Załącznik nr 2

Opis Przedmiotu Zamówienia

Analiza, rekomendacje oraz wdrożenie zmian dotyczących zgodności Zintegrowanego Rejestru Kwalifikacji z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności

Informacje dotyczące zamówienia

1. Zamawiający
   Instytut Badań Edukacyjnych
   ul. Górczewska 8, 01-180 Warszawa

2. Wstęp
   Instytut Badań Edukacyjnych w Warszawie (IBE) jest placówką badawczą prowadzącą interdyscyplinarne badania naukowe nad funkcjonowaniem i efektywnością systemu edukacji w Polsce. Jednym z projektów systemowych realizowanych przez IBE na zlecenie Ministerstwa Edukacji Narodowej współfinansowanych ze środków Unii Europejskiej, jest projekt pod nazwą „Prowadzenie i rozwój Zintegrowanego Rejestru Kwalifikacji" (projekt ZRK).

   Zintegrowany Rejestr Kwalifikacji stanowi ważne narzędzie systemowe służące realizacji polityki uczenia się przez całe. Rejestr pełni ważną rolę w integracji funkcjonujących w kraju systemów kształcenia: oświaty i szkolnictwa wyższego oraz obszaru edukacji pozaformalnej i nieformalnego uczenia się.

   ZRK gromadzi i udostępnia informacje na temat możliwych do uzyskania w Polsce kwalifikacji spełniających określone przez państwo (w ustawie) wymagania dotyczące m.in. standardu opisu kwalifikacji, przypisania poziomu PRK oraz zasad zapewniania jakości kwalifikacji. ZRK jest rejestrem publicznym w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

   ZRK jest rejestrem jawnym, a informacje o kwalifikacjach w nim gromadzone są powszechnie dostępne za pośrednictwem strony internetowej (portalu internetowego) w językach polskim i angielskim. Portal oferuje możliwość łatwego przeszukiwania, porządkowania i agregowania informacji. Portal polskiego rejestru, podobnie jak portale pozostałych krajów UE, będzie powiązany z portalem Europejskiej Ramy Kwalifikacji (ERK).

   IBE, od 1 stycznia 2018 r. jest instytucją pierwszego wyboru, do którego zwracają się różne instytucje lub osoby z pytaniami dotyczącymi ZRK. Grupy osób zainteresowanych informacjami zawartymi w ZRK to np. uczniowie, pracobiorcy, pracodawcy, nauczyciele, doradcy zawodowi, administracja państwowa, jednostki samorządu terytorialnego, organizacje pracodawców, związki zawodowe, izby gospodarcze, itd.

   Podmiot prowadzący rejestr jest naturalnym punktem kontaktowym dla tych grup.

Rejestr pełni funkcję „jednego okienka” dla instytucji składających wnioski. Zadania ZRK wynikające z ustawy o ZSK to m.in.:

1. Dokonywanie wpisów w ZRK i ich aktualizacji.
2. Formalna ocena wniosków: o włączenie kwalifikacji rynkowych do ZSK, o przywrócenie kwalifikacji rynkowej statusu kwalifikacji funkcjonującej, o nadanie uprawnień do certyfikowania kwalifikacji, o wpis na listę podmiotów uprawnionych do pełnienia funkcji zewnętrznego zapewniania jakości. Wnioski składane sa wyłącznie droga elektroniczną.
3. Prowadzenie portalu ZSK w części dotyczącej ZRK.
4. Gromadzenie, przechowywanie i udostępnianie ministrom właściwym, ministrowi koordynatorowi oraz Radzie Interesariuszy raportów i sprawozdań IC oraz PZZJ.
5. Gromadzenie informacji o: liczbie wydanych dokumentów potwierdzających nadanie poszczególnych kwalifikacji, wysokości opłat i przychodów za walidację i certyfikowanie.
6. Zapewnienie dostępu do informacji o Zintegrowanym Rejestrze Kwalifikacji, w szczególności za pośrednictwem Internetu.
7. Monitorowanie funkcjonowania ZRK.
8. Uzupełnianie informacji o wpisanych do ZRK kwalifikacjach o krótkie charakterystyki kwalifikacji w języku angielskim.

System informatyczny ZRK został zaprojektowany w IBE w latach 2013 - 2015 i uruchomiony w środowisku testowym w 2015 r., jeszcze przed wejściem w życie ustawy regulującej zasady działania ZRK (ustawa o ZSK). Rejestr został uruchomiony w lipcu 2016 r.

Materiały dotyczące realizowanych projektów, w tym raport referencyjny, słownik terminów dotyczących krajowego systemu kwalifikacji oraz inne informacje znajdują się na stronach: www.ibe.edu.pl, www.kwalifikacje.gov.pl. Rejestr kwalifikacji dostępny jest pod adresem rejestr.kwalifikacje.gov.pl

Przedmiot zamówienia

1. Działający obecnie w Instytucie Badań Edukacyjnych system informatyczny rejestru publicznego ZRK, wraz z dotyczącymi jego obsługi procedurami i procesami, wymaga przeprowadzenia analizy pod kątem zgodności z rozporządzeniem z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (wraz z poprawkami). Przeprowadzenie analizy podyktowane jest koniecznością dostosowania systemu

informatycznego ZRK oraz procedur i procesów do jego obsługi do zmieniających się przepisów prawa (zmiana rozporządzenia w sprawie Krajowych Ram Interoperacyjności 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 95/36/WE (ogólne rozporządzenie o ochronie danych - RODO), które będzie stosowane od dnia 25 maja 2018 r.) ze szczególnym uwzględnieniem prowadzonych w IBE badań statystycznych.

2. Celem realizowanego zamówienia są:
   2.1. zbadanie zgodności systemu informatycznego ZRK oraz procedur i procesów funkcjonujących w IBE z wymogami rozporządzenia o Krajowych Ramach Interoperacyjności w powiązaniu z rozporządzeniem o ochronie danych osobowych - RODO
   2.2. rekomendacje, które pozwolą Instytutowi Badań Edukacyjnych wdrożyć odpowiednie zmiany i procedury.
3. Realizacja zamówienia będzie polegała na przeprowadzeniu analizy oraz przygotowaniu i wdrożeniu rekomendacji z niej wynikających.

Sposób realizacji zamówienia

1. Termin realizacji: wszystkie prace określone w przedmiocie zamówienia muszą być zrealizowane w terminie trzech miesięcy od daty podpisania umowy.
2. Zakres zamówienia powinien obejmować:
   a. Audyt zgodności z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności:
      i. Analiza zgodności z Krajowymi Ramami Interoperacyjności;
      ii. Analiza zgodności z wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej;
      iii. Analiza zgodności z wymaganiami dla systemów teleinformatycznych, w tym:
         1. specyfikację formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym,
         2. sposoby zapewniania bezpieczeństwa przy wymianie informacji,
         3. standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej,
         4. sposoby zapewniania dostępu do zasobów informacji podmiotów publicznych z uwzględnieniem wymiany transgranicznej.

b. Audyt procedur i procesów przetwarzania i ochrony danych osobowych.
    i. Inwentaryzacja zbiorów i czynności przetwarzania danych w jednostce organizacyjnej:
        1. ustalenie rodzajów zbiorów danych klientów, pracowników czy danych powierzonych przez inne podmioty oraz celu ich przetwarzania,
        2. określenie statutu prawnego przetwarzanych danych,
        3. analiza procesów przetwarzania, w tym zbierania danych oraz ewentualnego profilowania osób lub szczególnych operacji przetwarzania, wymagających przeprowadzenia oceny skutków dla ochrony danych,
        4. analiza procesów przetwarzania, ze szczególnym uwzględnieniem danych osobowych gromadzonych na podstawie szczególnych przepisów prawa, a przede wszystkim znowelizowanego Kodeksu Pracy.
    ii. Analiza wypełnienia wymagań przepisów prawa (zarówno przepisów o ochronie danych osobowych, jak i przepisów sektorowych związanych z przetwarzaniem danych):
        1. analiza przesłanek legalności (podstaw prawnych), na podstawie których przetwarzane są dane osobowe,
        2. analiza realizacji obowiązku informacyjnego, w tym poprawności klauzul informacyjnych i oświadczeń na formularzach do zbierania danych osobowych,
        3. zbadanie realizacji obowiązków dotyczących celowości, adekwatności i czasu przetwarzania danych osobowych,
        4. analiza procedur dotyczących udostępniania danych innym podmiotom, w tym udostępniania danych do państw trzecich – poza UE,
        5. analiza umów związanych z powierzaniem danych innym podmiotom lub przez inny podmiot, ocena wypełnienia związanych z tym obowiązków,
        6. badanie realizacji praw osób, których dane są przetwarzane.
    iii. Ocena wypełnienia obowiązków technicznych i organizacyjnych:
        1. ocena przyjętej dokumentacji opisującej sposób przetwarzania danych,
        2. ocena prawidłowości zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych,
        3. ocena mechanizmów rozliczalności w aplikacjach przetwarzających dane osobowe;
        4. ocena realizacji zabezpieczenia systemu informatycznego i obszaru przetwarzania danych,

5. ocena realizacji działań dotyczących nadawania upoważnień osobom do przetwarzania danych osobowych oraz prowadzenia ewidencji upoważnionych,
6. ocena wykonywania czynności nadzoru nad przetwarzaniem danych – analiza obowiązku wyznaczenia inspektora ochrony danych zgodnie z RODO
7. ocena sposobu realizacji wynikających z RODO praw osób, których dane osobowe dotyczą (prawo dostępu do danych; do sprostowania danych; ograniczenia przetwarzania; usunięcia danych; do ograniczenia przetwarzania; przenoszenia danych; sprzeciwu),
8. ocena uwzględniania ochrony prywatności w fazie projektowania,
9. ocena realizowania zasady domyślnej ochrony prywatności (np. pseudonimizacja).

iv. Przygotowanie raportu zawierającego:
1. inwentaryzację procesów, danych i systemów IT oraz podmiotów, którym zlecono czynności przetwarzania danych osobowych,
2. ocenę adekwatności stosowanych dotychczas zabezpieczeń organizacyjnych oraz fizycznych i teleinformatycznych,
3. spis zaleceń mających na celu uporządkowanie procesów przetwarzania danych.

v. Spotkanie szkoleniowo-konsultacyjne dla kadry kierowniczej z przedstawieniem i analizą takich tematów jak:
1. obecne i przyszłe obowiązki podmiotów, jako administratorów danych, w świetle zmienianych przepisów prawa oraz zasady przetwarzania i współadministrowania danymi osobowymi w grupie podmiotów,
2. nowe obowiązki informacyjne administratora,
3. nowe prawa osób, których dane dotyczą,
4. nowy zakres odpowiedzialności za przetwarzanie danych niezgodnie z przepisami,
5. konieczne działania organizacyjne, prawne, techniczne, jakie należy podjąć, aby przygotować się do stosowania RODO – rozporządzenia ogólnego o ochronie danych osobowych.

c. Opracowanie metodyki Analizy ryzyka i Polityki zarządzania ryzykiem w obszarze bezpieczeństwa informacji:
i. Wstępna identyfikacja zagrożeń dla praw i wolności osób, których dane są przetwarzane;

ii. Przygotowanie arkusza analizy ryzyka;
iii. Przeprowadzenie analizy ryzyka procesów realizowanych w każdej komórce organizacyjnej pod kątem przetwarzania danych osobowych oraz identyfikacja aktywów w nich wykorzystywanych i ryzyk naruszenia praw i wolności osób, a także wskazanie zabezpieczeń wdrożonych i potencjalnych, zmniejszających ryzyko;
iv. Wyliczenie i ocena ryzyk oraz stworzenie listy (mapy) ryzyk;
v. Przygotowanie propozycji Planu postępowania z ryzykiem.

d. Aktualizacja i uzupełnienie systemu zarządzania bezpieczeństwem informacji ze szczególnym uwzględnieniem polityki bezpieczeństwa danych osobowych:
   i. Opracowanie projektów dokumentów dotyczących przetwarzania danych lub doprowadzenie do zgodności z wymogami przepisów prawa:
      1. polityki bezpieczeństwa informacji, w tym rejestru czynności przetwarzania,
      2. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych,
      3. metodyki analizy ryzyka,
      4. procedury obsługi naruszeń danych,
      5. ocena skutków dla ochrony danych oraz ustalenie, czy przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania danych osobowych,
      6. procedury obsługi wniosków podmiotów danych;
   ii. Opracowanie wzorów klauzul informacyjnych i klauzul oświadczeń zgody, z uwzględnieniem wymagań RODO oraz innych przepisów prawa;
   iii. Opracowanie wzorów zapisów i wskazówek do uzupełniania umów powierzenia przetwarzania danych osobowych, z uwzględnieniem wymagań RODO;
   iv. Optymalizacja procesów przetwarzania danych i zabezpieczeń organizacyjnych;
   v. Konsultacje przy zatwierdzaniu Planu postępowania z ryzykiem w zakresie określenia adekwatnych środków technicznych i teleinformatycznych oraz zabezpieczeń;
   vi. Konsultacje i wsparcie we wdrażaniu wszystkich działań doskonalących.

e. Szkolenie dla pracowników z zasad przetwarzania i ochrony danych:
   i. kto to jest administrator danych i jego obowiązki;

ii. organizacja nadzoru nad przestrzeganiem zasad i przepisów dotyczących ochrony danych;
iii. definicja oraz aspekty praktyczne dotyczące pojęcia danych osobowych, oraz inne podstawowe pojęcia;
iv. osoba upoważniona do przetwarzania danych – co to znaczy;
v. bezpieczeństwo osobowe na etapie rekrutacji, zatrudnienia, zakończenia zatrudnienia. Zasady dopuszczania do informacji chronionych (tajemnice przedsiębiorstwa). Organizacja nadawania i odbierania uprawnień związanych z dostępem do danych. Obowiązki pracowników przy przetwarzaniu danych, wynikające również ze szczególnych przepisów prawa
vi. organizacyjne i techniczne środki bezpieczeństwa, jakie powinny być stosowane do zapewnienia odpowiedniej ochrony danych;
vii. zagrożenia i metody wykradania danych, jak się przed nimi chronić;
viii. konsekwencje naruszenia przepisów dotyczących bezpieczeństwa informacji, w tym odpowiedzialność prawna.

f. Wsparcie i doradztwo powdrożeniowe:
   i. Dostępność za pośrednictwem środków telekomunikacyjnych (email, telefon) dla koordynatora ds. ochrony danych wyznaczonego przez Zamawiającego przez okres dwóch miesięcy od zakończenia usługi;
   ii. Wsparcie dla osoby lub osób wyznaczonych u Zamawiającego do nadzoru przestrzegania zasad ochrony danych osobowych we wdrażaniu procedur i instrukcji składających się na Politykę bezpieczeństwa informacji;
   iii. Odpowiedzi na pytania pracowników Zamawiającego, tj. osób upoważnionych do przetwarzania danych osobowych;
   iv. Pomoc w wyjaśnianiu sprzeciwów i pytań osób, których dane dotyczą (klientów, kontrahentów, byłych pracowników);
   v. Współudział w ocenie skutków dla ochrony danych oraz ustalenie, czy przetwarzanie danych osobowych w określonym procesie z dużym prawdopodobieństwem może powodować wysokie ryzyko dla poufności i integralności danych osobowych podmiotów danych.

Warunki realizacji zamówienia

1. Przebieg prac przy realizacji zamówienia:
   a. Prace realizowane w ramach zamówienia będą prowadzone z uwzględnieniem potrzeb Zamawiającego.
   b. Zamówienie realizowane będzie przez osobę lub osoby mające wiedzę i doświadczenie adekwatne do złożoności zamówienia.

c. Zakłada się wykonanie zamówienia w siedzibie Zamawiającego w terminie określonym w harmonogramie, przy stałym współudziale wybranych osób dopuszczonych do przetwarzania danych osobowych (np. administrator bezpieczeństwa informacji, wyznaczeni przedstawiciele komórek organizacyjnych oraz administrator systemów IT).
d. Nie wyklucza się wykorzystania we współpracy, w zależności od bieżących potrzeb, innych osób dopuszczonych do przetwarzania danych.
e. Infrastrukturę na szkolenia zapewni Zamawiający.

2. Formuła realizacji zamówienia zostanie określona w uzgodnieniu z Wykonawcą w trakcie spotkań roboczych:
    a. Wyniki prac będą odbierane przez Zamawiającego w formie przyjętej po obopólnych ustaleniach Stron.
    b. Wynikiem prac wdrożeniowych będzie kompleksowa Polityka bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych przekazana w formie papierowej i elektronicznej, opracowana zgodnie z przepisami prawa z zakresu ochrony danych osobowych, z wykorzystaniem i w oparciu o normy ISO z grupy 27000.
    c. Zamawiający otrzyma zaświadczenie o przejściu audytu z zakresu ochrony danych osobowych oraz wdrożeniu systemu zarządzania bezpieczeństwem informacji zapewniającym zgodność przetwarzania i ochrony danych z obowiązującymi przepisami prawa, w szczególności z RODO - ogólnym rozporządzeniem o ochronie danych.