

Opis przedmiotu zamówienia (OPZ)

W ramach realizacji przedmiotu Umowy Wykonawca pełni funkcję Inspektora Ochrony Danych (IOD) i świadczy na rzecz Zamawiającego oraz Jednostek kompleksowe usługi doradcze, nadzorcze, szkoleniowe i kontrolne w zakresie ochrony danych osobowych, zgodnie z RODO, ustawą o ochronie danych osobowych oraz innymi przepisami mającymi zastosowanie do działalności Zamawiającego i Jednostek. Usługa obejmuje w szczególności:

I. Nadzór nad zgodnością przetwarzania danych osobowych

- 1) Monitorowanie przestrzegania przepisów RODO, ustawy o ochronie danych osobowych oraz procedur obowiązujących u Zamawiającego i w Jednostkach.
- 2) Sprawdzanie zgodności procesów przetwarzania danych osobowych z obowiązującymi przepisami prawa i regulacjami wewnętrznymi.
- 3) Identyfikację procesów przetwarzania danych osobowych, kategorii danych, źródeł ich pozyskiwania, odbiorców danych, podstaw prawnych przetwarzania oraz przepływu informacji wewnątrz i na zewnątrz jednostki.
- 4) Weryfikację stosowanych środków organizacyjnych i technicznych służących ochronie danych osobowych.
- 5) Analizę rozwiązań informatycznych wykorzystywanych do przetwarzania danych osobowych pod kątem zgodności z art. 24, 25 i 32 RODO.
- 6) Wydawanie zaleceń oraz rekomendacji dotyczących poprawy poziomu ochrony danych osobowych.

II. Dokumentacja ochrony danych

- 1) Weryfikację kompletności i aktualności dokumentacji ochrony danych osobowych.
- 2) Opracowywanie projektów dokumentów, procedur i regulacji wewnętrznych związanych z ochroną danych osobowych oraz opiniowanie dokumentów przygotowanych przez Zamawiającego i Jednostki.
- 3) Bieżące rekomendowanie zmian w dokumentacji w związku ze zmianami przepisów prawa, organizacji pracy lub procesów przetwarzania.
- 4) Wsparcie Administratora w prowadzeniu:
 - rejestru czynności przetwarzania,
 - rejestru kategorii czynności przetwarzania,
 - rejestru naruszeń ochrony danych osobowych,
 - ewidencji upoważnień oraz
 - ewidencji umów powierzenia przetwarzania danych.
- 5) Coroczny przegląd dokumentacji ochrony danych osobowych, zakończony sporządzeniem pisemnych rekomendacji.

III. Analiza ryzyka i ocena skutków

- 1) Przeprowadzanie analiz ryzyka związanych z przetwarzaniem danych osobowych nie rzadziej niż raz w roku lub każdorazowo w przypadku istotnych zmian organizacyjnych lub technologicznych.
- 2) Identyfikację zagrożeń i podatności związanych z przetwarzaniem danych osobowych.
- 3) Doradzanie w zakresie oceny skutków dla ochrony danych (DPIA), opiniowanie przeprowadzonych ocen oraz monitorowanie realizacji wynikających z nich zaleceń.
- 4) Opracowywanie rekomendacji ograniczających ryzyko naruszenia praw i wolności osób, których dane dotyczą.

IV. Naruszenia ochrony danych osobowych

- 1) Przyjmowanie zgłoszeń dotyczących incydentów i naruszeń ochrony danych osobowych.
- 2) Analizowanie naruszeń pod kątem obowiązku ich zgłoszenia organowi nadzorczemu oraz osobom, których dane dotyczą.
- 3) Przygotowywanie projektów zgłoszeń naruszeń ochrony danych do Prezesa UODO oraz projektów zawiadomień osób, których dane dotyczą.
- 4) Prowadzenie i aktualizację rejestru naruszeń ochrony danych osobowych.
- 5) Opracowywanie rekomendacji działań korygujących i zapobiegawczych po wystąpieniu naruszeń.
- 6) Wykonywanie czynności związanych ze zgłoszeniem naruszenia do organu nadzorczego, w przypadku odrębnego upoważnienia udzielonego przez Administratora.

V. Doradztwo i bieżące wsparcie

- 1) Informowanie Administratora, osób upoważnionych do przetwarzania danych oraz kierownictwa jednostki o obowiązkach wynikających z przepisów o ochronie danych osobowych.
- 2) Udzielanie bieżących konsultacji i opinii w sprawach związanych z ochroną danych osobowych.
- 3) Opiniowanie umów powierzenia przetwarzania danych osobowych oraz innych dokumentów zawierających postanowienia dotyczące danych osobowych.
- 4) Opiniowanie klauzul informacyjnych i innych dokumentów realizujących obowiązki informacyjne.
- 5) Doradzanie przy wdrażaniu nowych procesów, usług, aplikacji oraz systemów informatycznych.
- 6) Współpracę z administratorem systemów informatycznych oraz osobami odpowiedzialnymi za cyberbezpieczeństwo.
- 7) Uczestnictwo w planowaniu i wdrażaniu rozwiązań organizacyjnych i technologicznych wpływających na procesy przetwarzania danych osobowych.

VI. Szkolenia i podnoszenie świadomości

- 1) Przeprowadzanie co najmniej jednego szkolenia okresowego rocznie dla pracowników Zamawiającego i każdej z Jednostek.
- 2) Przeprowadzanie szkoleń wstępnych dla nowo zatrudnionych pracowników w terminie uzgodnionym z właściwą Jednostką.
- 3) Opracowywanie i aktualizację materiałów szkoleniowych.

- 4) Dokumentowanie przeprowadzonych szkoleń, w tym list obecności lub innych dowodów uczestnictwa.
- 5) Prowadzenie działań podnoszących świadomość pracowników w zakresie ochrony danych osobowych i cyberbezpieczeństwa.

VII. Współpraca z organami nadzorczymi kontrolnymi

- 1) Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych.
- 2) Współpracę z organem nadzorczym we wszystkich sprawach związanych z ochroną danych osobowych.
- 3) Wspieranie Zamawiającego i Jednostek podczas kontroli, czynności sprawdzających oraz postępowań prowadzonych przez:
 - Prezesa UODO,
 - Najwyższą Izbę Kontroli,
 - Regionalną Izbę Obrachunkową oraz
 - inne uprawnione organy lub podmioty kontrolne bądź audytowe, w tym przygotowywanie projektów wyjaśnień, odpowiedzi oraz informacji wymaganych przez te organy.

VIII. AUDYTY I CZYNNOŚCI KONTROLNE

- 1) Wykonawca przeprowadza co najmniej jeden kompleksowy audyt zgodności z przepisami o ochronie danych osobowych w każdej Jednostce w każdym roku obowiązywania Umowy.
- 2) Audyt kończy się sporządzeniem raportu zawierającego co najmniej:
 - opis przeprowadzonych czynności,
 - stwierdzone niezgodności, ocenę poziomu ryzyka,
 - rekomendacje działań naprawczych oraz
 - proponowane terminy ich realizacji.
- 3) Na wniosek Kierownika Jednostki Wykonawca przeprowadza audyty doraźne lub problemowe.

IX. Raportowanie

- 1) Wykonawca sporządza i przekazuje Kierownikowi Jednostki raport kwartalny obejmujący:
 - wykaz wykonanych czynności,
 - ocenę stanu zgodności z przepisami ochrony danych osobowych,
 - wykaz stwierdzonych niezgodności,
 - status realizacji wcześniejszych zaleceń oraz
 - rekomendacje działań naprawczych.
- 2) Wykonawca prowadzi rejestr wydanych rekomendacji i zaleceń.
- 3) Wykonawca sporządza coroczne sprawozdanie z działalności IOD, przedstawiane Kierownikowi Jednostki, a w razie rozwiązania Umowy przed terminem – wraz z ostatnią płatnością.

X. Informowanie o ryzykach

- 1) W przypadku stwierdzenia niezgodności, naruszenia lub istotnego ryzyka naruszenia przepisów o ochronie danych osobowych Wykonawca sporządza pisemną informację zawierającą:
 - opis stanu faktycznego,
 - ocenę ryzyka,
 - wskazanie naruszonych lub zagrożonych przepisów oraz
 - rekomendowane działania naprawcze.
- 2) Informacja, o której mowa powyżej, przekazywana jest Kierownikowi Jednostki niezwłocznie, nie później niż w terminie 7 dni od dnia stwierdzenia nieprawidłowości.

XI. Standard świadczenia usługi

- 1) Wykonawca zapewnia możliwość kontaktu telefonicznego oraz elektronicznego w dni robocze.
- 2) Czas reakcji Wykonawcy wynosi:
 - do 4 godzin roboczych w przypadku zgłoszenia naruszenia ochrony danych osobowych,
 - do 1 dnia roboczego w przypadku incydentu wysokiego ryzyka oraz
 - do 2 dni roboczych w pozostałych sprawach.
- 3) Wykonawca realizuje wizyty robocze w siedzibie każdej Jednostki nie rzadziej niż raz na kwartał.
- 4) Wykonawca przedkłada roczny plan działań IOD na kolejny rok kalendarzowy.