Załącznik nr 1

**Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest diagnoza stanu spełniania przez Projekt Kępno Sp. z o.o. wymagań dotyczących bezpieczeństwa informacji stawianych przed administratorem danych osobowych.

Audyt jest prowadzony w celu stwierdzenia stopnia zgodności ocenianego systemu  
z określonym standardem lub normą, wybraną jako punkt odniesienia.

Mogą być to:

1. Ustawa o ochronie danych osobowych,

2. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności,

3. Ustawa o krajowym systemie cyberbezpieczeństwa.

4. Rekomendacja D, wydana przez Komisję Nadzoru Finansowego,

5. Norma PN-ISO/IEC 27001:2017-06,

System Zarządzania Bezpieczeństwem Informacji powinien być weryfikowany pod względem wymagań stawianych przez obowiązujące przepisy prawa jak np. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r., Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r., w sprawie Krajowych Ram Interoperacyjności, w zakresie minimalnych wymagań dla rejestrów publicznych   
i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247) oraz Rozporządzenie 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 (RODO).

**Zakres usługi**

**1. Audyt ochrony danych osobowych**

a. analiza posiadanej dokumentacji ochrony danych osobowych pod kątem aktualności i zgodności z prawem,

b. zbadanie legalności przetwarzania danych osobowych i wrażliwych,

c. weryfikacja celu, zakresu przetwarzania danych oraz adekwatności do celu przetwarzania.

d. weryfikacja procesów przetwarzania danych osobowych oraz określenie konieczności prowadzenia rejestru przetwarzania.

e. analiza fizycznych i logicznych zabezpieczeń infrastruktury informatycznej,

f. weryfikacja funkcjonalności aplikacji i poziomu ich zabezpieczeń,

g. weryfikacja poziomu zabezpieczeń zbiorów danych przetwarzanych w formie papierowej oraz elektronicznej,

h. weryfikacja poziomu wiedzy i świadomości pracowników w zakresie ochrony danych osobowych i weryfikacja zawartych umów pod kątem powierzenia przetwarzania danych osobowych,

**2. Wykonanie i przekazanie Raportu z Audytu**

a. opis zakresu przeprowadzonych prac audytowych,

b. analizę informacji zebranych podczas audytów,

c. wnioski i zalecenia związane z rozwiązaniem występujących problemów.

**3. Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji, połączona z weryfikacją legalnością użytkowanego oprogramowania:** skanowanie komputerów w poszukiwaniu programów komputerowych i plikówmultimedialnych.

**Dane wyjściowe do przeprowadzenia audytu:**

- liczba osób zatrudnionych 35 osób,

- 15 stanowisk komputerowych,

- 1 osoba pracująca na stanowisku informatycznym,

- spółka posiada inspektora ochrony danych osobowych.

- spółka znajduje się w trzech lokalizacjach:

a. Hala widowiskowo- sportowa, ul Sportowa 9, 63-600 Kępno;

b. Kryta pływalnia QARIUM Kępno, ul. Sportowa 11, 63-600 Kępno;

c. Strefa Płatnego Parkowania, ul. Ratuszowa 12, 63-300 Kępno.

**Polityka bezpieczeństwa informacji**

Zidentyfikowanie i zbadanie procesów przetwarzania i ochrony danych osobowych występujących w spółce (np. HR, sprzedaż, marketing), a następnie przeanalizowaniu ich pod kątem przepisów RODO. Sprawdzeniu podlegać mają m.in. treści klauzul informacyjnych, umowy powierzenia przetwarzania danych osobowych, procedury realizacji obowiązków wynikających z RODO, zgodność rejestru czynności przetwarzania z procesami biznesowymi.

Informacje dotyczące działań obejmujących ochrony danych osobowych – ich zbierania, wykorzystywania oraz zabezpieczenia. W toku przeprowadzonego audytu ustalone powinny zostać wszystkie rodzaje danych osobowych oraz zasadność, zakres i sposób ich przetwarzania, a także zastosowane zabezpieczenia pod kątem ich zgodności z RODO.

**Audyt legalności oprogramowania**

Celem jest wyeliminowanie nielicencjonowanego oprogramowania (nabytego w sposób nielegalny lub wykorzystywanego niezgodnie z umową licencyjną). Audyt legalności polegać ma na porównaniu posiadanych licencji na oprogramowanie z faktycznie wykorzystywanym na komputerach.

Audyt powinien być dostarczony w trzech egzemplarzach w wersji papierowej i jednej w wersji elektronicznej.

Termin realizacji zadania: 60 dni od podpisania umowy.

Płatność: 14 dni od daty dostarczenia faktury.

Termin związania z ofertą: 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.