Przedmiot zamówienia obejmuje:

- **dokonanie oceny w zakresie spełniania przez Zamawiającego obowiązków związanych z przetwarzaniem danych osobowych, które wynikają z obowiązujących przepisów prawa, w szczególności z 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, zwanego dalej: „RODO";**

oraz

- **pełnienie na rzecz Zamawiającego funkcji Inspektora Ochrony Danych przez okres 12 miesięcy od dnia zawarcia umowy.**

W ramach zamówienia Wykonawca zobowiązany jest do kompleksowej obsługi Zamawiającego w zakresie ochrony danych osobowych, która będzie obejmowała wykonywanie następujących czynności:

1. **Analiza, weryfikacja i dostosowanie działań Zamawiającego w zakresie ochrony danych osobowych**, w szczególności:

   1) Ocena spełnienia przez Zamawiającego obowiązków wynikających z obowiązujących przepisów prawa w zakresie przetwarzania danych osobowych, a także zgodności dokumentacji, procedur i sposobu funkcjonowania Zamawiającego z wytycznymi, wskazówkami i poradnikami właściwych urzędów (np. Urzędu Ochrony Danych Osobowych, Grupy Roboczej ds. art. 29). Zakres obowiązków Wykonawcy obejmuje w szczególności analizę dokumentacji i sposobu funkcjonowania Zamawiającego, w celu sprawdzenia, czy Zamawiający wypełnia obowiązki wynikające z obowiązujących przepisów prawa (RODO, przepisy krajowe), jak również czy jego dokumentacja regulująca przetwarzanie danych osobowych oraz sposób postępowania pozostaje w zgodzie z wytycznymi, poradnikami, zaleceniami i aktualnymi rozstrzygnięciami organu nadzoru, w szczególności tymi, które odnoszą się do przetwarzania danych osobowych przez organy administracji publicznej, na przykład:

      a) **w zakresie wymagań technicznych** – badanie zabezpieczenia fizycznego, bezpieczeństwa systemów informatycznych wykorzystywanych do przetwarzania danych osobowych, zabezpieczenia teletransmisji danych,

      b) **w zakresie wymagań organizacyjnych** – weryfikacja procedur i prawidłowości zarządzania incydentami naruszenia bezpieczeństwa, analiza zasad dostępu pracowników do systemów, opracowanie metodologii i formularza analizy ryzyka dla planowanych operacji przetwarzania danych osobowych, weryfikacja wiedzy i poziomu świadomości pracowników w zakresie ochrony danych osobowych, analiza danych podlegających retencji i niszczeniu oraz terminów, w jakich to jest dokonywane, analiza metod usuwania danych i ich skuteczności,

      c) **w zakresie wymagań formalno-prawnych** – ocena spełniania przez Zamawiającego obowiązków informacyjnych i obowiązków związanych z uprawnieniami osób, których dane przetwarza Zamawiający (art. 15-22 RODO), weryfikacja poprawności funkcjonujących u Zamawiającego klauzul informacyjnych oraz klauzul o zgodzie na przetwarzanie danych, a także ocena wypełnienia przez Zamawiającego obowiązków związanych z powierzeniem przetwarzania danych (zarówno gdy Zamawiający powierza przetwarzanie danych osobom trzecim, jak i gdy Zamawiający działa jako podmiot

przetwarzający) – weryfikacja adekwatności, kompletności i prawidłowości umów/klauzul o powierzeniu przetwarzania danych;

2) **Przedstawienie rezultatów działań, o których mowa w pkt 1 w formie sprawozdania**, obejmującego ocenę i analizę stosowanych rozwiązań, opis stwierdzonych uchybień i nieprawidłowości oraz zaproponowanie rozwiązań **pozwalających** na ich usunięcie;

3) **Weryfikacja i dostosowanie istniejącej dokumentacji**, w tym procedur dotyczących bezpieczeństwa informacji oraz ochrony danych osobowych u **Zamawiającego**, w celu zapewnienia jej zgodności z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych (w szczególności RODO i ustawą 10 maja 2018 o ochronie danych osobowych), a także z wytycznymi, poradnikami, zaleceniami i aktualnymi rozstrzygnięciami organu nadzoru, a w szczególności tymi, które odnoszą się do przetwarzania danych osobowych przez organy administracji publicznej;

4) **Opracowanie brakującej niezbędnej dokumentacji przetwarzania danych osobowych** (np. tej, która w ocenie Wykonawcy powinna zostać wprowadzona przez Zamawiającego, a której obecnie on nie posiada), w tym szczegółowych procedur, w tym procedury retencji danych, niszczenia danych z nośników papierowych oraz danych z nośników elektronicznych, procedury postępowania w razie wystąpienia incydentu ochrony danych osobowych.

2. **Wykonywanie funkcji Inspektora Ochrony Danych** przez okres 12 miesięcy od dnia podpisania umowy (w tym obecność w siedzibie Zamawiającego co najmniej przez 8 h w tygodniu – na zasadach określonych w umowie), przez co rozumie się w szczególności:

1) Informowanie administratora danych osobowych (lub podmiotu przetwarzającego) oraz pracowników Zamawiającego, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach wynikających z RODO oraz innych przepisów o ochronie danych osobowych i doradzanie im w tym zakresie;

2) Monitorowanie przestrzegania przepisów o ochronie danych osobowych u Zamawiającego poprzez wykonywanie audytów, sprawozdań i kontroli, zgodnie z przyjętymi przez administratora danych osobowych, planami w tym zakresie;

3) Udzielanie, na żądanie Zamawiającego, zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania, zgodnie z art. 35 RODO;

4) Nadzorowanie opracowywania, tworzenia i aktualizacji regulacji wewnętrznych dotyczących ochrony danych osobowych;

5) Opiniowanie stosowanych u Zamawiającego klauzul umownych, projektów umów powierzania przetwarzania danych osobowych, projektów procedur i regulacji wewnętrznych – w zakresie, w jakim mogą one dotyczyć przetwarzania danych osobowych i ich ochrony;

6) Opracowywanie opinii/wystąpień dla administratora danych osobowych, w zakresie realizowanych procesów, związanych z przetwarzaniem danych;

7) Udzielanie niezbędnych zaleceń w zakresie ochrony danych osobowych oraz monitorowanie ich wykonania;

8) Przeprowadzanie szkoleń dla pracowników Zamawiającego w zakresie ochrony danych osobowych w rozmiarze co najmniej 1 cyklu szkoleniowego w ciągu roku, szkoleń dla osób nowozatrudnionych oraz szkoleń w zależności od potrzeb zgłaszanych przez Zamawiającego;

9) Współpraca z organem nadzorczym ds. ochrony danych osobowych;

10) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami;

11) Prowadzenie dokumentacji przetwarzania danych osobowych, w tym prowadzenie i aktualizacja:

a) rejestru czynności przetwarzania danych osobowych,

b) rejestru kategorii przetwarzania danych osobowych,

c) rejestru upoważnień do przetwarzania danych osobowych,

d) rejestru umów powierzenia przetwarzania danych osobowych,

e) rejestru naruszeń przetwarzania danych osobowych;

12) Prowadzenie oceny ryzyka wynikającego z operacji przetwarzania danych osobowych

13) Prowadzenie oceny skutków dla ochrony danych (DPIA);

14) Rozpatrywanie zapytań i skarg osób, których dane dotyczą oraz obsługa dedykowanego adresu poczty elektronicznej Zamawiającego, przeznaczonego do załatwiania spraw związanych z przetwarzaniem danych osobowych przez Zamawiającego;

15) Rozpatrywanie wniosków o wydanie upoważnień do przetwarzania danych, uczestniczenie w procesie wydawania tych upoważnień przez administratora;

16) Zgłoszenia naruszeń oraz przeprowadzanie wewnętrznych postępowań wyjaśniających w przypadku powstałych naruszeń przepisów o ochronie danych osobowych oraz ich ewidencjonowanie;

17) Doradztwo Zamawiającemu i jego reprezentacja w toku postępowań kontrolnych, w tym bieżące wsparcie w przypadku przeprowadzania kontroli przez organ nadzoru oraz wsparcie Zamawiającego we wdrażaniu ewentualnych zaleceń pokontrolnych (opracowanie propozycji rozwiązań zidentyfikowanych nieprawidłowości itp.);

18) Nadzór nad procesem powierzania przetwarzania danych osobowych zewnętrznym podmiotom.

19) Udzielanie odpowiedzi na wszelkie pytania lub wątpliwości związane z ochroną danych osobowych m.in. poprzez:

a) spotkania w siedzibie Zamawiającego,

b) konsultacje mailowe i telefoniczne z Zamawiającym i jego pracownikami,

c) monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych,

d) kontrolę archiwizacji dokumentów zawierających dane osobowe,

e) współpracę z działem IT Zamawiającego w zakresie tych obszarów, które wiążą się z ochroną danych osobowych,

f) wykonywanie innych czynności niewymienionych wyżej, a do których realizacji Zamawiający będzie zobowiązany na mocy obowiązujących przepisów w tym zakresie;

20) Monitorowanie zmian w prawie w zakresie istotnym z punktu widzenia przetwarzania danych osobowych przez Zamawiającego oraz w orzecznictwie sądów i rozstrzygnięciach organu nadzoru – informowanie Zamawiającego z odpowiednim wyprzedzeniem o zmianach w prawie, a także niezwłoczne

informowanie o orzeczeniach i rozstrzygnięciach z zakresu ochrony danych osobowych i ich skutku dla przetwarzania danych przez Zamawiającego, w tym o konieczności dokonania zmiany w wewnętrznych procedurach Zamawiającego lub w praktyce jego funkcjonowania.