UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu …… pomiędzy

……

……

……

zwanym „Administratorem danych”

reprezentowanym przez: ……

oraz

……

……

……

zwanym „Podmiotem przetwarzającym”

reprezentowanym przez: ……

zwanych „Stronami”

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z zawarciem i realizacją umowy nr …… zawartej przez Strony, zwanej dalej 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 osobowych w imieniu Administratora danych zgodnie z Umową, Umową główną, RODO, a także innymi mającymi zastosowanie przepisami prawa powszechnie obowiązującego.

§ 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. Przetwarzanie danych osobowych podejmowane przez Podmiot przetwarzający w imieniu Administratora danych będzie miało następujący charakter:

   ……

   (*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 w celu zabezpieczenia powierzonych mu do przetwarzania danych osobowych, podejmuje wszelkie środki wymagane na mocy art. 32 RODO, tj. uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2. Podmiot przetwarzający zobowiązuje się przetwarzać dane osobowe przy zachowaniu należytej staranności.
3. Podmiot przetwarzający zapewnia nadanie upoważnienia do przetwarzania danych osobowych, powierzonych mu na podstawie niniejszej Umowy, 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. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora danych.
5. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania

osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.

6. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi danych wywiązać się z obowiązków określonych w art. 32-36 RODO. W szczególności, Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, zobowiązany jest zgłosić je Administratorowi danych bez zbędnej zwłoki, nie później jednak niż w ciągu 24 h od stwierdzenia naruszenia. Zgłoszenie powinno uwzględniać informacje, o których mowa w art. 33 ust. 3 RODO.

7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych, określonych w Umowie głównej 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.
8. Podmiot przetwarzający zobowiązuje się do wypełnienia ankiety bezpieczeństwa przetwarzania, stanowiącej Załącznik nr 1 do niniejszej Umowy i do dostarczenia jej Administratorowi danych w celu weryfikacji przez Administratora danych zdolności Podmiotu przetwarzającego do zapewnienia bezpieczeństwa przetwarzania powierzonych danych osobowych.

§ 4

Podpowierzenie

1. Podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego wyłącznie po uprzedniej zgodzie Administratora danych wyrażonej pisemnie i z zachowaniem warunków określonych poniżej.
2. Podmiot przetwarzający korzysta wyłącznie z usług takich innych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. W przypadku korzystania przez Podmiot przetwarzający z usług innych podmiotów przetwarzających (za zgodą Administratora danych, o której mowa powyżej), Podmiot przetwarzający nałoży na ten inny podmiot przetwarzający na mocy umowy te same obowiązki ochrony danych, jak w niniejszej Umowie.
3. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora danych.
4. 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 danych możliwość wyrażenia sprzeciwu wobec takich zmian.
5. W przypadku, gdy Administrator danych nie wyrazi sprzeciwu na wniosek Podmiotu przetwarzającego o udzielnie zgody ogólnej, o której mowa w ust. 4 powyżej, w terminie 14 dni od dnia otrzymania wniosku, należy brak sprzeciwu Administratora danych interpretować, jako udzielenie zgody.

6. 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.
7. W przypadku, gdy Administrator danych nie udzieli odpowiedzi na wniosek Podmiotu przetwarzającego o udzielenie szczegółowej zgody, o której mowa w ust. 6 powyżej, w terminie 14 dni od dnia otrzymania wniosku, należy wniosek uznać za odrzucony.
8. Jeżeli inny podmiot przetwarzający, zaangażowany przez Podmiot przetwarzający do przetwarzania danych osobowych powierzonych mu na mocy niniejszej Umowy, nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora danych za wypełnienie obowiązków tego innego podmiotu przetwarzającego, spoczywa na Podmiocie przetwarzającym.

§ 5

Prawo do kontroli

1. Administrator danych, zgodnie z art. 28 ust. 3 pkt h) RODO, ma prawo kontroli, czy Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych spełnia wymagania RODO i niniejszej Umowy.
2. Podmiot przetwarzający zobowiązuje się:
   a) niezwłocznie udostępnić Administratorowi danych, na każde jego żądanie, wszelkich informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Podmiocie przetwarzającym;
   b) umożliwić Administratorowi danych lub audytorowi upoważnionemu przez Administrator danych przeprowadzanie audytów, w tym inspekcji, i przyczyniać się do nich. Administrator danych każdorazowo zawiadomi Podmiot przetwarzający o zamiarze przeprowadzenia audytu i w takiej sytuacji Strony niezwłocznie uzgodnią termin i sposób jego przeprowadzenia.
3. Podmiot przetwarzający zobowiązuje się do zastosowania ewentualnych zaleceń pokontrolnych Administratora danych, dotyczących ochrony powierzonych danych osobowych oraz sposobu ich przetwarzania, o ile zalecenia te są zgodnie z niniejszą Umową i obowiązującymi przepisami prawa.
4. W przypadku stwierdzenia przez Administratora danych w wyniku czynności kontrolnych naruszenia przez Podmiot przetwarzający postanowień niniejszej Umowy lub przepisów o ochronie danych osobowych, w tym RODO, Podmiot przetwarzający zobowiązany jest do ich bezzwłocznego usunięcia w terminie wskazanym przez Administratora danych.

5. W przypadku uniemożliwienia przez Podmiot przetwarzający Administratorowi realizowania przysługującego mu prawa do kontroli, o którym mowa w niniejszym paragrafie, Podmiot przetwarzający zobowiązuje się do zapłaty na rzecz

Administratora danych kary umownej w wysokości …….. za każde naruszenie.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, w szczególności za udostępnienie osobom nieuprawnionym powierzonych mu do przetwarzania danych osobowych.
2. Podmiot przetwarzający zobowiązany jest do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający (lub dalszy podmiot przetwarzający) danych osobowych powierzonych mu przez Administratora danych na podstawie niniejszej Umowy, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego (lub dalszych podmiotów przetwarzających), a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania przez Podmiot przetwarzający (lub dalsze podmioty przetwarzające) tych danych osobowych. .

§ 7

Czas obowiązywania umowy

1. Umowa obowiązuje przez okres obowiązywania Umowy głównej.
2. W każdym wypadku niniejsza Umowa przestaje wiązać Strony z dniem rozwiązania Umowy głównej.
3. Administrator danych jest uprawniony do rozwiązania niniejszej Umowy w trybie natychmiastowym w przypadku niespełnienia przez Podmiot przetwarzający wymagań wynikających z art. 28 RODO lub rażącego naruszenia przez niego postanowień niniejszej Umowy, w szczególności, gdy Podmiot przetwarzający:
   a) nie usunął uchybień pokontrolnych w terminie określonym w § 5 ust. 4 niniejszej Umowy;
   b) wykorzystał powierzone mu przez Administratora danych dane osobowe w sposób niezgodny z niniejszą Umową;
   c) powierzył przetwarzanie danych osobowych powierzonych mu przez Administratora danych innemu podmiotowi przetwarzającemu niezgodnie z niniejszą Umową;
   d) naruszył w sposób rażący obowiązki określone w § 3 niniejszej Umowy, w szczególności obowiązek zgłaszania naruszeń ochrony danych, o którym mowa w § 3 ust. 6 niniejszej Umowy.

§ 8

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonywane w taki sam sposób, jak to określono w Umowie głównej.
2. W zakresie nieuregulowanym w niniejszej Umowie zastosowanie mają właściwe przepisy prawa, w szczególności RODO i kodeksu cywilnego.
3. Wszelkie spory wynikłe w związku z zawarciem lub wykonaniem niniejszej Umowy powierzenia rozstrzygane będą przez sąd powszechny właściwy miejscowo dla siedziby Administratora danych.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

……	……
Administrator danych	Podmiot przetwarzający

Załączniki:

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

Załącznik nr 1

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 zamykanych 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?	