

Umowa powierzenia przetwarzania danych osobowych

Wzór uwzględnia wytyczne EROD w zakresie uregulowania powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(zwana dalej „Umową”)

_____ [dane podmiotu, który zawiera Umowę]

zwanym(-ną) w dalszej części Umowy „Podmiotem przetwarzającym”, reprezentowanym(-ną) przez:

a

_____ [dane podmiotu, który zawiera Umowę], zwanym(-ną) w dalszej części Umowy „Administratorem danych” lub „Administratorem”, reprezentowanym(-ną) przez:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz.UE.L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem”), na zasadach, w zakresie i w celu określonych w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy dane [należy podać rodzaj danych, tj. tzw. dane zwykłe oraz dane szczególnych kategorii] dotyczące[należy podać kategorię osób, których dane dotyczą, np. pracowników administratora, klientów administratora itd.] w zakresie [należy podać kategorie danych osobowych, np. imiona i nazwiska, adresy zamieszkania, numery PESEL itd.].
2. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu [należy podać cel przetwarzania danych przez Podmiot przetwarzający, np. realizacji umowy z dnia nr w zakresie prowadzenia spraw kadrowych].
3. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie [należy wybrać właściwe] – które są w minimalnym zakresie niezbędne do realizacji celu, o którym mowa w ust. 2 powyżej.

§ 3

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z Rozporządzeniem, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Lista środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający stanowi załącznik nr 1 do Umowy.
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 osobowe, przy czym będą to jedynie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegali odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby, o których mowa w niniejszym ustępie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
5. Dla prawidłowej realizacji ust. 4 Podmiot Przetwarzający dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie 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 Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 Rozporządzenia. Podmiot przetwarzający – w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora w terminie 5 dni roboczych od otrzymania wiadomości [Administrator termin może określić dowolnie, z zastrzeżeniem terminowej realizacji zadań wynikających z Rozporządzenia]. Udzielając informacji, Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.
8. W przypadku stwierdzenia jakiegokolwiek naruszenia ochrony danych osobowych Podmiot przetwarzający lub podwykonawca Podmiotu przetwarzającego zgłasza je Administratorowi w ciągu [można wskazać np. w ciągu 24 h].

§ 4

Prawo kontroli

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo kontroli, mającej na celu weryfikację, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych będzie realizować prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum uprzedzeniem [należy wpisać, z ilu dniowym wyprzedzeniem Administrator informuje o kontroli].
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd

do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni *[Administrator termin może określić dowolnie]*.
5. Powyżej określone zasady kontroli Podmiotu Przetwarzającego mają zastosowanie do przeprowadzanych przez Administratora kontroli podwykonawców Podmiotu przetwarzającego, o których mowa w § 6 ust. 1 Umowy.

§ 5

Raportowanie

1. Na wniosek Administratora Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z Rozporządzenia.
2. Informacji, o których mowa w ust. 1, udziela się w terminie 15 dni roboczych *[Administrator termin może określić dowolnie, z zastrzeżeniem terminowej realizacji zadań wynikających z Rozporządzenia]* od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

§ 6

Dalsze powierzenie danych do przetwarzania

1. Administrator wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania przez podwykonawców Podmiotu przetwarzającego, w celu wykonania niniejszej Umowy, przy czym podwykonawcy Podmiotu przetwarzającego powinni spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający niniejszą Umową. Lista takich podmiotów (podprocesorów) stanowi załącznik nr 2 do Umowy.
2. W przypadku zmiany lub dodania innych podwykonawców biorących udział w przetwarzaniu danych powierzonych przez Administratora Podmiot przetwarzający informuje o zamierzonych zmianach, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian w terminie 5 dni roboczych od przekazania informacji o zamierzonych zmianach *[Administrator termin może określić dowolnie]*.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora danych, chyba że taki obowiązek nakłada na Podmiot przetwarzający prawo Unii Europejskiej 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.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązywanie się z obowiązków spoczywających na podwykonawcy, wynikających z niniejszej Umowy.

§ 7

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących 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, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 8

Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony od do* [należy wybrać].
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem okresu wypowiedzenia [należy wskazać okres wypowiedzenia].

§ 9

Rozwiązanie Umowy

1. Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
 - a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
 - b) przetwarza dane osobowe w sposób niezgodny z Umową,
 - c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 10

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, a także danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku z 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.

§ 11

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

Załączniki:

1. załącznik nr 1 – Wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający;
2. załącznik nr 2 – Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów).

Załącznik nr 1

Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający

PYTANIE	ODPOWIEDŹ
Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy?	
Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia?	
Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	
Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?	
Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji?	
Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany?	
Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?	
Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian hasel oraz zmian w razie zaistniałej potrzeby?	

Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób?	
Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	
Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka?	
Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamkniętych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	
Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach?	
Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane?	
Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych?	
Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu?	
Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych?	
Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe?	
Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych?	
Gdzie są przechowywane kopie zapasowe?	
Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania?	
Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design?	
Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default?	
Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?	
Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	

Załącznik nr 2

Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów)

Przy wykonaniu Umowy Procesor korzysta z usług następujących podprocesorów:

PODPROCESOR	ADRES SIEDZIBY

Informacje do powyższej umowy od IODO – p. J. Olejniczak

Forwarded message -----

Od: **jolejniczak jolejniczak** <jolejniczak@cuwpo.wloclawek.pl>

Date: pt., 9 lip 2021 o 10:50

Subject: informacja dla Dyrektorów

DECYZJA WYKONAWCZA KOMISJI (UE) 2021/915

z dnia 4 czerwca 2021 r.

w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725

Umowę powierzenia należy stosować do umów zleceń z podmiotami z zewnątrz (np. serwis informatyczny, wzór umowy umieszczony jest na stronie UODO, wzór przesyłam również w załączniku. Proszę stosować się do Decyzji z dnia 4 czerwca 2021 r. Umowę stosujemy wraz z załącznikami. Poniżej przedstawiam niektóre przykłady stosowania umów powierzenia:

Kiedy stosować umowę powierzenia?

Powierzenie przetwarzania danych osobowych będzie miało miejsce w sytuacji, gdy podmiot zewnętrzny świadczy pewien rodzaj usług na rzecz administratora, z którymi związane jest przetwarzanie danych osobowych. Istota powierzenia przetwarzania danych osobowych jest ściśle powiązana z pojęciem outsourcingu, przez które należy rozumieć zlecenie podmiotowi zewnętrznemu (wyspecjalizowanemu w określonej dziedzinie), realizacji czynności związanych z funkcjonowaniem administratora. Można zatem wymienić następujące przykłady sytuacji, w których co do zasady zobowiązani będziemy do zawarcia umowy powierzenia:

1. zewnętrzna obsługa w zakresie Inspektora Ochrony Danych,
2. zewnętrzna obsługa księgową przedsiębiorstwa,
3. zewnętrzna obsługa kadrowo – płacowa przedsiębiorstwa,
4. korzystanie z usług zewnętrznego archiwum,
5. zewnętrzne usługi niszczenia dokumentów,
6. prowadzenie kampanii marketingowych przez podmiot zewnętrzny na zbiorze danych przekazanych przez administratora lub budowanych na zlecenie administratora (np. mailing do klientów administratora),
7. świadczenie przez podmiot zewnętrznych usług IT (np. hosting),
8. usługi zewnętrznego call center,
9. świadczenie usług ochrony obiektów w tym ich monitorowania przez podmiot zewnętrzny,
10. usługi introligatorskie.