

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu [wpisać datę] r. (zwana dalej „Umową”) pomiędzy:

Centrum Andrzej Ryszard Szope, ul. Poznańska 14/23, 00 – 680 Warszawa, reprezentowaną przez.....(zwanym dalej Administratorem)

a

[wpisać dane przetwarzającego] (zwanym dalej **Podmiotem przetwarzającym**)

§ 1 Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ust. 3 Rozporządzenia 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 (zwanym dalej Rozporządzeniem).
2. Administrator oświadcza, że jest Administratorem powierzanych danych osobowych w rozumieniu przepisów Rozporządzenia oraz, że powierzane dane zgromadził zgodnie z obowiązującymi przepisami prawa z uwzględnieniem obowiązku informacyjnego o którym mowa w art. 13 i 14 Rozporządzenia.
3. Zasady i cele przetwarzania określa niniejsza Umowa, która nie narusza obowiązków wynikających z Rozporządzenia.
4. Niniejszej Umowy nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w Rozporządzeniu, ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.
5. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa właścicieli powierzanych danych.

§2 Zakres i cel przetwarzania danych

1. Kategorie osób, których dane osobowe Administrator powierza Podmiotowi przetwarzającemu do przetwarzania oraz zakres tych danych określono w **załączniku nr 1** do niniejszej Umowy.
2. *Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy głównej (umowy o świadczenie usług) nr.....z dnia.....[wpisać identyfikator umowy o świadczenie usług] r., chyba, że otrzyma on dalsze wyraźne polecenie Administratora.*

§3 Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne

polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.

2. Podmiot przetwarzający bezzwłocznie powiadamia Administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez Administratora narusza zapisy Rozporządzenia lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.
3. Podmiot przetwarzający zobowiązuje się zgodnie z wymaganiami Rozporządzenia:
 - a. do stosowania środków organizacyjnych i technicznych spełniających wymogi Rozporządzenia oraz chroniących prawa osób, których dane są powierzane do przetwarzania. Minimalny zakres zabezpieczeń wymieniono w załączniku nr 2 do niniejszej Umowy. Stosowane środki zapewniają ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą,
 - b. dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych,
 - c. do poinformowania Administratora przed rozpoczęciem przetwarzania danych o realizacji ewentualnego obowiązku prawnego polegającego na przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej (art. 28 ust. 3. lit. a Rozporządzenia).
4. Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), Podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, lub po rozwiązaniu umowy, zwraca Administratorowi wszystkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że przepisy powszechnie obowiązującego prawa Unii lub prawa krajowego nakazują przechowywanie tych danych osobowych.
6. Podmiot przetwarzający udostępnia Administratorowi, na jego uzasadnione żądanie, wszelkie informacje niezbędne do wykazania spełnienia przez Administratora obowiązków wynikających z art. 28 Rozporządzenia.
7. Podmiot przetwarzający, w miarę możliwości i w niezbędnym zakresie, pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia. Przy czym niezwłocznie zawiadamia Administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie ma prawa do udzielenia odpowiedzi na taki wniosek samodzielnie, chyba, że Administrator wyraził na to zgodę.

8. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych w jego zasobach:
 - a. niezwłocznie, jednak nie później niż w ciągu 48 h od stwierdzenia naruszenia, informuje Administratora o tym fakcie i podaje wszelkie znane informacje dotyczące naruszenia,
 - b. ustala przyczynę naruszenia lub wskazuje czynności podjęte w celu ustalenia tej przyczyny,
 - c. podejmuje wszelkie czynności mające na celu ograniczenie skutków naruszenia, usunięcie naruszenia oraz zabezpieczenie danych osobowych w sposób należyty przed dalszymi naruszeniami,
 - d. zbiera wszelkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości,
 - e. udziela Administratorowi wszelkiej pomocy w identyfikacji i zawiadomieniu osób, których praw dotyczyło naruszenie oraz w obsłudze ich roszczeń.
9. Podmiot przetwarzający w przypadku naruszenia ochrony danych osobowych z winy Administratora, a w szczególności w zakresie zasobów zarządzanych przez Administratora, w miarę możliwości udziela pomocy Administratorowi w:
 - a. ustaleniu przyczyny naruszenia,
 - b. ograniczeniu skutków naruszenia, usunięcia naruszenia oraz zabezpieczenia danych osobowych w sposób należyty przed dalszymi naruszeniami,
 - c. zgromadzeniu danych i dokumentów, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości,
 - d. pomocy w identyfikacji i zawiadomieniu osób, których praw dotyczyło naruszenie oraz w obsłudze ich roszczeń.
10. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o:
 - a. wszelkich postępowaniach, w szczególności administracyjnych lub sądowych, dotyczących przetwarzania przez Podmiot przetwarzający powierzonych danych,
 - b. wszelkich decyzjach administracyjnych lub orzeczeniach dotyczących przetwarzania tych danych skierowanych do Podmiotu przetwarzającego,
 - c. wszelkich planowanych lub realizowanych w Podmiocie przetwarzającym kontrolach i inspekcjach dotyczących przetwarzania powierzonych na podstawie niniejszej umowy danych, w szczególności prowadzonych przez przedstawicieli Prezesa Urzędu Ochrony Danych Osobowych.

§4 Obowiązki Administratora

1. Przetwarzając powierzone dane osobowe z wykorzystaniem narzędzi i mechanizmów udostępnionych przez Podmiot przetwarzający, Administrator i jego pracownicy zobowiązani są do stosowania się do technicznych i organizacyjnych środków bezpieczeństwa ustalonych przez Podmiot przetwarzający.
2. Administrator niezwłocznie, nie później niż w ciągu 24 godzin informuje Podmiot przetwarzający o:

- a. podejrzeniach naruszenia bezpieczeństwa danych osobowych,
- b. naruszeniach bezpieczeństwa danych osobowych,
- c. naruszeniach technicznych i organizacyjnych środków bezpieczeństwa przyjętych przez Podmiot przetwarzający,
- d. ujawnieniach technicznych i organizacyjnych środków bezpieczeństwa przyjętych przez Podmiot przetwarzający.

§5 Prawo kontroli

1. Na pisemny wniosek Administratora, Podmiot przetwarzający udziela informacji na temat przetwarzania powierzonych danych osobowych, w tym na temat zastosowanych przy przetwarzaniu danych osobowych środków technicznych i organizacyjnych, w ustalonym przez Administratora terminie nie krótszym niż 7 dni roboczych od dnia otrzymania wniosku.
2. Administrator ma prawo do przeprowadzenia audytów, realizowanych przez siebie lub upoważnionego audytora, oraz inspekcji spełnienia obowiązków określonych w niniejszej umowie w zakresie określonym w art. 28 ust. 3 lit. h Rozporządzenia.
3. Podmiot przetwarzający umożliwia i przyczynia się do realizacji audytów i inspekcji.
4. O planowanym audycie lub inspekcji Administrator informuje Podmiot przetwarzający nie później niż na 7 dni przed ich planowanym terminem w formie pisemnej w tym elektronicznej.
5. Administrator ma prawo do przeprowadzania audytów i inspekcji także u podwykonawców przetwarzania w trybie i zakresie określonym w niniejszej umowie. Podmiot przetwarzający zobowiązuje się zapewnić możliwość przeprowadzenia audytów i inspekcji u podmiotów, którym podpowierzył, w trybie §6 niniejszej umowy, przetwarzanie danych osobowych powierzonych przez Administratora.
6. Administrator zobowiązany jest zapewnić, że osoby wykonujące czynności kontrolne, w tym audytorzy zewnętrzni, którym Administrator zleca przeprowadzenie audytu, nie są zatrudnione, nie są współnikami, akcjonariuszami lub członkami organów podmiotów, wykonujących działalność konkurencyjną w stosunku do działalności gospodarczej prowadzonej przez Podmiot przetwarzający ani nie prowadzą takiej działalności konkurencyjnej we własnym imieniu.
7. Podmiot przetwarzający, w zakresie niezbędnym do przeprowadzenia czynności kontrolnych, będzie współpracować z Administratorem i upoważnionymi przez niego audytorami, w szczególności zapewniając im dostęp do pomieszczeń i dokumentów obejmujących dane osobowe Administratora oraz informacje o sposobie przetwarzania danych osobowych, infrastruktury teleinformatycznej oraz systemów IT, a także do osób mających wiedzę na temat procesów przetwarzania danych osobowych realizowanych przez Podmiot przetwarzający, z uwzględnieniem konieczności zapewnienia ciągłości działalności gospodarczej i procesów biznesowych realizowanych na bieżąco przez Podmiot przetwarzający. Administrator zapewni, że czynności kontrolne nie będą kolidowały z bieżącym wykonywaniem przez Podmiot przetwarzający czynności w ramach prowadzonej działalności gospodarczej.
8. O wynikach audytów i inspekcji Administrator informuje pisemnie Podmiot przetwarzający. Informacja pisemna zawiera opis podjętych czynności, opis ustalonego

stanu faktycznego, wnioski ustalone na podstawie zgromadzonych informacji i jasno sformułowane zalecenia.

9. Podmiot przetwarzający podejmuje działania naprawcze w zakresie stwierdzonych uchybień lub przekazuje wyjaśnienia o przyczynach niepodjęcia takich działań w terminie wskazanym przez Administratora nie krótszym niż 7 dni.

§6 Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający ma ogólną zgodę Administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu stanowiącego Załącznik nr 3. Podmiot przetwarzający informuje Administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej 30 dni, dając tym samym Administratorowi wystarczająco dużo czasu na wyrażenie sprzeciwu wobec takich zmian przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego (podmiotów podprzetwarzających). Podmiot przetwarzający przekazuje Administratorowi niezbędne informacje umożliwiające mu skorzystanie z prawa sprzeciwu.
2. W przypadku wyrażenia sprzeciwu przez Administratora, Podmiot przetwarzający nie jest uprawniony do zawarcia umowy z dalszym podmiotem przetwarzającym, którego dotyczy sprzeciw.
3. Jeżeli Podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu Administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszą Umową. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszej Umowy oraz Rozporządzenia.
4. Podmiot przetwarzający może przekazać powierzone dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie w przypadku:
 - a. pisemnego polecenia Administratora,
 - b. konieczności spełnienia obowiązku jaki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
 - c. podmiot, któremu podpowierzane jest przetwarzanie, w tym podmiot w państwie trzecim, winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
5. Odpowiedzialność wobec Administratora za niewywiązywanie się ze spoczywających na podmiocie podprzetwarzającym obowiązków ochrony danych ponosi Podmiot przetwarzający. Podmiot przetwarzający powiadamia Administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.

§ 7 Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za:
 - a. szkody wyrządzone wskutek niewykonania lub nienależytego wykonania obowiązków wynikających z niniejszej umowy,
 - b. udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym,
 - c. przetwarzanie z naruszeniem obowiązujących przepisów,
 - d. nieuprawnioną zmianę danych, uszkodzenie lub zniszczenie, które nastąpiły z winy Podmiotu przetwarzającego.
2. Odpowiedzialność ograniczona jest do szkody rzeczywistej.

§8 Odpowiedzialność Administratora

1. Administrator ponosi odpowiedzialność za szkody wyrządzone swoim działaniem niezgodnym z niniejszą umową oraz ustalonymi w trakcie ich realizacji zasadami bezpieczeństwa danych.

§9 Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakiegokolwiek inny sposób, zamierzony, czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
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. Administrator zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów, do których miał dostęp w wyniku realizacji swoich uprawnień wynikających z niniejszej umowy, w szczególności dotyczących stosowanych przez Podmiot przetwarzający środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa powierzanych danych. Zachowanie tajemnicy obowiązuje Administratora w trakcie realizacji niniejszej umowy i po zakończeniu jej obowiązywania

§10 Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje przez okres obowiązywania umowy, o której mowa w §2 ust. 2 niniejszej Umowy.
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem miesięcznego okresu wypowiedzenia.

§11 Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.

2. Załączniki nr 1-3 stanowią integralną część umowy.
3. Zmiany postanowień niniejszej Umowy i załączników wymagają formy pisemnej pod rygorem nieważności.
4. W razie sprzeczności między zapisami niniejszej Umowy a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszej Umowy lub zawartych po jej uzgodnieniu, pierwszeństwo mają zapisy Umowy.
5. Bez uszczerbku dla przepisów Rozporządzenia, w przypadku gdy Podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszej Umowy, Administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy Podmiot przetwarzający zapewni zgodność z niniejszą Umową. Podmiot przetwarzający niezwłocznie zawiadamia Administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszej Umowy.
6. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
7. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora.

Administrator

Podmiot przetwarzający

Kategorie osób i zakres danych przekazanych do przetwarzania:

- I. (np. pracownicy, klienci, kontrahenci)
 1. Zakres powierzanych do przetwarzania danych osobowych (art. 6 ust. 1 Rozporządzenia):
 - a. Imię i nazwisko,
 - b. Adres zamieszkania,
 - c. Adres email,
 - d. PESEL
 - e. Numer kontaktowy
 - f. Status na rynku pracy
 - g. Wykształcenie
 - h. Obywatelstwo
 2. Zakres powierzanych do przetwarzania danych osobowych (art. 9 ust. 1 Rozporządzenia):
 - a. Dane o stanie zdrowia

Wykaz środków technicznych i organizacyjnych

Środki techniczne i organizacyjne wymagane od Podmiotu przetwarzającego w celu zapewnienia odpowiedniego poziomu bezpieczeństwa powierzonych do przetwarzania danych osobowych:

1. Wdrożone i okresowo monitorowane polityki bezpieczeństwa, o których mowa w art. 24 ust. 2 Rozporządzenia.
2. Dopuszczanie do przetwarzania powierzonych danych wyłącznie pracowników posiadających upoważnienie.
3. Dopuszczanie do przetwarzania powierzonych danych wyłącznie pracowników zobowiązanych do zachowania w tajemnicy treści przetwarzanych danych, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.
4. Nadzór nad dostępem do danych osobowych powierzonych upoważnionym pracownikom.
5. Szkolenia pracowników w zakresie zgodnego z prawem przetwarzania danych osobowych.
6. Zapewnienie dostępu do systemów, w których przetwarzane są powierzone dane osobowe wyłącznie uprawnionym pracownikom.
7. Nadawanie uprawnień do systemów, w których przetwarzane są dane osobowe wyłącznie w zakresie niezbędnym do wykonania umowy.
8. Zapewnione jest tworzenie kopii zapasowych powierzonych danych osobowych na wypadek awarii systemów informatycznych, w tym zapewnienia możliwości ich przywrócenia w przypadku awarii systemów informatycznych.
9. Zastosowano środki chroniące sieci i urządzenia, za pomocą których przetwarzane są powierzone dane osobowe przed atakami w szczególności na podatności systemów, atakami DOS/DDoS, MAN-IN-THE-MIDDLE, wirusami, oprogramowaniem szpiegującym.
10. Stosowanie szyfrowania danych osobowych przenoszonych na przenośnych nośnikach danych lub przesyłanych drogą elektroniczną.
11. Zapewnienia ciągłości działania sieci i urządzeń za pomocą których przetwarzane są powierzone dane osobowe.
12. Systematyczna aktualizacja wykorzystywanego oprogramowania.

Wykaz podmiotów podprzetwarzających, z usług których korzysta Podmiot przetwarzający

Uwaga: przykład:

1. *hostingodawcy tacy jak: Home.pl, nazwa.pl, Google Inc.(gmail)*
2. *Podmioty świadczące usługi chmurowe: Microsoft Oracle, OneDrive, iCloud Drive*