

Załącznik nr 5 do SWZ

(Wzór) Umowa powierzenia przetwarzania danych osobowych

Nr/2026

zawarta dnia _____ pomiędzy:

(zwana dalej „Umową”)

_____ (*dane podmiotu przetwarzającego)

zwany w dalszej części umowy „**Podmiotem przetwarzającym**”

reprezentowana przez:

oraz

_____ (*dane podmiotu Administratora)

zwany w dalszej części umowy „**Administratorem danych**” lub „**Administratorem**”

reprezentowana przez:

§ 1**Powierzenie przetwarzania danych osobowych**

1. Administrator danych osobowych (dalej Administrator i/lub ADO) powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

§2**Zakres i cel przetwarzania danych**

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (*należy podać kategorie danych) np. dane zwykłe oraz dane szczególnych

*kategorii (*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.*

2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu (*należy podać cel przetwarzania Administratora, który ma realizować podmiot przetwarzający) np. prowadzenie spraw związanych z zatrudnieniem, obsługa monitoringu wizyjnego, obsługa rachunkowo-księgowa i finansowa.
3. Przedmiotem przetwarzania są dane osobowe objęte przedmiotem i celem Umowy Głównej.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia. Zakres wymagań minimalnych opisano w Załączniku nr 1 do niniejszej umowy powierzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je administratorowi do 24 godzin od wykrycia zdarzenia.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego. Zawiadomienie o planowanej kontroli Administrator przekaze pisemnie z 7 dniowym wyprzedzeniem. Jeżeli Podmiot przetwarzający popełnił naruszenie danych osobowych Administrator ma prawo realizować prawo do kontroli niezwłocznie. W tym przypadku Podmiot przetwarzający winien się poddać kontroli w ciągu 12 godzin od chwili zaistnienia naruszenia.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
4. Jeżeli termin usunięcia uchybień, wskazany w §4 ust. 3 z przyczyn obiektywnych, wskazanych przez Podmiot przetwarzający nie może zostać dotrzymany, Administrator może uzgodnić inny termin ich usunięcia. W przypadku wydłużenia terminu Podmiot przetwarzający zobowiązany jest do skutecznego usunięcia uchybień przy zastosowaniu środków tymczasowych.
5. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający powierzonych danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych

kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas, zgodnie z czasem realizacji Umowy Głównej.

§8

Rozwiązanie umowy

1. Rozwiązanie Umowy Głównej / zakończenie wykonywania kategorii przetwarzania dokonywanych w imieniu Administratora, stanowiących przedmiot przetwarzania niniejszej umowy, określony w § 2, powoduje rozwiązanie niniejszej umowy.
2. Rozwiązanie niniejszej umowy, z zastrzeżeniem okoliczności, o których mowa w ust. 1, ust. 3, ust. 4, wymaga zachowania 1 miesięcznego okresu wypowiedzenia, którego koniec przypada na ostatni dzień miesiąca następującego po miesiącu, w którym wypowiedzenie zostało skutecznie doręczone drugiej Stronie. Wypowiedzenie nie wymaga podania uzasadnienia, ale wymaga zachowania formy pisemnej pod rygorem nieważności.
3. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia, o którym mowa w ust. 2, w przypadku:
 - a. rażącego, udokumentowanego naruszenia przez Podmiot Przetwarzający postanowień niniejszej umowy,
 - b. wyrządzenia przez Podmiot Przetwarzający, w związku z realizacją niniejszej umowy, szkody Administratorowi,
 - c. zaistnieniu po stronie Podmiotu Przetwarzającego okoliczności uniemożliwiających dalsze, zgodne z umową i z przepisami prawa, przetwarzanie poleconych i powierzonych danych osobowych,
 - d. zaistnieniu po stronie Administratora okoliczności uniemożliwiających dalsze, zgodne z umową i z przepisami prawa polecanie i powierzanie przetwarzania danych osobowych.
4. Podmiot Przetwarzający może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia, o którym mowa w ust. 2, w przypadku:
 - a. rażącego, udokumentowanego naruszenia przez Administratora postanowień niniejszej umowy,
 - b. wyrządzenia przez Administratora, w związku z realizacją niniejszej umowy, szkody Podmiotowi przetwarzającemu,
 - c. zaistnieniu po stronie Podmiotu Przetwarzającego okoliczności uniemożliwiających dalsze, zgodne z umową i z przepisami prawa, przetwarzanie w imieniu Administratora poleconych mu danych osobowych,
 - d. zaistnieniu po stronie Administratora okoliczności uniemożliwiających dalsze, zgodne z umową i z przepisami prawa polecanie przetwarzania danych osobowych.

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Przed przystąpieniem do realizacji Umowy Głównej Podmiot przetwarzający składa oświadczenie zgodne z Załącznikiem nr 1. Za pobranie oświadczenia odpowiada osoba odpowiedzialna za realizację Umowy Głównej.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

Administrator danych

Podmiot przetwarzający

Załącznik nr 1 do Umowy powierzenia danych osobowych

Lista minimalnych środków organizacyjnych i technicznych w celu zachowania bezpieczeństwa danych osobowych przez Podmiot przetwarzający.

Legenda:

Zagadnienia – opis sposobu realizacji wdrożonych środków ochrony organizacyjnej oraz technicznej w zakresie przetwarzania danych osobowych,

Spełnia/Nie spełnia – informacja o tym czy organizacja spełnia czy nie spełnia opisu z kolumny Zagadnienia,

Uwagi – informacja dodatkowa, jeśli wydaje się wskazana. Może być również pytanie o ile wyda się zasadne,

ADO – Administrator Danych Osobowych, który powierza podmiotowi przetwarzającemu dane osobowe,

PP – podmiot przetwarzający, któremu ADO powierza dane osobowe do przetwarzania.

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
1.	Dane osobowe przetwarzane w ramach zawartej umowy (umów) są ograniczone przez PP do niezbędnych i proporcjonalnych w zakresie celu świadczenia usług.		
2.	Podmiot przetwarzający wie czym są/jest: dane osobowe, szczególne kategorie danych, naruszenie danych osobowych, Pseudonimizacja, minimalizacja, poufność, integralność danych osobowych.		
3.	Podmiot przetwarzający stosuje zasadę minimalizacji danych osobowych, zasadę najniższego przywileju (ang. least privilege) oraz zasadę wiedzy niezbędnej (uzasadnionej) (ang. need to know) w zakresie dostępu do danych powierzonych przez ADO.		
4.	PP prowadzi rejestr informacji dot. ujawniania danych na rzecz osób trzecich, w tym informacje na temat ujawnionych informacji osobowych.		
5.	PP nadaje upoważnienia własnym pracownikom do przetwarzania danych osobowych.		
6.	PP reguluje z podmiotami przetwarzającymi (również w ramach umów powierzenia-podpowierzenia)		

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
	dane zwrot, przekazanie i usuwanie powierzonych danych osobowych.		
7.	Dokumentacja dotycząca obszaru bezpieczeństwa obowiązująca w organizacji PP jest stale aktualizowana oraz wersjonowana w celu zachowania historii zmian.		
8.	W organizacji PP drukowanie na papier danych osobowych jest ograniczone do minimum.		
9.	PP zdefiniował procedury związane z przywracaniem danych z wykonywanej kopii bezpieczeństwa.		
10.	PP posiada wdrożoną politykę retencji danych, przez co należy rozumieć, że wie ile czasu może przetwarzać określone informacje.		
11.	Pliki oraz dokumenty wytwarzane w celu realizacji przedmiotu Umowy są składowane w repozytorium szyfrowanym, a informacje nadmiarowe lub tymczasowe są trwale usuwane zgodnie z opisanym sposobem zarządzania danymi dostępnymi w formie elektronicznej.		
12.	Transmisja danych osobowych odbywa się z użyciem protokołów gwarantujących szyfrowanie np: SSL, TLS, IPSec, Radius, SSH.		
13.	Dane osobowe składowane na przenośnych nośnikach danych i/lub przesyłane pocztą elektroniczną są szyfrowane w sposób bezpieczny, który oznacza zastosowanie algorytmu co najmniej XTS-AES-128.		
14.	PP ograniczył do minimum możliwość przesyłania danych osobowych pocztą elektroniczną, zapisywania w chmurze lub kopiowania danych na nośniki przenośne.		
15.	Jeżeli PP wykorzystuje chmurę do przetwarzania danych robi to z pełną wiedzą i świadomością, posiadając przy		

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
	tym właściwą wiedzę organizacyjną i techniczną do zarządzania chmurą.		
16.	PP precyzyjnie wie jaki zakres danych przetwarza w chmurze.		
17.	PP precyzyjnie wie jaki zakres danych przetwarza w zarządzanych przez niego środowiskach teleinformatycznych.		
18.	Dane osobowe przesyłane przez publiczne sieci transmisji danych są szyfrowane przed transmisją np.: archiwum zip + hasło.		
19.	Wydrukowane dokumenty papierowe są niszczone z użyciem niszczarek.		
20.	Każdy pracownik PP posiada indywidualny login i hasło logowania do systemu operacyjnego oraz do aplikacji dziedzinowych, w których przetwarzane są dane osobowe PP. Login i hasło służą do poprawnej realizacji procesu autoryzacji oraz potwierdzania tożsamości użytkownika/pracownika organizacji.		
21.	Autoryzacja użytkowników zachodzi w oparciu o centralną bazę zarządzaną przez PP np.: LDAP, Microsoft Active Directory lub inną.		
22.	Wszędzie gdzie jest to możliwe PP stosuje funkcję wieloskładnikowego uwierzytelniania (MFA) albo przynajmniej dwuskładnikowego uwierzytelniania (2FA).		
23.	PP posiada wdrożoną politykę zarządzania kontami pracowników przetwarzających dane osobowe Administratora, która gwarantuje zachowanie poufności oraz higieny w zakresie sprawnego regulowania (nadawania, odbierania, zmiany) uprawnień do danych osobowych.		
24.	PP utrzymuje przynajmniej przez 12 miesięcy historię logowania użytkowników należących do niego systemów operacyjnych oraz aplikacji dziedzinowych w celu umożliwienia		

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
	odtworzenia historii dostępu do danych osobowych.		
25.	W przypadku wygaśnięcia konta użytkownika nie jest ono przekazywane innemu użytkownikowi.		
26.	PP przetwarza powierzone dane osobowe w znanej lokalizacji na terenie Unii Europejskiej oraz posiada informacje umożliwiające identyfikację podmiotów, które są dostawcami infrastruktury oraz oprogramowania umożliwiającego przetwarzanie danych.		
27.	PP weryfikuje rzeczywiste i rejestruje po weryfikacji, możliwości organizacyjne i techniczne dla podmiotów, którym podpowierza dane ADO.		
28.	PP nie podpowierza danych innemu PP bez wiedzy i zgody ADO.		
29.	PP nie rzadziej niż dwa razy w roku prowadzi szkolenia dla personelu mające na celu podniesienie wiedzy i świadomości w zakresie przetwarzania danych osobowych oraz bezpieczeństwa informacji w tym cyberbezpieczeństwa.		
30.	PP wdrożył oprogramowanie antywirusowe na każdej stacji roboczej oraz na każdym serwerze. Wdrożone oprogramowanie charakteryzuje się stabilnością działania, wysoką skutecznością oraz posiada aktualne bazy sygnatur wirusów.		
31.	PP na bieżąco (bez zbędnej zwłoki) aktualizuje posiadane systemy operacyjne oraz aplikacje dziedzinowe w celu eliminowania podatności na ataki i zapewnienia stabilności pracy.		
32.	PP nie wykorzystuje systemów operacyjnych oraz aplikacji nieposiadających bieżącego i aktywnego wsparcia ich producentów np: Windows XP, Vista, 7, 8, 8.1.		
33.	PP posiada aktualną politykę dostępu do pomieszczeń oraz zawartości szaf, szuflad oraz innych elementów		

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
	wyposażenia umożliwiających przetwarzanie danych osobowych.		
34.	W przypadku przetwarzania danych osobowych na papierze PP posiada miejsca ich składowania zamykane na klucz (pokoje, szafy, biurka), w którym składowane są dane osobowe.		
35.	PP posiada zidentyfikowane strefy przetwarzania danych szczególnych.		
36.	PP sprawuje stały nadzór nad personelem sprząającym. Personel sprząający przechodzi szkolenia z zakresu bezpieczeństwa danych osobowych oraz wie jak postępować podczas powierzonych mu czynności w zakresie bezpieczeństwa informacji.		
37.	PP posiada wdrożone procedury oraz narzędzie gwarantujące zachowanie ciągłości działania.		
38.	PP posiada wdrożone procedury i narzędzie gwarantujące ochronę danych osobowych przed przypadkowym zniszczeniem.		
39.	Dane osobowe oraz inne informacje przetwarzane na komputerach użytkowników są szyfrowane w całości z użyciem algorytmu co najmniej AES-256.		
40.	Dane osobowe oraz inne informacje przetwarzane na serwerach są szyfrowane w całości z użyciem algorytmu co najmniej AES-256.		
41.	Dane osobowe oraz inne informacje przetwarzane na urządzenia do składowania kopii zapasowych są szyfrowane w całości z użyciem algorytmu co najmniej AES-256.		
42.	Dane osobowe oraz inne informacje przetwarzane na smartfonach są w całości szyfrowane (stosowane jest pełne szyfrowanie zawartości każdego smartfona) z użyciem algorytmu co najmniej AES-256.		

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
43.	Smartfony/tablety na których przetwarzane są dane osobowe są chronione przed nieautoryzowanym dostępem poprzez użyciem kodu pin lub rysowanego znaku na ekranie lub odcisku palca.		
44.	Smartfony/tablety na których przetwarzane są dane osobowe są chronione przed nieautoryzowanym dostępem poprzez użycie przynajmniej jednej z metod: <ul style="list-style-type: none"> • sześciocyfrowego kodu pin, • sześciopunktowego wzoru rysowanego na ekranie, • odcisku palca osoby wykorzystującej urządzenie, • rozpoznawania twarzy osoby wykorzystującej urządzenie. 		
45.	PP nie dopuszcza do użytkowania prywatnych smartfonów/tabletów do realizacji celów służbowych bez pisemnego upoważnienia oraz weryfikacji minimalnych środków ochrony technicznej i organizacyjnej zabezpieczeń stosowanych przez ich właściciela.		
46.	PP nie dopuszcza do użytkowania prywatnych komputerów do realizacji celów służbowych bez pisemnego upoważnienia oraz weryfikacji minimalnych środków ochrony technicznej i organizacyjnej zabezpieczeń stosowanych przez ich właściciela.		
47.	PP nie dopuszcza do instalowania dowolnego oprogramowania na smartfonach/tabletach.		
48.	PP nie dopuszcza do instalowania dowolnego oprogramowania na komputerach, służących do przetwarzania danych.		
49.	PP przekazuje wszystkim osobom listę wymagań w zakresie stosowania		

L.p.	Zagadnienie	Spełnia/Nie spełnia	Uwagi
	środków organizacyjnych i technicznych w celu bezpiecznego przetwarzania danych osobowych.		
50.	Poczty elektroniczna wykorzystywana przez PP znajduje się na serwerach działających w obszarze Unii Europejskiej (dotyczy również adresów poczty elektronicznej w przypadku podpowierzenia albo BYOD).		
51.	PP nie wykorzystuje do przetwarzania danych osobowych Administratora narzędzi opartych o sztuczną inteligencję (AI)?		
52.	PP nie wykorzystuje AI do wykonywania innych zadań np.: w codziennej pracy?		