczególności: szyfrowanie nośników i połączeń zdalnych, uwierzytelnianie wieloskładnikowe do kont uprzywilejowanych, zasadę najmniejszych uprawnień, rozdzielenie kont administracyjnych od roboczych, rejestrowanieostępów oraz kopie zapasowe z okresowym testem odtworzenia.
- Pomaga Administratorowi w realizacji żądań osób, których dane dotyczą (rozdział III RODO), oraz w wypełnieniu obowiązków z art. 32–36 RODO, w zakresie, w jakim to możliwe z uwagi na charakter przetwarzania.
- Zgłasza Administratorowi każde naruszenie ochrony danych **bez zbędnej zwłoki, nie później niż w ciągu 24 godzin** od jego stwierdzenia, przekazując opis naruszenia, kategorie i przybliżoną liczbę osób i rekordów, prawdopodobne konsekwencje oraz podjęte i proponowane środki zaradcze.
- Po zakończeniu świadczenia usług, zgodnie z decyzją Administratora, **usuwa albo zwraca** wszystkie dane oraz usuwa istniejące kopie, chyba że prawo nakazuje ich przechowanie. Termin: 30 dni od zakończenia umowy głównej. Na żądanie wystawia oświadczenie o usunięciu.
- Udostępnia Administratorowi informacje niezbędne do wykazania spełnienia obowiązków z art. 28 RODO i umożliwia audyty, w tym inspekcje, prowadzone przez Administratora lub upoważnionego audytora, po uzgodnieniu terminu z wyprzedzeniem co najmniej 14 dni, nie częściej niż raz w roku kalendarzowym, chyba że audyt jest następstwem naruszenia.
- Niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane polecenie narusza RODO lub inne przepisy o ochronie danych.
- Prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratora (art. 30 ust. 2 RODO).

§ 3. DALSZE POWIERZENIE

- Administrator udziela **ogólnej zgody** na korzystanie z dalszych podmiotów przetwarzających wymienionych w **Załączniku nr 2**.
- O zamiarze dodania lub zastąpienia dalszego podmiotu Podmiot przetwarzający informuje Administratora z wyprzedzeniem co najmniej 14 dni. Administrator może w tym czasie wnieść uzasadniony sprzeciw; jeżeli strony nie uzgodnią rozwiązania, Administrator może wypowiedzieć umowę główną bez zachowania okresu wypowiedzenia.
- Na dalsze podmioty nakładane są te same obowiązki ochrony danych co w niniejszej umowie. Za ich działania i zaniechania Podmiot przetwarzający odpowiada wobec Administratora jak za własne.

§ 4. PRZEKAZYWANIE POZA EUROPEJSKI OBSZAR GOSPODARCZY

Domyślnie dane nie są przekazywane poza EOG: infrastruktura jest utrzymywana w Polsce lub w Unii Europejskiej. Jeżeli konkretna usługa wymaga wyjątku, jest on wskazany w Załączniku nr 2 razem z podstawą transferu (standardowe klauzule umowne Komisji Europejskiej lub decyzja o adekwatności) i wymaga wcześniejszej pisemnej zgody Administratora.

§ 5. ODPOWIEDZIALNOŚĆ I POSTANOWIENIA KOŃCOWE

- Każda ze stron odpowiada za szkody wyrządzone przetwarzaniem na zasadach art. 82 RODO.
- Zmiany umowy wymagają formy pisemnej albo dokumentowej (skan podpisanego dokumentu) pod rygorem nieważności.
- W sprawach nieuregulowanych stosuje się RODO, ustawę o ochronie danych osobowych i Kodeks cywilny. Spory rozstrzyga sąd właściwy dla siedziby Administratora.
- Umowę sporządzono w dwóch jednobrzmiących egzemplarzach albo podpisano elektronicznie; każda forma jest równoważna.

ADMINISTRATOR · DATA I PODPIS

PODMIOT PRZETWARZAJĄCY · DATA I PODPIS

Załącznik nr 1. Zakres powierzenia

Wypełniany przy podpisaniu. Puste wiersze skreśla się, żeby nie powierzać więcej, niż trzeba.

KATEGORIA OSÓB	RODZAJ DANYCH	CZY POWIERZONE
Pracownicy i współpracownicy Administratora	Imię i nazwisko, służbowy adres e-mail, login, numer telefonu, stanowisko, dane logowania do systemów firmowych	tak / nie
Klienci i kontrahenci Administratora	Dane w bazach, na dyskach i w poczcie, do których wgląd jest technicznie możliwy przy diagnostyce i administrowaniu	tak / nie
Osoby kontaktujące się z Administratorem	Dane w skrzynkach pocztowych, formularzach i systemie zgłoszeń	tak / nie
Inne (wpisać)		tak / nie

Szczególne kategorie danych (art. 9 RODO) oraz dane o wyrokach (art. 10 RODO): domyślnie nie są powierzane. Jeżeli w systemach Administratora takie dane występują (np. dane o zdrowiu w gabinecie, dane kadrowe o niepełnosprawności), wymaga to wyraźnego wskazania poniżej i osobnych środków ochrony uzgodnionych przed rozpoczęciem prac.

SYSTEMY OBJĘTE POWIERZENIEM

Lista spisywana w ciągu pierwszych 30 dni współpracy i aktualizowana przy każdej zmianie infrastruktury. Poza listą nie ma powierzenia i nie ma dostępu.

Załącznik nr 2. Dalsze podmioty przetwarzające

Lista jest jawna i aktualna na dzień podpisania. Zmiana wymaga zawiadomienia z 14-dniowym wyprzedzeniem.

PODMIOT	ROLA	LOKALIZACJA PRZETWARZANIA	PODSTAWA TRANSFERU POZA EOG
	Hosting infrastruktury	Polska / UE	nie dotyczy
	Poczta i pakiet biurowy		
	Kopie zapasowe		
	Narzędzie zdalnego dostępu		

Wiersze wypełniane są nazwami konkretnych dostawców faktycznie użytych w Twoim środowisku, a nie listą wszystkiego, z czego kiedykolwiek korzystam. Jeżeli w trakcie współpracy dochodzi nowy dostawca, dostajesz zawiadomienie, zanim zaczniesz przetwarzać dane.

ADMINISTRATOR · DATA I PODPIS

PODMIOT PRZETWARZAJĄCY · DATA I PODPIS