Załącznik nr 4
do Zapytania ofertowego nr BA-OZ.25.9.2018.2.IM

Szczegółowy Opis Przedmiotu Umowy

na wykonanie usługi pn.:

„Audyt organizacji oraz systemów informatycznych CUPT w zakresie dostosowania do wymagań Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r."

I. PRZEDMIOT ZAMÓWIENIA

Zamówienie będzie polegać na przeprowadzeniu audytu procedur obowiązujących w Centrum Unijnych Projektów Transportowych (dalej: CUPT) oraz systemów informatycznych CUPT celem przygotowania się do wymagań 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 tych danych oraz uchylenia dyrektywy 95/46/WE* (dalej: RODO).

II. CEL AUDYTU

Celem audytu jest zbadanie, czy rozwiązania przyjęte w ramach, wdrożonego w CUPT systemu ochrony informacji, którego częścią jest Polityka Bezpieczeństwa Informacji,
w zakresie ochrony danych osobowych, są adekwatne do potrzeb CUPT i funkcjonują prawidłowo oraz w jakim stopniu dostosowane są do obwiązujących procedur i do wymogów wynikających z RODO. Dodatkowo audyt ma na celu ustalenie aktualnego stanu bezpieczeństwa systemów informatycznych CUPT tj. wykrycie potencjalnych zagrożeń i nieprawidłowości oraz ocenę bezpieczeństwa przetwarzanych w tych systemach danych.

III. KLUCZOWE ZAGADNIENIA AUDYTU

W ramach realizacji zadania Wykonawca, podejmie czynności polegające na przeprowadzeniu weryfikacji obowiązujących w CUPT procedur i procesów

w systemie ochrony danych osobowych w zakresie przetwarzania i zabezpieczenia tych danych w szczególności poprzez ocenę:

1. zgodności przetwarzania danych osobowych w CUPT z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: Ustawa) oraz aktów wykonawczych, a w szczególności:
   a) z zasadami, o których mowa w art. 23-27 i art. 31-35 Ustawy;
   b) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37-39 ustawy oraz przepisach wydanych na podstawie art. 39 a Ustawy;
   c) z zasadami przekazywania danych osobowych, o których mowa w art. 47-48 Ustawy;
   d) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 Ustawy;
2. zgodności i skuteczności oraz zasadności zastosowanych zabezpieczeń dostępu do danych w systemach teleinformatycznych;
3. zabezpieczeń fizycznych danych osobowych oraz kontroli nad ich przepływem;
4. sposobu tworzenia i przechowywania kopii zapasowych zbiorów danych oraz naprawy i konserwacji nośników danych osobowych;
5. ocena treści dokumentacji opisującej sposób przetwarzania danych osobowych (w szczególności Polityki bezpieczeństwa danych osobowych wraz z Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych stanowiącymi element Polityki Bezpieczeństwa Informacji CUPT), upoważnień do przetwarzania danych, ewidencji osób upoważnionych do przetwarzania danych osobowych, umów powierzenia przetwarzania danych stronom trzecim, rejestru powierzeń, klauzul zgód na przetwarzanie danych osobowych, sposobu formułowania klauzul informacyjnych, umów z podmiotami wsparcia oraz z dostawcami);
6. zgodności i efektywności funkcjonowania w CUPT procesu zarządzania obszarem ochrony danych osobowych, w tym w szczególności sposobu zarządzania ryzykiem w tym obszarze, sposobu organizacji zbiorów danych osobowych, narzędzi dostępnych dla ABI w celu wykonania prawidłowo funkcji w CUPT;
7. przygotowania pracowników do reakcji w przypadku wystąpienia incydentu w zakresie ochrony danych osobowych;

8. czy stosowane procedury zapewniają prawa osób, których dane dotyczą i czy są one zgodne z faktycznymi procesami;
9. czy stosowane klauzule wymagają dostosowania do RODO, w zakresie:
   - poprawności stosowanych klauzul informacyjnych i ich stopnia dostosowania do rozszerzonego obowiązku informacyjnego,
   - gotowości organizacji do stosowania przepisów w zakresie: profilowania, uwzględniania ochrony danych w fazie projektowania i stosowania domyślnej ochrony danych,
10. ocena adekwatności poziomu zabezpieczeń dla zbiorów danych przetwarzanych w formie papierowej.

IV. PODSTAWOWE ZAŁOŻENIA METODOLOGICZNE

Zadanie audytowe należy przeprowadzić na podstawie obowiązujących aktów prawnych, tj.:

1. ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych, (Dz. U. z 2016 r. poz. 922 z późn. zm.);
2. Normy PN-ISO/IEC 27001:2014-12 (wersja polska);
3. Normy PN-ISO/IEC 27002: 2014-12 (wersja polska).

   Za równoważne do w/w norm uznaje się Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r., w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2017 poz. 2247);

4. W ramach audytu wykonawca oceni mechanizmy kontrolne funkcjonujące w CUPT oraz zbada wskazane przez Zamawiającego umowy:
   - z dostawcami,
   - z podmiotami świadczącymi usługi doradcze,
   - z Beneficjentami.

V. WYMAGANIA DOTYCZĄCE PRZEDSTAWIENIA WYNIKÓW AUDYTU

W oparciu o ocenę stanu faktycznego Wykonawca przygotuje rekomendacje, których celem będzie doprowadzenie procesu przetwarzania danych osobowych w CUPT do zgodności z wymogami wynikającymi z RODO.

Wykonawca przedstawi pisemny raport końcowy, który powinien składać się co najmniej z następujących elementów:

a) spisu treści,
b) daty rozpoczęcia audytu,
c) opisu metodologii zadania audytowego,
d) szczegółowego opisu i oceny stanu wszystkich obszarów podlegających audytowi według kryteriów przyjętych w programie audytu,
e) wskazania wyników audytu wraz z ich interpretacją oraz skutków i ryzyk będących konsekwencją stwierdzonych niezgodności,
f) rekomendacji opisujących szczegółowy sposób i zakres dostosowania obecnie funkcjonujących w CUPT systemów, w których są przetwarzane dane osobowe oraz związanych z nimi procedur do wymogów wynikających z RODO,
g) ewentualnych załączników.

Raport końcowy zostanie przekazany Zamawiającemu zarówno w formie elektronicznej (w pliku do odczytu w pdf i docx), jak i drukowanej (w liczbie 2 egzemplarzy). Wersja robocza zostanie przekazana Zamawiającemu jedynie w formie elektronicznej.

Wyniki prac będą przekazywane sukcesywnie, po zakończeniu badania każdego obszaru, jednak nie rzadziej niż raz na 10 dni.

Wykonawca uwzględniając wyniki przeprowadzonego audytu, przygotuje rekomendacje do wdrożenia wymogów wynikających z RODO w niżej wymienionych w obszarach oraz plan ich realizacji:

a) analizy ryzyka związanej z przetwarzaniem danych osobowych;
b) inwentaryzacji zbiorów danych osobowych;
c) przystosowania i modyfikacji istniejącej Polityki Bezpieczeństwa Informacji opisującej sposób przetwarzania danych osobowych;
d) weryfikacji i opracowania właściwych klauzul zgód i klauzul informacyjnych w powszechnie zrozumiałej formie dla osób, których dane dotyczą w tym w szczególności: podstawy prawnej, okresu przetwarzania danych, prawa wniesienia sprzeciwu;
e) zapisy umów z dostawcami;

f) procedur, które zapewniają prawa osób, których dane dotyczą w tym: dostępu do danych; poprawiania danych; usunięcia danych; wniesienia sprzeciwu; ograniczenia przetwarzania danych, w tym w odniesieniu do zautomatyzowanego procesu decyzyjnego; przenoszalności danych;

g) implementacji (wdrożenia) rejestru czynności przetwarzania danych;

h) procesu reagowania na incydenty naruszenia ochrony danych osobowych;

i) powołania Inspektora Ochrony Danych Osobowych;

j) zakresu modyfikacji i przystosowania systemów teleinformatycznych przetwarzających dane osobowe.

Dodatkowo, Wykonawca uwzględniając wyniki przeprowadzonego audytu i przygotowane rekomendacje, sporządzi informację zarządczą i prezentację dla Kierownictwa CUPT.

Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował jako Informacje Chronione i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego.

VI. WYMAGANIA DOTYCZĄCE WSPÓŁPRACY ZAMWIAJĄCEGO Z WYKONAWCĄ

1. W trakcie realizacji zadania audytowego Wykonawca jest zobowiązany:
   a) do sprawnej i terminowej realizacji zamówienia;
   b) pozostawania w stałym kontakcie z Zamawiającym w uczestnictwa w spotkaniach z przedstawicielami Zamawiającego odpowiednio do potrzeb;
   c) przedstawienia programu audytu w terminie 3 dni roboczych od dnia podpisania umowy – program wymaga zatwierdzenia przez Zamawiającego,
   d) program audytu będzie zawierał szczegółowy zakres audytu systemów teleinformatycznych Zamawiającego;
   e) bezzwłocznego przedstawiania na żądanie Zamawiającego raportu z postępu w realizacji zamówienia;
   f) bezzwłocznego informowania o pojawiających się problemach, zagrożeniach lub opóźnieniach w realizacji w stosunku do programu audytu, a także innych zagadnieniach istotnych dla realizacji zamówienia;

g) konsultowania z Zamawiającym decyzji związanych z metodologią zamówienia, podejmowanych w wyniku ewentualnego pojawienia się trudności w trakcie jego realizacji;

h) wyniki prac w postaci dokumentacji opisu procedur itp., powinny być bezpośrednio powiązane z specyfiką działalności CUPT;

i) przekazania Zamawiającemu pełnej dokumentacji opracowanej w trakcie realizacji zamówienia: wzorów narzędzi badawczych, ostatecznej wersji raportu, wraz ze wszystkimi załącznikami;

j) oznaczenia wszystkich materiałów przygotowanych w trakcie badania, zgodnie

z zasadami wizualizacji Funduszy Europejskich oraz POIiŚ (określonymi w Księdze Identyfikacji Wizualnej Znaku marki Fundusze Europejskie i znaków programów polityki spójności 2014-2020).

VII. INFORMACJE DODATKOWE

1. W CUPT wyznaczony został i zgłoszony do GIODO Administrator Bezpieczeństwa Informacji.
2. W CUPT funkcjonuje system ochrony informacji w oparciu o PN/ISO 27001.
3. Audyt, o którym mowa w pkt. 1, zostanie przeprowadzony w siedzibie CUPT przy Plac Europejski 2 w Warszawie.
4. Obecnie w ramach struktury organizacyjnej CUPT funkcjonuje VI Departamentów i III Biura oraz pracuje ponad 300 osób.