Załącznik nr 6 do zaproszenia do złożenia oferty

Projekt umowy powierzenia danych osobowych

Numer postępowania ADM.016.2026.10.AS

Kosakowo, 9 listopada 2026 r.

Zawarta dnia ..... pomiędzy Przedsiębiorstwem Usług Komunalnych „PEKO” sp. z o.o. w Kosakowie, ul. Chrzanowskiego 44, 81-198 Kosakowo, NIP 9581154984, REGON 191416896, KRS 0000038875, dalej „Administrator”, reprezentowanym przez ....., a ....., NIP ....., reprezentowanym przez ....., dalej „Podmiot przetwarzający”, w związku z umową audytu nr ..... . Umowę zawiera się przed dostępem, jeżeli czynności stanowią przetwarzanie danych w imieniu PEKO. Strony uzupełniają wykaz faktycznie udostępnianych systemów i zaakceptowanych dalszych podmiotów przed dostępem.

1 Zakres cel i czas

Administrator powierza dane wyłącznie w celu wykonania audytu, bezpiecznych testów, analizy dowodów i sporządzenia wyników zgodnie z umową główną, OPZ i poleceniami. Przetwarzanie trwa przez wykonywanie zadań i uzgodniony okres zwrotu lub usunięcia. Nie obejmuje własnego marketingu, profilowania, innych analiz ani trenowania AI.

Element	Zakres
Osoby	Pracownicy, współpracownicy, przedstawiciele dostawców oraz inne osoby, których niezbędne dane znajdują się w badanej dokumentacji lub systemach.
Dane	Dane identyfikacyjne i kontakty służbowe, role i uprawnienia, identyfikatory kont, niezbędne logi i metadane techniczne, dokumentacja incydentów, faktyczny udział i wyniki szkoleń. Konkretne systemy i dokumenty: ..... .
Czynności	Dostęp i odczyt, porządkowanie i analiza, minimalne dowody, zapis wyników, bezpieczne przekazanie PEKO, korekta, zwrot i usunięcie.
Minimalizacja	Nie pobiera się całych baz ani kopii produkcyjnych bez konieczności i odrębnego polecenia. Nie gromadzi się danych zdrowotnych, prywatnej korespondencji, haseł, MFA ani tokenów w dowodach. Przypadkowo ujawnione dane zabezpiecza się i zgłasza, ograniczając ich dalsze przetwarzanie.

2 Polecenia i personel

Podmiot działa wyłącznie na udokumentowane polecenia Administratora wynikające z dokumentów umowy i późniejszych zgodnych poleceń. Jeżeli polecenie narusza RODO, niezwłocznie informuje Administratora. Jeśli przetwarzanie nakazuje prawo, informuje o obowiązku przed działaniem, chyba że prawo tego zabrania.

Dostęp otrzymują wyłącznie imiennie upoważnione, zobowiązane do poufności i odpowiednio przeszkolone osoby. Uprawnienia są minimalne, czasowe i rozliczalne. Podmiot zapewnia oddzielenie danych różnych klientów i zakaz używania danych do własnych celów. Kontakty i wyniki udostępnia wyłącznie uprawnionym odbiorcom.

3 Bezpieczeństwo i lokalizacja

Podmiot wdraża środki odpowiednie do ryzyka z art. 32 RODO: szyfrowaną transmisję i przechowywanie, oddzielne przekazywanie haseł, indywidualne konta, MFA dla dostępów uprzywilejowanych, ograniczenie i logowanie dostępów, bezpieczne i aktualne narzędzia, zabezpieczenie urządzeń, kopie i możliwość odtworzenia oraz okresową ocenę środków. Dowody anonimizuje lub pseudonimizuje, gdy identyfikacja nie jest konieczna. Wyniki i klucze nie mogą być przekazywane jednym niezabezpieczonym kanałem.

Dane i kopie przechowuje się w UE. Zdalny dostęp lub przekazanie z państwa trzeciego wymaga uprzedniej pisemnej zgody Administratora i spełnienia rozdziału V RODO, z zachowaniem lokalizacji przechowywania w UE. Wybór globalnego dostawcy nie jest zgodą na transfer.

4 Dalsze powierzenie

Dalszy podmiot wymaga uprzedniej szczegółowej pisemnej zgody Administratora. Podmiot nakłada na niego co najmniej te same obowiązki i odpowiada za jego działanie. Wykaz obejmuje także dostawcę chmury lub narzędzi, jeżeli otrzymuje dane w imieniu PEKO. Zmiana wymaga nowej uprzedniej zgody. Brak wpisu oznacza brak zgody, a nie możliwość swobodnego dalszego powierzenia.

Podmiot i usługa	Dane i zakres	Lokalizacja i dostęp	Zgoda PEKO

5 Naruszenia pomoc i kontrola

Naruszenie danych zgłasza się bez zbędnej zwłoki, najpóźniej w 24 godziny od stwierdzenia, na odo@pukpeko.pl i do koordynatora PEKO. Pierwsze zgłoszenie nie może czekać na komplet ustaleń. Obejmuje czas, charakter, dane i osoby w znanym zakresie, możliwe skutki, działania i kontakt. Informacje uzupełnia się na bieżąco, zabezpieczając dowody. Dla krytycznej podatności lub trwającego naruszenia obowiązuje krótszy termin 4 godzin z OPZ.

Podmiot niezwłocznie przekazuje żądania osób i pomaga Administratorowi przy realizacji praw oraz obowiązków z art. 32–36 RODO, w tym ocenie skutków, analizie naruszenia i zawiadomieniach. Nie odpowiada osobom ani organowi w imieniu Administratora bez podstawy lub polecenia, z zachowaniem własnych ustawowych obowiązków.

Podmiot udostępnia informacje wykazujące zgodność i umożliwia audyty lub inspekcje Administratora albo upoważnionego kontrolującego. Zwykłą kontrolę uzgadnia się z wyprzedzeniem 3 dni roboczych; przy naruszeniu lub żądaniu organu działa się niezwłocznie. Kontrola chroni dane innych klientów i nie ogranicza uprawnień organów. Zwykła pomoc i weryfikacja są objęte ceną umowy głównej.

6 Zakończenie i odpowiedzialność

Po wykonaniu Podmiot przekaże Administratorowi pełne wyniki i niezbędne dowody. Następnie, według decyzji Administratora, zwróci lub usunie dane i kopie robocze w 30 dni. Niedostępne do zwykłego użycia kopie bezpieczeństwa usuwa najpóźniej w 90 dni; do tego czasu są chronione i niewykorzystywane. Odtworzenie kopii powoduje obowiązek ponownego wykonania zleconego usunięcia. Zamknięcie dostępów potwierdza przy zakończeniu prac.

Podmiot pisemnie potwierdzi zwrot lub usunięcie. Jeśli prawo nakazuje zachowanie części danych, wskaże podstawę, zakres i termin, utrzymując ochronę i zakaz własnego wykorzystania. Dane przetwarzane na odrębnej podstawie jako samodzielny administrator wymagają uprzedniej przejrzystej informacji i rozdzielenia od powierzenia. Umowa nie zmienia ustawowych praw ani odpowiedzialności z art. 82 RODO. Zmiany wymagają formy pisemnej lub elektronicznej z podpisami kwalifikowanymi.

Kontakt Podmiotu w sprawach danych: .....

Opis zastosowanych zabezpieczeń i lokalizacji — uzupełniony przed dostępem załącznik z datą: .....

Administrator: ..... Podmiot przetwarzający: .....