

Załącznik nr 13 do SWZ

PROJEKT UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

dotyczący postępowania OR.271.4.2026 – „Zakup usług audytu bezpieczeństwa, testów penetracyjnych, testów socjotechnicznych, SZBI oraz szkoleń dedykowanych dla Urzędu Gminy Dobra i jednostek podległych w ramach projektu Cyberbezpieczna Gmina Dobra”

zawarta pomiędzy Gminą Dobra, 34-642 Dobra 233, NIP 737-100-59-69, jako Administratorem, a, jako Podmiotem przetwarzającym.

§ 1. Przedmiot i podstawa powierzenia

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wyłącznie w zakresie i celu niezbędnym do wykonania umowy głównej, zgodnie z art. 28 rozporządzenia (UE) 2016/679 (RODO).
2. Powierzenie nie uprawnia do przetwarzania danych dla własnych celów Podmiotu przetwarzającego ani do ich wykorzystywania do trenowania, dostrajania, testowania lub zasilania modeli generatywnej sztucznej inteligencji.
3. Przetwarzanie rozpoczyna się nie wcześniej niż z dniem zawarcia niniejszej umowy i trwa wyłącznie przez okres niezbędny do wykonania i rozliczenia czynności wymagających dostępu do danych.

§ 2. Zakres, cel, rodzaj danych i osoby, których dane dotyczą

1. Cel przetwarzania: wykonanie audytów, testów socjotechnicznych, czynności związanych z SZBI, szkoleń i — w zakresie niezbędnym — testów bezpieczeństwa oraz przygotowanie raportów i dowodów wykonania usług.
2. Kategorie osób: pracownicy, współpracownicy i osoby wykonujące zadania na rzecz Administratora i jednostek objętych zamówieniem; użytkownicy systemów i usług objętych testami.
3. Kategorie danych: dane identyfikacyjne i służbowe dane kontaktowe, identyfikatory użytkowników, adresy e-mail, informacje o jednostce/komórce organizacyjnej, techniczne identyfikatory i logi niezbędne do testów, adresy IP, znaczniki czasu oraz metryki zachowania w kontrolowanych testach socjotechnicznych.
4. Bezwzględnie zabrania się pozyskiwania, przesyłania i przechowywania rzeczywistych haseł, kodów jednorazowych, tokenów MFA, kluczy dostępu, sekretów aplikacyjnych i innych danych uwierzytelniających. Formularze testowe muszą rejestrować wyłącznie zdarzenie lub metrykę próby, bez utrwalania treści wpisanej przez użytkownika.
5. Przetwarzanie szczególnych kategorii danych osobowych jest niedopuszczalne, chyba że Administrator wyda uprzednie, odrębne, udokumentowane polecenie określające podstawę prawną, zakres i zabezpieczenia.

§ 3. Udokumentowane polecenia Administratora

1. Podmiot przetwarzający przetwarza dane wyłącznie na udokumentowane polecenie Administratora, w tym w zakresie przekazywania danych do państwa trzeciego lub organizacji międzynarodowej.
2. Jeżeli Podmiot przetwarzający uzna polecenie za naruszające RODO lub inne przepisy o ochronie danych, niezwłocznie informuje o tym Administratora i wstrzymuje wykonanie polecenia w zakresie budzącym wątpliwości do czasu uzyskania stanowiska Administratora.

§ 4. Poufność i personel

1. Do danych mogą mieć dostęp wyłącznie osoby upoważnione, których dostęp jest niezbędny do wykonania powierzonych czynności.
2. Podmiot przetwarzający zapewnia, że osoby te zobowiązały się do zachowania poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
3. Dostęp są nadawane zgodnie z zasadą minimalnych uprawnień i niezwłocznie odbierane po ustaniu potrzeby dostępu.

§ 5. Środki bezpieczeństwa

1. Podmiot przetwarzający stosuje środki odpowiadające art. 32 RODO oraz ryzyku wynikającemu z charakteru zamówienia, w tym co najmniej: szyfrowanie transmisji danych, szyfrowanie nośników lub repozytoriów zawierających dane, uwierzytelnianie wieloskładnikowe do systemów przechowujących dane, ograniczenie dostępu, rejestrowanie operacji administracyjnych oraz ochronę przed nieuprawnionym kopiowaniem danych.
2. Dane Administratora nie mogą być przechowywane w prywatnych kontach pocztowych, prywatnych chmurach, komunikatorach konsumenckich ani w systemach generatywnej AI.
3. Podmiot przetwarzający utrzymuje logiczne oddzielenie danych Administratora od danych innych klientów.
4. Kopie robocze i eksporty danych ogranicza się do niezbędnego minimum. Po odbiorze odpowiedniego etapu dane robocze usuwa się bez zbędnej zwłoki, nie później niż 14 dni po odbiorze końcowym, chyba że Administrator poleci wcześniejsze usunięcie albo przepis prawa wymaga dłuższego przechowania.

§ 6. Testy socjotechniczne

1. Testy prowadzone są wyłącznie według scenariuszy i grup odbiorców zatwierdzonych przez Administratora.
2. Dopuszczalne jest rejestrowanie takich zdarzeń jak dostarczenie/otwarcie wiadomości, kliknięcie łącza, wejście na stronę testową, pobranie bezpiecznego załącznika testowego, podjęcie próby wpisania danych oraz zgłoszenie wiadomości jako podejrzaney.
3. System techniczny użyty do testu musi być skonfigurowany tak, aby wartość wpisana w pole symulujące hasło lub inny sekret nie była przesyłana do serwera ani zapisywana w logach; może zostać utrwalona wyłącznie informacja, że podjęto próbę wpisania danych.

4. Raportowanie imienne jest dopuszczalne wyłącznie, jeżeli Administrator wyraźnie zleci taką formę i posiada podstawę prawną; domyślnie wyniki przedstawia się w sposób zagregowany lub pseudonimizowany.

§ 7. Dalsze powierzenie

1. Dalsze powierzenie danych wymaga uprzedniej szczegółowej pisemnej zgody Administratora. Nie stanowi zgody samo dopuszczenie podwykonawstwa w umowie głównej.

2. Podmiot przetwarzający przedstawi Administratorowi dane dalszego podmiotu przetwarzającego, zakres i miejsce przetwarzania oraz stosowane zabezpieczenia.

3. Umowa z dalszym podmiotem przetwarzającym musi nakładać co najmniej te same obowiązki ochrony danych jak niniejsza umowa. Podmiot przetwarzający odpowiada wobec Administratora za działania dalszego podmiotu przetwarzającego.

§ 8. Naruszenia ochrony danych

1. Podmiot przetwarzający zgłasza Administratorowi każde podejrzenie lub stwierdzone naruszenie ochrony danych bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od jego stwierdzenia.

2. Zgłoszenie zawiera co najmniej: opis zdarzenia, czas jego wykrycia i wystąpienia (jeżeli znany), kategorie danych i osób, szacunkową skalę, możliwe konsekwencje, zastosowane lub proponowane działania ograniczające skutki oraz dane osoby kontaktowej.

3. Podmiot przetwarzający zabezpiecza materiał dowodowy i współpracuje z Administratorem przy realizacji obowiązków z art. 33 i 34 RODO.

§ 9. Prawa osób, DPIA i współpraca

1. Podmiot przetwarzający, z uwzględnieniem charakteru przetwarzania, pomaga Administratorowi w realizacji praw osób, których dane dotyczą, oraz obowiązków z art. 32–36 RODO.

2. Żądania osób dotyczące danych Administratora są niezwłocznie przekazywane Administratorowi i nie są samodzielnie rozpatrywane, chyba że Administrator wyda inne polecenie.

§ 10. Kontrola i audyt

1. Podmiot przetwarzający udostępnia Administratorowi informacje niezbędne do wykazania spełnienia obowiązków z art. 28 RODO oraz umożliwia audyty i kontrole, w tym inspekcje, prowadzone przez Administratora lub upoważnionego audytora.

2. Podmiot przetwarzający niezwłocznie usuwa stwierdzone niezgodności w terminie uzgodnionym z Administratorem, a w przypadku ryzyka wysokiego — niezwłocznie.

§ 11. Zakończenie przetwarzania

1. Po zakończeniu świadczenia usług Podmiot przetwarzający, według decyzji Administratora, usuwa albo zwraca wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo krajowe nakazuje ich przechowywanie.
2. Usunięcie danych jest potwierdzane Administratorowi w formie dokumentowej. Jeżeli usunięcie z kopii zapasowych nie jest technicznie możliwe natychmiast, dane pozostają odseparowane, nie są dalej wykorzystywane i są usuwane zgodnie z cyklem retencji kopii zapasowych.

§ 12. Postanowienia końcowe

1. W sprawach nieuregulowanych stosuje się RODO, ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych oraz postanowienia umowy głównej.
2. W razie sprzeczności w zakresie ochrony danych pierwszeństwo mają postanowienia niniejszej umowy oraz bezwzględnie obowiązujące przepisy prawa.
3. Zmiana niniejszej umowy wymaga formy dokumentowej, chyba że przepisy lub umowa główna wymagają formy surowszej.

ADMINISTRATOR: PODMIOT PRZETWARZAJĄCY:
.....