ALDERHALL / WZÓR ROBOCZY

Umowa powierzenia przetwarzania danych osobowych - wzór

Wersja: 0.9

Data: 31 lipca 2026 r.

Status: do przeglądu osoby odpowiedzialnej za ochronę danych

Dokument wymaga uzupełnienia pól i końcowego przeglądu przed użyciem produkcyjnym.

> Załącznik stosuje się tylko wtedy, gdy ARSIMO/ALDERHALL przetwarza dane osobowe w imieniu Klienta. Nie zastępuje analizy ról dla każdego procesu.

§ 1. Strony i związek z umową główną

Umowa zostaje zawarta pomiędzy:

[pełna firma Klienta], **[dane]**, dalej „Administrator”,

a

ARSIMO sp. z o.o., ul. Augustyna Szamarzewskiego 21/2, 60-514 Poznań, KRS **[KRS]**, NIP **[NIP]**, operatorem marki ALDERHALL, dalej „Podmiot Przetwarzający”.

1. Powierzenie jest związane z Umową Ramową z dnia **[data]** i zaakceptowanymi Zleceniami („Umowa Główna”).
2. W razie rozbieżności w sprawach ochrony danych pierwszeństwo ma niniejsza Umowa.
3. Pojęcia mają znaczenie nadane w RODO.

§ 2. Przedmiot i czas

1. Administrator powierza dane wyłącznie w zakresie niezbędnym do kwalifikacji, realizacji, dokumentowania i zamknięcia Zleceń wskazanych w Załączniku A.
2. Przetwarzanie trwa od udostępnienia danych do ich zwrotu/usunięcia po zakończeniu Umowy Głównej lub Zlecenia, z uwzględnieniem retencji i kopii bezpieczeństwa.
3. Podmiot Przetwarzający nie staje się właścicielem danych ani nie może używać ich dla własnego marketingu, profili, portfolio lub trenowania modeli.

§ 3. Udokumentowane polecenia

1. Podmiot Przetwarzający działa wyłącznie na udokumentowane polecenie Administratora, także przy transferze danych poza EOG.
2. Polecenia mogą wynikać z Umowy Głównej, Karty Zlecenia, Panelu lub wiadomości osoby uprawnionej.
3. Jeżeli polecenie zdaniem Podmiotu Przetwarzającego narusza RODO lub inne prawo ochrony danych, informuje on Administratora i wstrzymuje wykonanie w zakresie ryzyka, o ile prawo nie zabrania.
4. Jeżeli prawo nakazuje przetwarzanie niezależnie od polecenia, Podmiot Przetwarzający informuje Administratora przed rozpoczęciem, chyba że prawo zabrania takiej informacji.

§ 4. Osoby upoważnione i poufność

1. Dostęp mają wyłącznie osoby upoważnione według potrzeby.
2. Osoby są związane poufnością ustawową, umowną lub pracowniczą i przeszkolone w zakresie powierzonych czynności.
3. Podmiot Przetwarzający prowadzi rejestr upoważnień i niezwłocznie odbiera dostęp po zmianie roli lub zakończeniu współpracy.

§ 5. Środki techniczne i organizacyjne

1. Podmiot Przetwarzający wdraża środki adekwatne do ryzyka, opisane w Załączniku B.
2. Minimum obejmuje:

- indywidualne konta i zakaz współdzielenia haseł;
- MFA dla systemów, które je obsługują;
- menedżer haseł lub bezpieczny kanał przekazania tajemnic;
- kontrolę dostępu według roli i potrzeby;
- szyfrowanie transmisji i urządzeń/nośników, gdzie jest zasadne;
- aktualizacje, ochronę urządzeń i blokadę ekranu;
- kopie bezpieczeństwa oraz test odtworzenia dla systemów krytycznych;
- oddzielenie katalogów i projektów klientów;
- rejestr dostępu administracyjnego i zmian wysokiego ryzyka;
- procedurę incydentu, zakończenia i odebrania dostępu.

3. Podmiot Przetwarzający może zmieniać środki na równoważne lub silniejsze, o ile nie obniża uzgodnionego poziomu bezpieczeństwa.
4. Dla szczególnie wrażliwego Zlecenia Strony mogą uruchomić Tryb Sejf, ograniczający zewnętrzne narzędzia i zakres dostępu.

§ 6. Podprocesorzy

1. Administrator udziela **[ogólnej / szczegółowej]** zgody na dalsze powierzenie podmiotom wskazanym w Załączniku C.
2. Przy zgodzie ogólnej Podmiot Przetwarzający informuje o planowanej zmianie co najmniej **[14] dni** wcześniej, umożliwiając uzasadniony sprzeciw.
3. Umowa z podprocesorem nakłada co najmniej te same obowiązki ochrony danych.
4. Podmiot Przetwarzający pozostaje wobec Administratora odpowiedzialny za wykonanie obowiązków podprocesora w zakresie wymaganym RODO.
5. Sprzeciw może spowodować zmianę narzędzia, ograniczenie Zlecenia albo rozwiązanie części usługi, jeżeli brak równoważnej alternatywy.

§ 7. Transfery poza EOG

1. Dane nie są przekazywane poza EOG bez udokumentowanego polecenia i właściwego mechanizmu prawnego.
2. Podmiot Przetwarzający przekazuje informacje o lokalizacji i mechanizmie transferu dla używanych podprocesorów.
3. Jeżeli narzędzie generatywne lub chmurowe mogłoby powodować transfer, jego użycie wymaga wcześniejszej oceny i zgodności z Załącznikiem C.

§ 8. Prawa osób

1. Podmiot Przetwarzający, uwzględniając charakter przetwarzania, pomaga Administratorowi obsługiwać żądania osób.
2. Żądanie otrzymane bezpośrednio przekazuje Administratorowi bez zbędnej zwłoki, nie później niż w **[2] dni robocze**, i nie odpowiada merytorycznie bez polecenia, chyba że prawo wymaga inaczej.
3. Koszt niestandardowej pomocy wykraczającej poza zwykły zakres jest wcześniej uzgadniany, z wyjątkiem działań wymaganych z powodu naruszenia po stronie Podmiotu Przetwarzającego.

§ 9. Pomoc w obowiązkach Administratora

Podmiot Przetwarzający w rozsądnym zakresie pomaga w:

- bezpieczeństwie przetwarzania;
- analizie ryzyka i ocenie skutków DPIA;
- konsultacji z organem nadzorczym;
- rejestrze kategorii czynności;
- ustaleniu faktów incydentu;
- realizacji obowiązku zawiadomienia UODO i osób;
- wykazaniu zgodności dla zakresu usług ALDERHALL.

§ 10. Naruszenia ochrony danych

1. Podmiot Przetwarzający zgłasza Administratorowi stwierdzone naruszenie bez zbędnej zwłoki, docelowo nie później niż **24 godziny** od potwierdzenia, że dotyczy powierzonych danych.
2. Pierwsze zgłoszenie zawiera dostępne informacje:

- charakter i przybliżony zakres;
- kategorie danych i osób;
- czas wykrycia i prawdopodobny czas zdarzenia;
- możliwe konsekwencje;
- podjęte i planowane działania;
- osobę kontaktową;
- informacje jeszcze nieznane i plan ich ustalenia.

3. Brak pełnych danych nie opóźnia zgłoszenia; informacje są uzupełniane etapami.
4. Podmiot Przetwarzający zabezpiecza dowody, ogranicza skutek i współpracuje przy analizie.
5. Komunikację z UODO i osobami prowadzi Administrator, chyba że udzieli odrębnego upoważnienia.

§ 11. Audyt i informacje

1. Podmiot Przetwarzający udostępnia informacje potrzebne do wykazania zgodności w zakresie usług.
2. Administrator może przeprowadzić audyt nie częściej niż raz w roku, z co najmniej 14-dniowym wyprzedzeniem, w sposób nienaruszający bezpieczeństwa innych klientów.
3. Ograniczenie częstotliwości nie dotyczy uzasadnionego incydentu, żądania organu ani istotnego podejrzenia naruszenia.

4. W pierwszej kolejności wykorzystuje się dokumenty, ankietę, certyfikaty i zdalne dowody. Audyt na miejscu wymaga uzgodnienia zakresu i poufności audytora.
5. Koszt zwykłego audytu ponosi Administrator; koszt usunięcia niezgodności i dodatkowej weryfikacji wynikającej z naruszenia Podmiotu Przetwarzającego ponosi Podmiot Przetwarzający.

§ 12. Zwrot, usunięcie i retencja

1. Po zakończeniu Administrator wybiera zwrot albo usunięcie danych, o ile prawo nie wymaga przechowania.
2. Dane robocze są zwracane/usuwane w terminie **[14] dni**, a dostęp jest odbierany niezwłocznie.
3. Kopie bezpieczeństwa są nadpisywane w zwykłym cyklu nie dłuższym niż **[90] dni** i do tego czasu pozostają chronione oraz nieużywane do innych celów.
4. Podmiot Przetwarzający może zachować minimum danych potrzebne do obrony roszczeń lub obowiązków prawnych jako odrębny administrator, informując o podstawie i retencji.
5. Na żądanie potwierdza zakończenie i wskazuje wyjątki.

§ 13. Odpowiedzialność

1. Odpowiedzialność Stron wynika z RODO, prawa krajowego i Umowy Głównej.
2. Ograniczenia odpowiedzialności z Umowy Głównej stosuje się w zakresie dopuszczalnym prawem i nie ograniczają praw osób ani kompetencji organu.
3. Podmiot Przetwarzający ponosi koszty działań naprawczych w zakresie, w jakim incydent wynika z jego zawinionego naruszenia.

§ 14. Czas i zakończenie

1. Umowa obowiązuje przez okres powierzonego przetwarzania.
2. Istotne naruszenie uprawnia Administratora do wstrzymania przekazywania danych, żądania naprawy i rozwiązania zakresu, którego nie można bezpiecznie kontynuować.
3. Poufność, audyt incydentu, odpowiedzialność i retencja obowiązują także po zakończeniu w zakresie koniecznym.

§ 15. Postanowienia końcowe

1. Do Umowy stosuje się prawo polskie i RODO.
2. Zmiany wymagają formy dokumentowej, z wyjątkiem przypadków wymagających formy szczególnej.
3. Spory podlegają zasadom Umowy Głównej.

Podpisy

ADMINISTRATOR / KLIENT Imię i nazwisko: _____ Data i podpis: _____

PODMIOT PRZETWARZAJĄCY / ARSIMO sp. z o.o. Imię i nazwisko: Kasandra Nikola Kamińska-Tatara Funkcja: Prezes Zarządu Data i podpis: _____

Załącznik A - Opis przetwarzania

Pole	Uzupełnienie
Przedmiot	[np. obsługa zgłoszeń, przygotowanie dokumentów, utrzymanie formularza]
Czas	[okres]
Charakter operacji	[zbieranie, przeglądanie, porządkowanie, zapisywanie, udostępnianie według polecenia, usuwanie]
Cel	[konkretny cel Zlecenia]
Kategorie osób	[klienci, pracownicy, kandydaci, dostawcy, użytkownicy strony, osoby kontaktowe]
Kategorie danych	[identyfikacyjne, kontaktowe, zatrudnienie, rozliczeniowe, korespondencja, dostęp techniczny]
Dane szczególne / karne	[nie / tak - jakie i dlaczego]
Systemy i lokalizacje	[lista]
Osoby uprawnione do poleceń	[lista]
Retencja	[okres i podstawa]

Załącznik B - Środki bezpieczeństwa

Tożsamość i dostęp

- indywidualne konta;
- MFA dla administratorów i systemów kluczowych;
- role i zasada najmniejszych uprawnień;
- kwartalny przegląd dostępów lub częściej przy zmianie zespołu;
- natychmiastowe odebranie dostępu po zakończeniu.

Urządzenia i transmisja

- blokada urządzenia i szyfrowanie dysku, gdzie dostępne;
- aktualizacje systemu i aplikacji;
- ochrona antymalware odpowiednia do ryzyka;

- TLS dla transmisji;
- zakaz przechowywania na prywatnych nośnikach bez zgody.

Hasła i tajemnice

- menedżer haseł;
- brak haseł w zwykłym e-mailu i w treści Zlecenia;
- odrębne konta zamiast wspólnych loginów;
- rotacja po incydencie i odebraniu dostępu.

Pliki, kopie i ciągłość

- oddzielne katalogi klientów;
- kopie według krytyczności;
- test odtworzenia;
- kontrola eksportów i udostępnień;
- rejestr zmian wysokiego ryzyka.

Organizacja

- NDA/upoważnienia personelu;
- szkolenie i procedura incydentu;
- checklista rozpoczęcia i zakończenia klienta;
- ocena podprocesorów;
- polityka AI i Tryb Sejf;
- zasada dwóch osób przy czynnościach wysokiego ryzyka, gdy jest możliwa.

Załącznik C - Podprocesorzy

Podmiot	Usługa	Lokalizacja danych	Mechanizm transferu	Kategorie danych	Data zgody/informacji
[dostawca]	[hosting/poczta/panel/backup]	[EOG/inne]	[nie dotyczy/SCC/inny]	[zakres]	[data]

Nota: Przed podpisaniem należy uzupełnić rzeczywistą listę dostawców, lokalizacje danych, transfery, cykle kopii i kontakt incydentowy. Nie wolno pozostawić Załącznika C jako pustej deklaracji, jeżeli produkcyjnie używane są podprocesory.