

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu pomiędzy

.....

.....

.....

zwanym „Administratorem danych”

reprezentowanym przez:

oraz

.....

.....

.....

zwanym „Podmiotem przetwarzającym”

reprezentowanym przez:

zwanymi „Stronami”

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z zawarciem i realizacją umowy nr zawartej przez Strony, jako „Umowa główna” Administrator danych powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych zgodnie z art. 28 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35) (dalej: RODO), wyłącznie w zakresie koniecznym do prawidłowej realizacji Umowy głównej oraz w celu w niej określonym.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania danych w imieniu Administratora danych zgodnie z umową, RODO, a także innymi przepisami prawa powszechnie obowiązującego, co do zgodności takiego przetwarzania z prawem.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał na podstawie niniejszej umowy dane
(należy podać rodzaj danych: dane zwykłe lub dane szczególnej kategorii) dotyczące
(należy podać kategorię osób, których dane dotyczą) w zakresie
(należy podać kategorię danych osobowych, np. imię i nazwisko, nr PESEL, adres e-mail itp.).
2. Podmiot przetwarzający zobowiązuje się w imieniu Administratora danych przetwarzać dane osobowe w celu
(należy podać cel przetwarzania: np. realizacja umowy nr z dnia w zakresie).
3. Podmiot przetwarzający zobowiązuje się w imieniu Administratora danych przetwarzać dane osobowe w charakterze
(należy podać charakter przetwarzania danych np.: zautomatyzowany, częściowo zautomatyzowany obejmujący operacje na danych osobowych np.: organizowanie, modyfikowanie, pobieranie itp.)

§ 3

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu danych osobowych zobowiązuje się do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, przy uwzględnieniu stanu wiedzy technicznej, zapewniających adekwatny stopień bezpieczeństwa w kontekście ryzyka przetwarzania związanym z przetwarzaniem danych osobowych, o czym mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się przetwarzać dane osobowe przy zachowaniu należytej staranności, przestrzeganiu zasad przetwarzania z art. 5 RODO
3. Podmiot przetwarzający zapewnia nadanie upoważnienia do przetwarzania danych osobowych osobom przeszkolonym z zakresu ochrony danych osobowych, a także zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, a także po ustaniu takiego zatrudnienia.
4. Przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora danych.
5. Podmiot przetwarzający pomaga Administratorowi danych:
 - 1) Wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III (Prawa osoby, której dane dotyczą), poprzez odpowiednie środki techniczne i organizacyjne

- 2) Wywiązać się z obowiązków określonych w art. 32-36 RODO, w przypadku stwierdzenia naruszenia, podmiot przetwarzający zobowiązany jest zgłosić administratorowi nie później niż w terminie 48 godzin od chwili stwierdzenia naruszenia.
6. Podmiot przetwarzający po zakończeniu umowy jest zobowiązany zależnie od decyzji Administratora danych do usunięcia lub zwrócenia wszelkich danych osobowych oraz usunięcia wszelkich istniejących ich kopii, chyba, że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych
7. Podmiot przetwarzający zobowiązuje się do wypełnienia ankiety bezpieczeństwa przetwarzania z załącznika nr 1 i dostarczenia jej Administratorowi danych w celu weryfikacji przez Administratora danych zdolności przez Podmiot przetwarzający do zapewnienia bezpieczeństwa przetwarzania.

§ 4

Podpowierzenie

1. Podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego wyłącznie po uprzedniej zgodzie Administratora danych wyrażonej pisemnie.
2. Inny podmiot przetwarzający powinien zapewniać, zgodnie z art. 28 ust. 4 RODO, gwarancje bezpieczeństwa przetwarzania i obowiązki, które zostały nałożone na Podmiot przetwarzający na podstawie umowy między Administratorem danych a Podmiotem przetwarzającym. Umowa zawarta pomiędzy Podmiotem przetwarzającym a innym podmiotem przetwarzającym nakłada na inny podmiot przetwarzający takie same obowiązki, jakie Administrator danych nałożył na Podmiot przetwarzający.
3. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora danych. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora danych o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
4. Podmiot przetwarzający wnioskuje do Administratora danych o udzielenie szczegółowej zgody. Pisemny wniosek zawiera informacje o innym podmiocie przetwarzającym, czynnościach przetwarzania i zakresie danych, do których ma odnosić się szczegółowa zgoda na korzystanie z usług innego podmiotu przetwarzającego.
5. W przypadku, gdy Administrator danych nie udzieli odpowiedzi na wniosek Podmiotu przetwarzającego o udzielenie szczegółowej zgody w terminie 14 dni, należy wniosek uznać za odrzucony.
6. W przypadku, gdy Administrator danych nie wyrazi sprzeciwu na wniosek Podmiotu przetwarzającego o udzielenie zgody ogólnej w terminie 14 dni, należy brak sprzeciwu Administratora danych interpretować, jako udzielenie zgody.

§ 5

Prawo do kontroli

1. Administrator danych ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu danych spełniają postanowienia niniejszej umowy i RODO
2. Podmiot przetwarzający zobowiązanych na każdy pisemny wniosek Administratora danych udzielić pisemnej informacji dotyczącej przetwarzania powierzonych mu danych osobowych w terminie 7 dni od dnia otrzymania takiego wniosku.
3. Administrator danych ma prawo do faktycznej weryfikacji sposobu przetwarzania powierzonych danych osobowych, w sposób każdorazowo ustalony przez Strony, po zgłoszeniu zamiaru weryfikacji przez Administratora danych
4. W przypadku uniemożliwienia kontroli przeprowadzonej przez Administratora danych lub nieudzielenia pisemnej informacji dotyczących przetwarzania powierzonych danych Podmiot przetwarzający zobowiązuje się do zapłaty na rzecz Administratora danych kary umownej w wysokości za każde naruszenie.
5. Podmiot przetwarzający udostępnia wszelkie informacje Administratorowi danych w celu wykazania przestrzegania art. 28 RODO.
6. Po stwierdzeniu przez Administratora danych naruszeń niniejszej umowy Podmiot przetwarzający zobowiązany jest do ich usunięcia w terminie i sposobie określonym przez Strony.

§ 6

Odpowiedzialności Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, w szczególności za udostępnienie osobom nieuprawnionym powierzonych do przetwarzania danych osobowych.
2. Podmiot przetwarzający zobowiązany jest do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych

§ 7

Czas obowiązywania umowy

1. Umowa obowiązuje przez okres trwania Umowy głównej.
2. W każdym wypadku Umowa powierzenia przestaje wiązać Strony z dniem rozwiązania Umowy głównej.

3. Wszelkie spory wynikłe w związku z zawarciem lub wykonaniem Umowy powierzenia rozstrzygane będą przez sąd powszechny właściwy miejscowo dla siedziby Administratora danych.

.....

Administrator danych

.....

Podmiot przetwarzający

Załączniki:

1. Załącznik nr 1 – Ankieta bezpieczeństwa przetwarzania: środki techniczne i organizacyjne przyjęte przez Podmiot przetwarzający

**Ankieta bezpieczeństwa przetwarzania:
środki techniczne i organizacyjne przyjęte przez Podmiot przetwarzający**

Lp.	Pytanie	Odpowiedź
1	Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych?	
2	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?	
3	Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
4	Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
5	Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
6	Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
7	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy?	
8	Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO?	
9	Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	
10	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?	
11	Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
12	Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?	

13	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?	
14	Czy każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych?	
15	Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby?	
16	Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób?	
17	Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	
18	Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamkniętych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	
19	Czy zapewniono licencjonowane oraz aktualizowane oprogramowanie antywirusowe na wszystkich stacjach oraz urządzeniach mobilnych?	
20	Czy stosuje się szyfrowanie dysków komputerów przenośnych?	
21	Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?	
22	Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne?	
23	Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
24	Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych?	
25	Gdzie są przechowywane kopie zapasowe?	
26	Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?	
27	Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"?	
28	Czy organizacja działa zgodnie z zasadą "privacy by default"?	
29	Czy organizacja prowadzi ocenę skutków dla ochrony danych?	
30	Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do odgraniczenia przetwarzania, prawo do bycia zapomnianym?	