

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Sztumie w dniu r. pomiędzy:

Starostą Powiatu Sztumskiego, działającym przy pomocy Starostwa Powiatowego w Sztumie, ul. Mickiewicza 31, 82-400 Sztum, jako administratorem danych osobowych w zakresie danych przetwarzanych w związku z prowadzeniem ewidencji gruntów i budynków, zwanym dalej „Administratorem”,

a

[Wykonawca – pełna nazwa, adres, NIP, REGON, KRS/CEIDG, reprezentacja], zwanym dalej „Podmiotem przetwarzającym” lub „Procesorem”,

łącznie zwanymi dalej „Stronami”. Umowa zostaje zawarta w wykonaniu Umowy GK dotyczącej zadania: „Doprowadzenie do zgodności oznaczenia klasoużytków (użytków gruntowych, klas bonitacyjnych) pomiędzy częścią opisową (rejestr gruntów) a częścią graficzną (mapa ewidencji gruntów) bazy danych ewidencji gruntów i budynków”, dalej „Umowa główna”.

§ 1. Przedmiot, czas, charakter i cel powierzenia

1. Administrator powierza Procesorowi przetwarzanie danych osobowych wyłącznie w zakresie niezbędnym do wykonania Umowy głównej i wyłącznie na udokumentowane polecenie Administratora, w rozumieniu art. 28 RODO.
2. Powierzenie obejmuje czas od udostępnienia Procesorowi pierwszego dostępu do danych do wykonania obowiązków zwrotu/usunięcia po zakończeniu Umowy głównej, chyba że prawo Unii lub prawo krajowe nakazuje dalsze przechowywanie określonych danych.
3. Charakter operacji obejmuje w szczególności: dostęp, przeglądanie, analizę, porządkowanie, zestawianie, dopasowywanie, modyfikowanie danych w granicach zaakceptowanych zmian EGiB, przygotowywanie plików i dokumentacji oraz techniczne zasilenie bazy EGiB – wyłącznie w zakresie wynikającym z Umowy głównej i Warunków Technicznych.
4. Celem przetwarzania jest wykonanie czynności koniecznych do doprowadzenia do zgodności danych EGiB oraz sporządzenia i wdrożenia wyników prac. Procesor nie jest uprawniony do wykorzystywania danych we własnych celach, w tym analitycznych, szkoleniowych, marketingowych, testowych, rozwojowych ani do tworzenia własnych baz.

§ 2. Kategorie osób i danych

1. Kategorie osób, których dane mogą być przetwarzane, obejmują w szczególności właścicieli, współwłaścicieli, użytkowników wieczystych, władających, osoby, których prawa lub inne oznaczenia ujawniono w dokumentach źródłowych PZGiK i EGiB, pełnomocników oraz osoby występujące w dokumentacji geodezyjnej.
2. Kategorie danych obejmują wyłącznie dane rzeczywiście występujące w materiałach niezbędnych do realizacji zadania, w szczególności: imię i nazwisko, adres lub inne dane lokalizacyjne, identyfikatory i oznaczenia nieruchomości, numery działek, numery ksiąg wieczystych, dane dotyczące praw do nieruchomości oraz inne dane znajdujące się w dokumentach źródłowych, jeżeli ich przetwarzanie jest konieczne do wykonania Umowy głównej.
3. Procesor stosuje zasadę minimalizacji: nie pozyskuje, nie kopiuje i nie utrzuca danych, które nie są konieczne do wykonania konkretnej czynności.

§ 3. Polecenia Administratora i zgodność z prawem

1. Procesor przetwarza dane wyłącznie na udokumentowane polecenie Administratora, w tym w zakresie przekazywania danych do państwa trzeciego lub organizacji międzynarodowej, chyba że obowiązek taki nakłada prawo Unii lub prawo krajowe; w takim przypadku Procesor informuje Administratora przed rozpoczęciem przetwarzania, o ile prawo nie zabrania takiej informacji.
2. Jeżeli zdaniem Procesora polecenie narusza RODO albo inne przepisy o ochronie danych, Procesor niezwłocznie informuje Administratora przed jego wykonaniem, wskazując przyczynę zastrzeżenia.
3. Procesor nie podejmuje samodzielnie decyzji o celach przetwarzania ani nie rozszerza zakresu danych poza polecenia i Umowę główną.

§ 4. Osoby upoważnione i poufność

1. Procesor zapewnia, że do danych mają dostęp wyłącznie osoby imiennie upoważnione w zakresie niezbędnym do wykonywanych zadań. Upoważnienia są udzielane najpóźniej przed uzyskaniem dostępu i są niezwłocznie odwoływane po ustaniu potrzeby dostępu.
2. Procesor prowadzi aktualną ewidencję osób upoważnionych i na żądanie Administratora przekazuje informację o osobach posiadających dostęp, ich roli i okresie dostępu.
3. Osoby upoważnione są zobowiązane do zachowania poufności na podstawie zobowiązania umownego lub ustawowego, również po ustaniu upoważnienia.
4. Procesor zapewnia osobom upoważnionym odpowiednie instrukcje i szkolenie z zakresu ochrony danych i bezpieczeństwa informacji.

§ 5. Środki techniczne i organizacyjne

1. Procesor wdraża i utrzymuje przez cały okres powierzenia środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku, zgodnie z art. 32 RODO i załącznikiem nr 1 (TOMs).
2. Procesor nie może obniżyć poziomu bezpieczeństwa określonego w TOMs bez uprzedniej pisemnej zgody Administratora. Administrator może, z uzasadnionych przyczyn bezpieczeństwa, nakazać zastosowanie dodatkowego środka adekwatnego do ryzyka, jeżeli nie prowadzi to do nieuzasadnionej zmiany przedmiotu Umowy głównej.
3. Dane są przetwarzane co do zasady w środowisku teleinformatycznym Zamawiającego przez dostęp zdalny. Lokalne kopiowanie danych jest zabronione, chyba że Administrator wyrazi uprzednią pisemną zgodę i określi warunki zabezpieczenia.

§ 6. Dalsze powierzenie

1. Procesor nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniego szczegółowego pisemnego upoważnienia Administratora. Za upoważnione uważa się podmioty jednoznacznie wskazane w ofercie i zaakceptowane przy zawieraniu Umowy głównej – wyłącznie w zakresie ujawnionym Administratorowi.
2. Wprowadzenie nowego podprocesora albo zmiana zakresu podpowierzenia wymaga uprzedniej pisemnej zgody Administratora.
3. Procesor nakłada na podprocesora, na podstawie umowy lub innego aktu prawnego, co najmniej te same obowiązki ochrony danych, które wynikają z niniejszej Umowy, i odpowiada wobec Administratora za wykonanie obowiązków podprocesora.
4. Na żądanie Administratora Procesor udostępni informację o tożsamości podprocesora, miejscu przetwarzania i zakresie powierzonych mu operacji.

§ 7. Pomoc Administratorowi

Procesor, uwzględniając charakter przetwarzania i dostępne informacje, pomaga Administratorowi w szczególności w:

- 1) realizacji praw osób, których dane dotyczą;
- 2) zapewnieniu bezpieczeństwa przetwarzania; 3) ocenie skutków dla ochrony danych i uprzednich konsultacjach, jeżeli będą wymagane;
- 3) wyjaśnianiu skarg, postępowań i kontroli organu nadzorczego;
- 4) wykazaniu zgodności z art. 28–36 RODO.

§ 8. Naruszenia ochrony danych i incydenty

1. Procesor zgłasza Administratorowi każde naruszenie ochrony danych osobowych lub zdarzenie, które może prowadzić do naruszenia poufności, integralności lub dostępności danych, niezwłocznie, nie później niż w ciągu 12 godzin od jego wykrycia.
2. Zgłoszenie obejmuje – w zakresie możliwym na danym etapie – opis charakteru zdarzenia, kategorię i przybliżoną liczbę osób i rekordów, prawdopodobne konsekwencje, zastosowane lub proponowane środki zaradcze, datę i czas wykrycia oraz dane osoby kontaktowej.
3. Jeżeli pełne informacje nie są dostępne jednocześnie, Procesor przekazuje je etapami bez dalszej nieuzasadnionej zwłoki i zachowuje dowody oraz logi związane ze zdarzeniem.
4. Procesor nie zawiadamia samodzielnie osób, których dane dotyczą, ani Prezesa UODO bez polecenia Administratora, chyba że obowiązek taki bezpośrednio wynika z prawa i Procesor jest adresatem tego obowiązku.

§ 9. Audyty, informacje i dowody zgodności

1. Procesor udostępnia Administratorowi wszystkie informacje niezbędne do wykazania spełnienia obowiązków z art. 28 RODO oraz umożliwia i przyczynia się do audytów, w tym inspekcji, wykonywanych przez Administratora lub audytora przez niego upoważnionego.
2. Audyt może obejmować w szczególności kontrolę dokumentacji, upoważnień, logów, ustawień bezpieczeństwa urządzeń wykorzystywanych do realizacji Umowy, sposobu dalszego powierzenia oraz potwierdzenia usunięcia danych.
3. Administrator co do zasady zawiadomi o audycie z wyprzedzeniem co najmniej 2 dni roboczych, chyba że zachodzi incydent, uzasadnione podejrzenie naruszenia lub kontrola organu, gdy audyt może być przeprowadzony niezwłocznie.

§ 10. Transfery poza EOG

Procesor nie przekazuje danych poza Europejski Obszar Gospodarczy ani nie korzysta z usług, których użycie powoduje taki transfer, bez uprzedniej pisemnej zgody Administratora oraz zapewnienia podstawy transferu zgodnej z rozdziałem V RODO.

§ 11. Zakończenie przetwarzania

1. Po zakończeniu świadczenia usług związanych z przetwarzaniem Procesor – według decyzji Administratora – zwraca Administratorowi dane i ich kopie albo usuwa je w sposób uniemożliwiający odtworzenie, chyba że prawo nakazuje dalsze przechowywanie.
2. Obowiązek wykonuje się nie później niż w terminie 7 dni od zakończenia dostępu albo otrzymania polecenia Administratora. Procesor przekazuje pisemne potwierdzenie wykonania usunięcia lub zwrotu, wskazując zakres danych, datę i sposób wykonania.
3. Jeżeli określone dane muszą być przechowywane na podstawie prawa, Procesor izoluje je od bieżącego przetwarzania i wykorzystuje wyłącznie w celu wynikającym z tego obowiązku.

§ 12. Odpowiedzialność i relacja z Umową główną

1. Każda ze Stron ponosi odpowiedzialność na zasadach wynikających z RODO i prawa krajowego. Procesor odpowiada w szczególności za naruszenie obowiązków RODO skierowanych bezpośrednio do podmiotów przetwarzających oraz za działanie poza zgodnymi z prawem instrukcjami Administratora lub wbrew nim.
2. Naruszenie niniejszej Umowy stanowi jednocześnie naruszenie obowiązków bezpieczeństwa i ochrony danych określonych w Umowie głównej i może skutkować przewidzianymi w niej karami, rozwiązaniem Umowy i odpowiedzialnością odszkodowawczą.
3. W razie sprzeczności między niniejszą Umową a Umową główną w zakresie przetwarzania danych osobowych pierwszeństwo ma niniejsza Umowa.

§ 13. Kontakt i postanowienia końcowe

1. Kontakt do Administratora/Inspektora Ochrony Danych: Inspektor Ochrony Danych – Dariusz Klimowski, e-mail: iod@fioi.org, tel. 55 239 48 74. Zmiana danych kontaktowych IOD nie wymaga aneksu i jest skuteczna po poinformowaniu Procesora.
2. Osoba kontaktowa Procesora ds. ochrony danych i incydentów: [...], e-mail: [...], tel. [...].
3. Zmiana niniejszej Umowy wymaga formy pisemnej pod rygorem nieważności, z wyjątkiem danych kontaktowych i zmian TOMs podnoszących poziom bezpieczeństwa, uzgodnionych w formie dokumentowej.
4. W sprawach nieuregulowanych stosuje się RODO, ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych oraz przepisy Kodeksu cywilnego w zakresie zgodnym z charakterem stosunku.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej Strony.

ADMINISTRATOR	PODMIOT PRZETWARZAJĄCY
..... Starosta Sztumski	 osoba uprawniona

Załącznik nr 1 do Umowy powierzenia – minimalne środki techniczne i organizacyjne (TOMs)

Obszar	Minimalne wymaganie
Zarządzanie dostępem	Imienne konta; zasada najmniejszych uprawnień; niezwłoczne blokowanie dostępu po ustaniu potrzeby; okresowy przegląd uprawnień; zakaz kont współdzielonych.
Uwierzytelnianie	Silne hasła zgodne z wymaganiami Zamawiającego; MFA, jeżeli jest technicznie dostępne/wymagane; blokada konta po wielokrotnych nieudanych próbach.
Urządzenia końcowe	Wyłącznie urządzenia uzgodnione z Zamawiającym, przeznaczone do realizacji zadania, z legalnym i wspieranym systemem Windows 11, aktualizacjami bezpieczeństwa, aktywnym firewall i ochroną antywirusową/EDR.
Szyfrowanie	Szyfrowanie dysków urządzeń przenośnych i stacjonarnych wykorzystywanych do realizacji zadania; szyfrowane kanały komunikacji; zakaz przysyłania danych przez niezabezpieczone kanały.
RDP/VDI	Dostęp wyłącznie z zaakceptowanych stałych adresów IP i urządzeń. Zamawiający może wyłączyć kopiowanie przez schowek, mapowanie lokalnych dysków, drukarek i portów oraz lokalny zapis plików.
Nośniki i chmura	Zakaz zapisu danych na prywatnych nośnikach USB, prywatnych chmurach, prywatnych kontaktach e-mail i usługach niezaakceptowanych przez Administratora.
Logowanie i rozliczalność	Rejestrowanie logowań i istotnych operacji w zakresie zapewnianym przez system Zamawiającego; zakaz usuwania lub modyfikowania logów; współpraca przy ich zabezpieczeniu na potrzeby incydentu.
Kopie bezpieczeństwa	Przed zasileniem produkcyjnej bazy EGiB Zamawiający wykonuje lub potwierdza aktualną kopię bezpieczeństwa i dostępność procedury odtworzenia. Wykonawca nie rozpoczyna zasilenia bez takiego potwierdzenia.
Integralność danych	Zmiany w bazie wyłącznie po zaakceptowaniu dokumentacji i na polecenie Zamawiającego; obowiązek zachowania wersji historycznych i przypisanych operatów; walidacja po zasileniu.
Poufność	Imienne upoważnienia; zobowiązania do poufności; szkolenie personelu; brak dostępu osób nieupoważnionych do stanowiska pracy; automatyczna blokada ekranu.
Praca zdalna	Praca w miejscu zapewniającym ochronę przed podglądem i dostępem osób postronnych; zakaz pracy na publicznych, niezauważanych sieciach bez zaakceptowanego bezpiecznego tunelu.
Incydenty	Procedura niezwłocznego zgłaszania; maksymalnie 12 godzin od wykrycia do pierwszego zgłoszenia Administratorowi; zachowanie logów i dowodów; współpraca przy analizie i ograniczaniu skutków.
Usuwanie danych	Po zakończeniu zadania bezpieczne usunięcie danych i kopii z urządzeń Procesora oraz potwierdzenie tego faktu; wyjątek wyłącznie dla danych wymaganych prawem.
Podprocesorzy	Tylko po uprzedniej zgodzie Administratora i po nałożeniu równoważnych obowiązków; Procesor prowadzi listę zaakceptowanych podprocesorów.
Audyty	Procesor umożliwia weryfikację urządzeń i organizacji zabezpieczeń związanych z realizacją zadania w zakresie niezbędnym do potwierdzenia zgodności.