Załącznik nr 1 do umowy
nr 780/DIM/BSU/2017

Opis obowiązków

1. Usługa przejęcia obowiązków Administratora Bezpieczeństwa Informacji obejmuje wykonywanie u Zamawiającego m. in. następujących zadań:
   1.1. bieżące monitorowanie wypełniania przez Zamawiającego obowiązków prawnych dotyczących wprowadzenia i utrzymywania na wymaganym prawem poziomie środków technicznych i organizacyjnych służących zabezpieczeniu danych osobowych, w szczególności zabezpieczeniu danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem, zniszczeniem, zmianą, utratą oraz przetwarzaniem z naruszeniem przepisów prawa;
   1.2. przeprowadzenie corocznego audytu podsumowującego wykonywanie u Zamawiającego zadań wynikających z przepisów o ochronie danych osobowych, z uwzględnieniem specyfiki prowadzonej działalności. Audyt jest każdorazowo zakończony notatką zawierającą: zakres i rodzaje badanych dokumentów lub nośników, obszarów u Zamawiającego, w których został przeprowadzony, analizę prawną badanych zagadnień oraz zalecenia i propozycje konkretnych rozwiązań;
   1.3. opracowywanie oraz aktualizacja polityki bezpieczeństwa, instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe, umów o powierzenie przetwarzania danych osobowych, zawieranych przez Zamawiającego w ramach prowadzonej działalności gospodarczej, wzorów upoważnień do przetwarzania danych osobowych nadawanych na podstawie art. 37 ustawy o ochronie danych osobowych, wniosków o udostępnienie danych, oraz nadzór nad doskonaleniem procesów ochrony danych osobowych w związku ze zmianami organizacyjnymi u Zamawiającego lub zmianami przepisów prawa;
   1.4. opracowywanie wniosków rejestracyjnych lub aktualizacyjnych zgłaszanych do GIODO, w przypadku zaistnienia takiego wymogu;
   1.5. nadzór nad realizacją, pod względem merytorycznym i terminowym, zaleceń będących wynikiem przeprowadzanych audytów mających na celu dostosowanie procesów biznesowych związanych z przetwarzaniem danych osobowych oraz systemów informatycznych służących do przetwarzania danych osobowych do obowiązujących wymagań prawnych;
   1.6. pomoc i reprezentacja profesjonalnego pełnomocnika (adwokata lub radcy prawnego) w kontaktach z GIODO:

1.6.1. konsultowanie odpowiedzi na pisma GIODO,
1.6.2. pomoc w przygotowaniu do kontroli GIODO i reprezentacja Zamawiającego w przypadku kontroli,
1.6.3. sporządzanie pytań kierowanych w imieniu Zamawiającego do GIODO w sprawach związanych z jej działalnością w obszarze przetwarzania danych osobowych;
1.7. reprezentacja Zamawiającego przez profesjonalnego pełnomocnika (adwokata lub radcy prawnego) w postępowaniu odwoławczym, zainicjowanym postępowaniem przed GIODO;
1.8. reprezentacja Zamawiającego przez profesjonalnego pełnomocnika (adwokata lub radcy prawnego) w postępowaniach sądowych w przedmiocie naruszenia przepisów o ochronie danych osobowych;
1.9. pomoc w sytuacji wystąpienia incydentów naruszenia ochrony danych osobowych, w tym:
1.9.1. analiza sytuacji naruszenia ochrony danych osobowych w systemie informatycznym lub naruszenia danych osobowych przetwarzanych w sposób tradycyjny,
1.9.2. rekomendowanie zmian mających na celu minimalizację ryzyka wystąpienia sytuacji naruszenia ochrony danych;
1.10. przygotowywanie, przy współpracy z Zamawiającym, wszystkich procedur niezbędnych z uwagi na przepisy o ochronie danych osobowych (m.in. procedura archiwizacji, procedura udostępniania danych, procedura monitoringu pracowników, etc.);
1.11. bieżące konsultacje dla pracowników lub współpracowników Zamawiającego w zakresie ochrony danych osobowych, świadczone w ramach:
1.11.1. dyżurów w siedzibie Zamawiającego – pakiet godzin w liczbie minimum 5 godzin w miesiącu,
1.11.2. dyspozycyjności telefonicznej i elektronicznej w godzinach pracy (8:00-18:00);
1.12. szkolenia dla pracowników i współpracowników z zakresu przyjętych u Zamawiającego zasad przetwarzania danych osobowych - wstępne oraz cykliczne, w siedzibie Zamawiającego, w ramach wspomnianych w punkcie 1.11.1 pakietów godzin:
1.12.1. szkolenie wstępne w wymiarze 4 godzin w ciągu jednego dnia,
1.12.2. szkolenia cykliczne – przynajmniej raz na sześć miesięcy w wymiarze 4 godzin w ciągu jednego dnia.

2. Przeprowadzenie szczegółowego audytu bezpieczeństwa informacji, prowadzącego do ustalenia wszelkich okoliczności przetwarzania danych osobowych, pozwalającego następnie na wykonanie zadań, o których mowa w podpunktach poniżej:
   2.1. świadczenie kompleksowej obsługi prawnej w sprawach związanych z ochroną danych osobowych, w szczególności:
      2.1.1. przygotowywanie umów powierzenia danych osobowych,
      2.1.2. przygotowywanie regulaminów, klauzul zgód i innych dokumentów,
      2.1.3. uczestniczenie w negocjacjach,
      2.1.4. konsultowanie odpowiedzi na zapytania i pisma GIODO, sporządzanie zapytań prawnych do GIODO,
      2.1.5. przygotowywanie odpowiedzi dla podmiotów danych realizujących swoje uprawnienia wynikającej z ustawy;
   2.2. wdrożenie RODO u Zamawiającego do dnia 25 maja 2018 r. w szczególności poprzez:
      2.2.1. przygotowanie procedury dokonywania oceny skutków dla ochrony danych osobowych,
      2.2.2. przygotowanie procedury mającej obowiązywać w zakresie privacy by design, privacy by default,
      2.2.3. przygotowanie procedury notyfikacji naruszeń do organu nadzorczego oraz do podmiotu danych,
      2.2.4. przygotowanie procedur w zakresie sposobu realizacji praw pomiotów danych określonych w RODO, w szczególności w jaki sposób powinno odbywać się realizowanie prawa do przenoszenia danych, prawa do ograniczenia przetwarzania, prawo do bycia zapomnianym i inne,
      2.2.5. dokonanie analizy podstaw przetwarzania danych osobowych w kontekście RODO oraz przygotowanie nowych klauzul informacyjnych oraz treści zgód,
      2.2.6. dokonanie analizy podstaw oraz prawidłowości dokonywania transferu danych poza obszar EOG,
      2.2.7. przygotowanie nowych polityk dotyczących ochrony danych osobowych spełniających wymagania RODO, w tym rejestru czynności przetwarzania oraz innych wymaganych przez RODO dokumentów i wzorów umów,
      2.2.8. ocena poziomu ryzyka naruszeń ochrony danych w procesach przetwarzania danych oraz proponowanych zabezpieczeń;
   2.3. wykonywanie funkcji Inspektora Ochrony Danych (dalej jako: „DPO") po dniu 25.05.2018 r. i pełnienie funkcji punktu kontaktowego zgodnie z wymaganiami RODO dla organu nadzorczego oraz podmiotu danych.