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

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i celu opisanym w **Załączniku nr 1**, wyłącznie w celu wykonania umowy głównej.
2. 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.
3. Umowa obowiązuje przez czas trwania umowy głównej i wygasa razem z nią.
4. 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

1. Dopuszcza do danych wyłącznie osoby z pisemnym upoważnieniem, zobowiązane do zachowania poufności. Lista osób jest prowadzona i udostępniana Administratorowi na żądanie.
2. 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, rejestrowanie dostępów oraz kopie zapasowe z okresowym testem odtworzenia.
3. 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.
4. 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.
5. 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. Podmiot przetwarzający może zachować wyłącznie dane niezbędne do ustalenia, dochodzenia lub obrony roszczeń oraz do wykazania zgodności z prawem (art. 17 ust. 3 lit. e RODO): logi dostępów, korespondencję i dokumentację zgłoszeń, przez okres przedawnienia roszczeń z umowy głównej, wyłącznie w tym celu.
6. 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. Koszt własnej obsługi pierwszego audytu w roku ponosi Podmiot przetwarzający; każdy kolejny audyt oraz pomoc wykraczająca poza czynności z ust. 3 i 4 są rozliczane według stawki godzinowej z umowy głównej, po uprzednim podaniu szacunku.
7. Niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane polecenie narusza RODO lub inne przepisy o ochronie danych, i **może wstrzymać jego wykonanie** do czasu wyjaśnienia. Wstrzymanie z tej przyczyny nie jest niewykonaniem umowy głównej i nie rodzi odpowiedzialności Podmiotu przetwarzającego za wynikłe z niego opóźnienie.
8. Prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratora (art. 30 ust. 2 RODO).

§ 3. OBOWIĄZKI I OŚWIADCZENIA ADMINISTRATORA

1. Administrator oświadcza, że jest uprawniony do powierzenia danych objętych **Załącznikiem nr 1** i że ich przetwarzanie w celu wskazanym w § 1 ma podstawę prawną, a wobec osób, których dane dotyczą, spełniono obowiązek informacyjny.
2. Administrator wydaje wyłącznie polecenia zgodne z prawem i odpowiada za ich treść. Jeżeli osoba trzecia albo organ nadzorczy zgłosi roszczenie wynikające z niezgodnego z prawem polecenia albo z braku podstawy prawnej po stronie Administratora, Administrator przejmuje jego obronę i pokrywa uzasadnione koszty Podmiotu przetwarzającego.
3. Administrator udostępnia dane w zakresie **minimalnym**, potrzebnym do wykonania umowy głównej. W szczególności dane testowe przekazywane do prac programistycznych powinny być zanonimizowane wszędzie tam, gdzie nie przeszkadza to w testach.
4. Administrator niezwłocznie informuje o zmianie zakresu powierzenia, o zmianie osób upoważnionych do wydawania poleceń oraz o każdym naruszeniu ochrony danych stwierdzonym po swojej stronie.
5. Naruszenie ochrony danych, którego przyczyną jest działanie Administratora, jego pracownika albo systemu pozostającego poza zakresem umowy głównej, nie jest naruszeniem obowiązków Podmiotu przetwarzającego.
6. Strony nie są współadministratorami w rozumieniu art. 26 RODO: celów i sposobów przetwarzania nie ustalają wspólnie. Dane kontaktowe przedstawicieli Administratora, potrzebne do wykonania i rozliczenia umowy głównej, Podmiot przetwarzający przetwarza **jako administrator** we własnym interesie (art. 6 ust. 1 lit. b i f RODO) i nie są one objęte powierzeniem.

§ 4. DALSZE POWIERZENIE

1. Administrator udziela **ogólnej zgody** na korzystanie z dalszych podmiotów przetwarzających wymienionych w **Załączniku nr 2**.
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.
3. 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.

§ 5. 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.

§ 6. ODPOWIEDZIALNOŚĆ I POSTANOWIENIA KOŃCOWE

1. Każda ze stron odpowiada za szkody wyrządzone przetwarzaniem na zasadach art. 82 RODO. W zakresie, w jakim prawo na to pozwala, odpowiedzialność Podmiotu przetwarzającego wobec Administratora z tytułu niniejszej umowy podlega ograniczeniom przewidzianym w umowie głównej. Ograniczenia nie dotyczą szkody wyrządzonej umyślnie ani odpowiedzialności wobec osób, których dane dotyczą, ani administracyjnych kar pieniężnych nałożonych na stronę odpowiedzialną za naruszenie.
2. Zmiany umowy wymagają formy pisemnej albo dokumentowej (skan podpisanego dokumentu) pod rygorem nieważności.
3. W sprawach nieuregulowanych stosuje się RODO, ustawę o ochronie danych osobowych i Kodeks cywilny. Spory rozstrzyga sąd właściwy dla siedziby Administratora.
4. 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 zacznie przetwarzać dane.

_____ _____

ADMINISTRATOR · DATA I PODPIS PODMIOT PRZETWARZAJĄCY · DATA I PODPIS

Wzór, nie porada prawna. Ostateczna treść ustalana indywidualnie.