

UMOWA

powierzenia przetwarzania danych osobowych

§ 1.

Na użytek niniejszej umowy przyjmuje się definicje określone w art. 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 (Dziennik Urzędowy Unii Europejskiej L 119 z późn. zm.), zwanego dalej rozporządzeniem 2016/679.

§ 2.

Standardowe klauzule przyjęte na użytek niniejszej umowy określone zostały zgodnie z decyzją wykonawczą 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 2016/679.

§ 3.

Strony niniejszej umowy wymienione w załączniku I uzgodniły jej treść w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 rozporządzenia 2016/679.

§ 4.

Umowa ta ma zastosowanie do przetwarzania danych osobowych określonego w załączniku II.

§ 5.

Strony niniejszej umowy zobowiązują się nie zmieniać jej treści z wyjątkiem dodawania informacji do załączników I-IV lub aktualizowania zawartych w nich informacji.

§ 6.

W przypadku sprzeczności klauzul niniejszej umowy z postanowieniami innych umów zawartych pomiędzy stronami, istniejących w chwili uzgadniania jej treści lub zawartych po jej uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

§ 7.

1. Każdy podmiot niebędący stroną niniejszej umowy może za zgodą stron przystąpić do procesu przetwarzania danych osobowych jako administrator lub podmiot przetwarzający w dowolnym czasie, wypełniając załączniki i podpisując załącznik I.
2. Po wypełnieniu i podpisaniu załączników do niniejszej umowy podmiot przystępujący będzie traktowany jako strona umowy z prawami i obowiązkami administratora lub podmiotu przetwarzającego, zgodnie z rolą nadaną mu w załączniku I.

§ 8.

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

§ 9.

1. Niniejsza umowa stanowi udokumentowane polecenie administratora, o którym mowa w art. 28 rozporządzenia 2016/679. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na tej podstawie, 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 rozporządzenie (UE) 2016/679 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

§ 10.

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

§ 11.

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

§ 12.

1. W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. 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.
2. 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.

3. 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.

§ 13.

1. Strony są w stanie wykazać zgodność przetwarzania danych osobowych z niniejszą umową.
2. Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszą umową.
3. Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679. 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 posiada podmiot przetwarzający.
4. Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub w obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
5. Na wniosek właściwego organu nadzorczego Strony udostępniają mu informacje, o których mowa w niniejszej umowie, w tym wyniki wszelkich audytów.
6. Podmiot przetwarzający niezwłocznie zawiadamia administratora o postępowaniach kontrolnych i wynikach tych kontroli, jeśli obszar obejmował również powierzone dane.

§ 14.

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 na 14 dni przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik IV zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika IV.
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 postanowień niniejszej umowy oraz rozporządzenia (UE) 2016/679.

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 klauzulę dotyczącą osób trzecich, zgodnie z którą to klauzulą – 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.

§ 15.

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 rozporządzenia (UE) 2016/679.
2. Jeżeli 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 rozporządzenia (UE) 2016/679, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, wyłącznie gdy spełnione są warunki stosowania standardowych klauzul umownych.

§ 16.

1. Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą, w zakresie realizacji jej praw. 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 w tym zakresie podmiot przetwarzający stosuje się do poleceń administratora.
3. Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie ust. 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 organem nadzorczym 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 rozporządzenia (UE) 2016/679,
4. Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

§ 17.

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

§ 18.

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:

- 1) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu 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);
- 2) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:
 - a) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
 - b) możliwe konsekwencje naruszenia ochrony danych osobowych,
 - c) 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) przy wypełnianiu – zgodnie z art. 34 rozporządzenia (UE) 2016/679 – 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.

§ 19.

W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający, podmiot przetwarzający zgłasza ten fakt administratorowi niezwłocznie (w ciągu 24 godzin) po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

- 1) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);

- 2) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
- 3) 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.

§ 20.

Jeżeli przekazanie wszystkich informacji, o których mowa w § 18 i § 19 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. Podmiot przetwarzający zobowiązany jest zabezpieczyć środki dowodowe pozwalające na ocenę zdarzenia.

§ 21.

Strony określają w załączniku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679.

§ 22.

1. 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 klauzulami umownymi. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do wymogów określonych niniejszą umową.
2. Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z klauzulami umownymi, jeżeli:
 - a) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z ust. 1 i jeżeli zgodność z klauzulami umownymi nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia,
 - b) podmiot przetwarzający poważnie lub stale narusza klauzule umowne lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679,
 - c) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego organu nadzorczego, dotyczącej jego obowiązków wynikających z niniejszej umowy z przepisów rozporządzenia (UE) 2016/679.
3. Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z klauzulami umownymi, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne, administrator nalega na wypełnienie polecenia, wydanego zgodnie z § 9 ust. 1 niniejszej umowy.
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 klauzul umownych do czasu usunięcia lub zwrotu danych.

Wykaz stron

Administrator:

**Województwo Kujawsko-Pomorskie – Urząd Marszałkowski Województwa
Kujawsko-Pomorskiego w Toruniu**

NIP: 956-19-45-671, REGON: 871121290

Plac Teatralny 2, 87-100 Toruń, reprezentowane przez:

Marszałka Województwa Kujawsko-Pomorskiego – Piotra Całbeckiego,

w którego imieniu niniejszą umowę podpisuje:

.....

Podpis i data przystąpienia:

.....

Podmiot przetwarzający:

.....

.....

.....

NIP: REGON:

w którego imieniu niniejszą umowę podpisuje:

.....

Podpis i data przystąpienia:

.....

Opis przetwarzania

1. Kategorie osób, których dane osobowe są przetwarzane:

.....

2. Kategorie przetwarzanych danych osobowych:

.....

3. 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:

.....

.....

4. Charakter przetwarzania:

.....

5. Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora:

.....

6. Czas trwania przetwarzania:

.....

(W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania.)

.....

.....

.....

**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:

- 1) środki umożliwiające pseudonimizację i szyfrowanie danych osobowych;
- 2) środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- 3) środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- 4) procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
- 5) środki umożliwiające identyfikację i autoryzację użytkowników;
- 6) środki zapewniające ochronę danych w czasie ich przekazywania;
- 7) środki zapewniające ochronę danych w czasie ich przechowywania;
- 8) środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe;
- 9) środki umożliwiające rejestrowanie zdarzeń;
- 10) środki służące do konfiguracji systemu, w tym konfiguracji domyślnej;
- 11) środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT;
- 12) środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów
- 13) środki zapewniające minimalizację danych
- 14) środki zapewniające odpowiednią jakość danych
- 15) środki zapewniające ograniczone zatrzymywanie danych
- 16) środki zapewniające rozliczalność
- 17) 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:

.....

.....

.....

Wykaz podmiotów podprzetwarzających

(UWAGA WYJAŚNIAJĄCA: niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających, zgodnie z § 14 umowy powierzenia przetwarzania danych osobowych.)

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. Imię i nazwisko lub nazwa:

.....

Adres:

.....

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

.....

Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

.....

2. Imię i nazwisko lub nazwa:

.....

Adres:

.....

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

.....

Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

.....