

Projekt Umowy powierzenia przetwarzania danych osobowych

zawarta w dniu 20..... roku

pomędzy:

.....z siedzibą w(adres:), wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy Wydział Gospodarczy pod numerem KRS, NIP:, kapitał zakładowy, w imieniu której działa:

.....

.....

zwaną dalej „Administratorem”

a

..... z siedzibą w(adres:), wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy Wydział Gospodarczy pod numerem KRS, NIP:, kapitał zakładowy, w imieniu, której działa:

.....

.....

zwaną dalej „Podmiotem przetwarzającym”

zwane dalej również pojedynczo „Stroną” lub łącznie „Stronami”.

§1. Cel i zakres

1. Celem niniejszej umowy („umowa”) jest zapewnienie przestrzegania art. 28 ust. 3 i 4 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, zwane dalej RODO)
2. Niniejsza umowa ma zastosowanie do przetwarzania danych osobowych określonych w załączniku I.
3. Załączniki I–III stanowią integralną część umowy.
4. Niniejsza umowa pozostaje bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy RODO.

§2. Niezmiennność umowy

1. Strony zobowiązują się nie zmieniać umowy z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.
2. Postanowienie to, nie uniemożliwia stronom stosowania klauzul o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem, że nie będą one bezpośrednio lub pośrednio sprzeczne z umową ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

§3. Wykładnia

1. Jeżeli w niniejszej umowie użyto terminów zdefiniowanych w RODO, terminy te mają takie samo znaczenie jak w RODO.
2. Niniejsza umowa odczytuje się i interpretuje w świetle przepisów RODO.
3. Niniejszej umowy nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w RODO ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

§4. Hierarchia

W razie sprzeczności między niniejszą umową a postanowieniami umów zawartych między stronami, pierwszeństwo ma niniejsza umowa.

OBOWIĄZKI STRON

§5. Opis przetwarzania

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorii danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w załączniku I.

§6. Obowiązki stron

Polecenia

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 RODO lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

Ograniczenie celu

3. Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w załączniku I, chyba, że otrzyma dalsze polecenia od administratora.

Czas trwania przetwarzania danych osobowych

4. Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w załączniku I.

Bezpieczeństwo przetwarzania

5. W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża, co najmniej środki techniczne i organizacyjne określone w załączniku II. Zapewnienie bezpieczeństwa danych obejmuje 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.
6. Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

Dane wrażliwe

7. 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.

Dokumentacja i zgodność

8. Strony są w stanie wykazać zgodność z niniejszą umową.
9. Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszą umową.
10. Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszej umowie i wynikają

bezpośrednio z RODO. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszą umową i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.

11. Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
12. Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej umowie, w tym wyniki wszelkich audytów.

§7. Korzystanie z usług podmiotów podprzetwarzających

OPCJA 1: UPRZEDNIA SZCZEGÓŁOWA ZGODA:

1. Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu administratora zgodnie z niniejszą umową podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody co najmniej [NALEŻY PODAĆ TERMIN] przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik III zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika III.

OPCJA 2: OGÓLNA PISEMNA ZGODA:

1. Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu. Podmiot przetwarzający informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej [NALEŻY PODAĆ TERMIN], 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. 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 RODO.
3. Na wniosek administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.
4. Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.
5. Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym umowę dotyczącą beneficjenta będącego osobą trzecią, zgodnie, z którą to umową, – jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

§8. Międzynarodowe przekazywanie danych

1. Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V RODO.
2. Jeżeli zgodnie z umową podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V RODO, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V RODO za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 RODO, pod warunkiem że spełnione są warunki stosowania tych standardowych umowy umownych.

§9. Pomoc dla administratora

1. Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba, że administrator wyraził na to zgodę.
2. Podmiot przetwarzający pomaga administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z pkt. 1. i 2., podmiot przetwarzający stosuje się do poleceń administratora.
3. Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z pkt 2. podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
 - a. obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych”), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
 - b. obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego ograniczenia;
 - c. obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;
 - d. obowiązki określone w art. 32 RODO.
4. Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej umowy, jak również zakres wymaganej pomocy.

§10. Zgłaszanie naruszenia ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 RODO, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.
2. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:
 - a. przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi (-om) nadzorczemu(-ym) niezwłocznie po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
 - b. przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO powinny być zawarte w zgłoszeniu administratora i obejmować, co najmniej:

- i. charakter danych osobowych, w tym w miarę możliwości kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - ii. możliwe konsekwencje naruszenia ochrony danych osobowych;
 - iii. środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;
4. Przy wypełnianiu – zgodnie z art. 34 RODO – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
5. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu.
6. Zgłoszenie to powinno zawierać co najmniej:
 - a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
 - b) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
 - c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.
7. Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.
8. Strony określają w załączniku II wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 RODO.

POSTANOWIENIA KOŃCOWE

§11. *Naruszenie umowy i rozwiązanie umowy*

1. Bez uszczerbku dla przepisów RODO, 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, lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszej umowy.
2. Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszą umową, jeżeli:
 - a. administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z pkt 1. i jeżeli zgodność z niniejszą umową nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
 - b. podmiot przetwarzający poważnie lub stale narusza niniejszą umowę lub swoje obowiązki wynikające z RODO;
 - c. podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych umowy lub z RODO.
3. Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszą umową, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z §6 pkt 2 niniejszej umowy, administrator nalega na wypełnienie polecenia.

4. Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba, że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych umowy do czasu usunięcia lub zwrotu danych.

.....
Administrator

.....
Podmiot przetwarzający

ZAŁĄCZNIK I

Opis przetwarzania

Kategorie osób, których dane osobowe są przetwarzane
Kategorie przetwarzanych danych osobowych
Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa.
Charakter przetwarzania
Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora
Czas trwania przetwarzania

ZAŁĄCZNIK II

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

UWAGA WYJAŚNIAJĄCA:

Środki techniczne i organizacyjne należy opisać szczegółowo, a nie w sposób ogólny.

Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych:

--

Przykłady możliwych środków:

- ☐ Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych
- ☐ Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
- ☐ Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
- ☐ Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
- ☐ Środki umożliwiające identyfikację i autoryzację użytkowników
- ☐ Środki zapewniające ochronę danych w czasie ich przekazywania
- ☐ Środki zapewniające ochronę danych w czasie ich przechowywania
- ☐ Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe
- ☐ Środki umożliwiające rejestrowanie zdarzeń
- ☐ Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej
- ☐ Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT
- ☐ Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów
- ☐ Środki zapewniające minimalizację danych
- ☐ Środki zapewniające odpowiednią jakość danych
- ☐ Środki zapewniające ograniczone zatrzymywanie danych
- ☐ Środki zapewniające rozliczalność
- ☐ Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania]

W przypadku przekazywania danych podmiotom przetwarzającym lub podprzetwarzającym należy również opisać konkretne środki techniczne i organizacyjne, jakie powinien zastosować podmiot przetwarzający lub podprzetwarzający, aby móc udzielić pomocy administratorowi.

Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy administratorowi:

--

ZAŁĄCZNIK III

Wykaz podmiotów podprzetwarzających

UWAGA WYJAŚNIAJĄCA:

Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających (§7 pkt 1, opcja 1).

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1.	Imię i nazwisko lub nazwa	
	Adres	
	Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających)	
2.	Imię i nazwisko lub nazwa	
	Adres	
	Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających)	