ST

Nr sprawy: ST.0150.9.2018 Poznań, 29.01.2018

Zapytanie ofertowe

1. Opis przedmiot zamówienia:
Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji spełniającej wymogi RODO, KRI oraz PN-ISO/IEC 27001:2014 zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącego załącznik nr 1 do niniejszego zapytania ofertowego.

2. Wymagany termin wykonania zamówienia:
Raport z audyty– do 30.03.2018,
Opracowanie dokumentacji – 15.05.2018r. - wersja zaakceptowana przez Zamawiającego.

3. Warunki udziału w postępowaniu oraz sposób ich weryfikacji (*wymagane dokumenty*):
a) znajomość metodyki audytu w zakresie bezpieczeństwa informacji (audytor prowadzący audyt musi posiadać i przesłać certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001),
b) co najmniej 2 osoby posiadające wykształcenie kierunkowe (np. studia podyplomowe ODO, bezpieczeństwo informacji, zarządzanie bezpieczeństwem informacji) – skany dyplomów,
c) certyfikat audytora wewnętrznego normy ISO 20000,
d) poświadczenie bezpieczeństwa dostępu do informacji niejawnych ABW lub SKW,
e) posiadanie wersji komercyjnej oprogramowania Nessus niezbędnego do wykonania Audytu Bezpieczeństwa Sieci,
f) co najmniej 5 letnie doświadczenie w zakresie tworzenia dokumentacji ODO,
g) doświadczenie poświadczone referencjami z przynajmniej 3 projektów w których wykonawca przeprowadzał audyt bezpieczeństwa informacji,
h) doświadczenie poświadczone referencjami z przynajmniej 3 projektów w których wykonawca przeprowadzał szkolenie z zakresu zmian w obszarze ochrony danych osobowych wynikających z Rozporządzenia Ogólnego (RODO)
i) co najmniej 1 projekt dostosowania wymagań systemu do Rozporządzenia Rady Ministrów 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 zakończony w okresie ostatnich 48 miesięcy,
j) co najmniej dwie usługi polegające na przeprowadzeniu audytu bezpieczeństwa systemów teleinformatycznych, w tym testów penetracyjnych aplikacji Web oraz analiz konfiguracji systemów IT pod kątem bezpieczeństwa, przy czym wartość każdej usługi była nie mniejsza niż 20 000 PLN brutto zakończone w okresie ostatnich 48 miesięcy,
k) co najmniej jeden projekt powinien obejmować dostosowanie dokumentacji 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 takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
W postępowaniu nie mogą brać udziału podmioty, z którymi, w czasie postępowania ofertowego, Zamawiający ma podpisane klauzule lub umowy o powierzeniu danych osobowych.

4. Opis kryteriów wyboru oferty najkorzystniejszej :
cena,
doświadczenie wykonawcy.

5. Opis sposobu przygotowania oferty cenowej:
Cena całkowita netto.

6. Miejsce i termin składania oferty cenowej:
Termin składania ofert: 5.02.2018r. godz. 12.00
Oferty wysyłane drogą elektroniczną należy wysyłać na adres e-mail: d.gedziorowski@posir.poznan.pl
Oferty w formie papierowej należy składać w sekretariacie Dyrekcji POSiR – liczy się termin wpływu oferty do sekretariatu.
Zamawiający ma prawo odrzucić oferty wpływające po wyznaczonym terminie.

7. Wskazanie osób upoważnionych przez Zamawiającego do kontaktu z Wykonawcami:
Damian Gędziorowski tel. 61 835 79 17, e-mail: d.gedziorowski@posir.poznan.pl

Zamawiający informuje, iż do wyboru oferty najkorzystniejszej nie mają zastosowania przepisy ustawy Prawo zamówień publicznych.
W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert, zmodyfikować treść dokumentów zawierających istotne warunki zamówienia. Dokonane w ten sposób uzupełnienie umieszczone zostanie niezwłocznie na stronie www zamawiającego.
W toku dokonywania oceny złożonych ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
Zamawiający nie ponosi żadnej odpowiedzialności ani jakichkolwiek kosztów związanych z przygotowaniem oferty przez Wykonawcę, a w szczególności związanych z przystąpieniem do procesu ofertowego, przygotowaniem i złożeniem oferty, negocjacji, przygotowaniami do zawarcia umowy.
Zamawiający zastrzega sobie prawo do dowolnego wyboru Wykonawcy.
Zamawiający zastrzega sobie prawo do odrzucenia ofert o rażąco niskiej cenie.

Pełnomocnik Dyrektora POSiR
ds. Systemu Zarządzania Jakością
Damian Gędziorowski
2.9.01.18

data i podpis Kierownika Oddziału/Działu/Pracownika
na samodzielnym stanowisku

zał. nr 1 do zapytania ofertowego nr ST.0150.9.2018

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest usługa polegająca na:

1. Przeprowadzenie audytu spełnienia wymogów 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 obejmującego:

a) Ocenę dostosowania systemu zarządzania w POSiR do wymagań RODO - Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych zwane RODO);

b) Ocenę dostosowania systemu zarządzania w POSiR do wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie KRI - Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w POSiR (zwane KRI);

c) Ocenę dostosowania systemu Zarządzania Bezpieczeństwem Informacji w oparciu o normę PN-ISO/IEC 27001:2014 w POSiR.

2. W oparciu o raport z audytu opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji spełniającej wymogi KRI, RODO oraz PN-ISO/IEC 27001:2014.

3. Szkolenie pracowników

1. Audyt

1.1 Cel audytu

Audyt w Dyrekcji POSiR oraz we wszystkich jego oddziałach na terenie miasta Poznania, którego celem jest:

a) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 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,

b) Weryfikacja poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia

2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w POSiR, zwanego dalej KRI,

c) Weryfikacja poziomu spełnienia wymagań normy PN-ISO/IEC 27001:2014 przez POSiR, w tym ocena skuteczności funkcjonujących zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych w POSiR, w obszarach określonych załącznikiem A do ww. normy,

d) Przeprowadzenie inwentaryzacji wszystkich zbiorów danych osobowych,

e) Przeprowadzenie inwentaryzacji aktywów informacyjnych związanych z bezpieczeństwem informacji,

f) Opracowanie koncepcji przystosowania organizacji do wymagań ISO 27001:2014, RODO oraz KRI, w tym przedstawienie szczegółowego harmonogramu prac.

1.2 Zakres audytu

1. Zakres prac podczas audytu zerowego będzie obejmował w szczególności:

a) Zapoznanie się ze strukturą organizacyjną POSiR;

b) Analizę i ocenę dokumentacji w zakresie:

- bezpieczeństwa informacji,
- ochrony danych osobowych,
- zarządzania ryzykiem,

w tym polityk, procedur, zarządzeń, instrukcji, regulaminów wewnętrznych, umów powierzenia danych osobowych zawieranych przez POSiR, dokumentacji dotyczącej zarządzania ryzykiem, rejestrów zbiorów danych osobowych, dokumentacji szkoleń, identyfikacji procesów oraz innych dokumentów;

c) Weryfikację poziomu spełnienia poszczególnych wymogów RODO, KRI oraz ISO 27001:2014 pod kątem charakterystyki organizacji, jej modelu biznesowego, zasobów oraz aktywów;

d) Ocenę stanu bezpieczeństwa fizycznego siedziby dyrekcji POSiR oraz wszystkich oddziałów POSiR (budynki oraz pomieszczenia) na podstawie wizji lokalnej miejsc przetwarzania danych osobowych;

e) Przeprowadzenie inwentaryzacji zbiorów danych osobowych (cel, zakres, podstawa prawna przetwarzanych danych osobowych, systemy przetwarzające dane osobowe, podmioty, którym dane osobowe są powierzane) w stosunku do których Zamawiający występuje jako administrator danych lub podmiot, któremu powierzono przetwarzanie danych, w tym również analiza operacji wykonywanych na danych zawartych w zbiorach;

f) Analizę bezpieczeństwa systemów teleinformatycznych, ze szczególnym uwzględnieniem systemów w których przetwarzane są dane osobowe - inwentaryzację aktywów/grup aktywów związanych z bezpieczeństwem informacji oraz weryfikację poziomu zabezpieczeń do kategorii danych przetwarzanych w systemach informatycznych i ustalenie poziomów zabezpieczeń danych

zgodnych z wymogami RODO w systemach POSiR;

g) Analizę procesu zarządzania incydentami naruszenia ochrony danych osobowych;

h) Analizę procesów przetwarzania danych osobowych (z uwzględnieniem zasady legalności oraz adekwatności), w szczególności w takich obszarach jak:

- pozyskiwanie danych m.in. w związku z usługami świadczonymi drogą elektroniczną, działalnością marketingową, w tym: analiza podstawy prawnej pozyskiwania danych osobowych, przegląd formularzy służących do zbierania danych i klauzul zgód;
- przechowywanie/analiza procedur retencji danych z uwzględnieniem ograniczenia czasowego przechowywania danych oraz obowiązku zapewnienia odpowiedniego zabezpieczenia danych;
- usuwanie –analiza procedur usuwania danych z systemów Zamawiającego.

i) Analizę wykonywania obowiązku informacyjnego spoczywającego na Zamawiającym, w szczególności:

- przegląd klauzul informacyjnych oraz zgód pod kątem ich treści, formy, miejsca zamieszczenia,
- analiza procesów informacyjnych.

j) Inwentaryzację podmiotów, którym Zamawiający powierza do przetwarzania dane osobowe, obejmująca:

- identyfikację takich podmiotów oraz weryfikację istnienie umów powierzenia przetwarzania danych;
- analizę treści wzorów umów powierzania przetwarzania danych osobowych,
- analizę zakresu powierzenia przetwarzania danych osobowych.

k) Analizę realizacji praw osób, których dane dotyczą m.in. prawa do bycia zapomnianym, prawa do przenoszenia danych itd.

l) Ustalenie czy podejmowanie są decyzje opart na zautomatyzowanym przetwarzaniu danych, w tym profilowaniu;

ł) Weryfikację rozwiązań służących zapewnieniu ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych (privacy by design, privacy by default);

m) Audyt Bezpieczeństwa Sieci (ABS):

Cel: Zidentyfikowanie a następnie wyeliminowanie podatności na zagrożenia w systemach informatycznych.

Opis usługi:

Usługa ta polega na badaniu (z wykorzystaniem najnowszej wersji oprogramowania Nessus) podatności sieci komputerowej na próby ataków pod kątem luk bezpieczeństwa wykorzystywanego oprogramowania, zabezpieczeń sieciowych oraz konfiguracji. Podczas audytu dokonuje się następujących badań i analiz na wybranej próbie systemów i stacji roboczych określonych na początku audytu:

· Badanie sieci pod kątem wykrytych adresów.

· Wybranie poszczególnych hostów, które będą podlegały audytowi.

· Testy wewnętrzne sieci.

· Testy zewnętrzne sieci.

· Przygotowanie podstawowych rekomendacji do wykrytych podatności.

· Analiza udostępnionych zasobów sieciowych.

· Analiza polityki haseł na stacjach.

· Analiza wyników indywidualnych dla każdego audytu z rekomendacjami.

Wynik:

Raport zawiera wykryte podatności podzielone i przypisane, według wielkości zagrożenia, do jednej z grup:

· Zagrożenia krytyczne.

· Zagrożenia wysokie.

· Zagrożenia średnie.

· Zagrożenia niskie.

Raport zawiera dodatkowo:

· Wykaz adresów IP hostów poddanych testom.

· Wykaz udostępnionych zasobów sieciowych, do których dostęp można uzyskać bez podania poświadczeń.

· Zalecenia dotyczące polityki haseł.

· Sugestie dotyczące zwiększenia bezpieczeństwa.

· Indywidualne zalecenia dotyczące wykrytych podatności

n) Opracowanie raportu końcowego z przeprowadzonego audytu (w tym Audytu Bezpieczeństwa Sieci) zawierającego co najmniej opis poziomu spełnienia wymogów RODO, KRI, ISO 27001:2014 ze wskazaniem ewentualnych niezgodności i rekomendacji naprawczych oraz propozycji konfiguracji lub zmian w systemach informatycznych, a także zmian zapisów w regulacjach wewnętrznych dostosowanych do specyfiki badanego podmiotu i jego możliwości organizacyjnych.

2. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji spełniającej wymogi KRI, RODO oraz PN-ISO/IEC 27001:2014 w tym w szczególności:

2.1. Dokumenty wynikające z RODO:

2.1.1. Rejestr czynności przetwarzania danych prowadzony przez administratora danych (30.1)

2.1.2. Rejestr kategorii czynności prowadzonych przez podmiot przetwarzający (30.2)

2.1.3. Dokument wdrożenia technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. (24.1)

2.1.4. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1., zawierający ocenę odpowiedniości stopnia bezpieczeństwa. (32)

2.1.5. Upoważnienie do przetwarzania danych osobowych (29, 32)

2.1.6. Dokument uchylenia (odebrania, wycofania, stwierdzenia nieważności) upoważnienia do przetwarzania danych osobowych (29, 32)

2.1.7. Polecenie przetwarzania danych osobowych (29, 32)

2.1.8. Dokument uchylenia (odebrania, wycofania, stwierdzenia nieważności) polecenia przetwarzania danych osobowych (29, 32)

2.1.9. Dokument wskazania osób uprawnionych do odwrócenia pseudonimizacji (Pre 29)

2.1.10. Polityka Ochrony Danych (24.2.)

2.1.11. Dokument wdrożenia Polityki ochrony danych (24.2.)

2.1.12. Dokument umożliwiający realizację obowiązku informacyjnego w przypadku zbierania danych od osoby, której one dotyczą, w tym informacja o fakcie i konsekwencjach profilowania. (12, 13)

2.1.13. Dokument potwierdzający realizację obowiązku informacyjnego w przypadku zbierania danych nie od osoby, której one dotyczą, w tym informacja o fakcie i konsekwencjach profilowania. (12,14)

2.1.14. Dokument zawierający dane umożliwiające realizację uprawnień informacyjnych (uprawnień kontrolnych) (15)

2.1.15. Dokument potwierdzający realizację uprawnień informacyjnych (uprawnień kontrolnych) (15)

2.1.16. Dokument umożliwiający realizację prawa do usunięcia danych przez osobę której dane dotyczą (17.1)

2.1.17. Dokument potwierdzający realizację obowiązku usunięcia danych przez administratora (17.1)

2.1.18. Dokument uzasadniający niezrealizowanie obowiązku usunięcia danych przez administratora (17.3)

12.1.9. Dokument umożliwiający realizację prawa do sprostowania danych. (16)

2.1.20. Dokument potwierdzający realizację prawa do sprostowania danych (16)

2.1.21. Dokument umożliwiający realizację prawa żądania ograniczenia przetwarzania (18.1)

2.1.22. Dokument potwierdzający umożliwienie realizacji prawa żądania ograniczenia przetwarzania (18.2)

2.1.23. Informacja skierowana do osoby, której dane dotyczą, która żądała ograniczenia na mocy art. 18 ust 1 RODO o uchyleniu ograniczenia.

2.1.24. Informacja o zamiarze uchylenia ograniczenia przetwarzania skierowana do osoby, która żądała ograniczenia przetwarzania na mocy art. 18 ust 1 RODO.

2.1.24. Dokument uchylenia ograniczenia przetwarzania (18.3)

2.1.25. Informacja o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu

przetwarzania (Art. 19) skierowana do odbiorców danych, którym udostępniono dane osobowe.
2.1.26. Przeprowadzenie analizy ryzyka wraz z planami postępowania z ryzykiem dla wszystkich danych osobowych Zamawiającego zgodnie z metodyką analizy ryzyka obowiązującą u Zamawiającego,
2.1.27. Wykonanie oceny skutków dla ochrony danych osobowych (DPIA) spełniająca wymagania RODO art. 35 dla wszystkich danych osobowych przetwarzanych w POSiR zgodnie z jedną z metodyk wymienioną w *„Wytycznych dotyczących oceny skutków dla ochrony danych (DPIA)..."* Grupy roboczej art. 29 ds. Ochrony danych (FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015 lub UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office ICO, 2014).
2.1.28. Dokument uzasadniający niewykonanie oceny skutków dla ochrony danych (35)
2.1.29. Dokument stwierdzenia naruszenia ochrony danych osobowych przez ADO (33.1)
2.1.30. Dokument stwierdzenia naruszenia ochrony danych osobowych przez PP (33.1)
2.1.31. Dokument zgłoszenia naruszenia stwierdzonego przez PP administratorowi (33.2)
2.1.32. Dokument zaistnienia naruszenia ochrony danych osobowych, zawierający m.in. okoliczności naruszenia ochrony danych osobowych, skutki naruszenia, podjęte działania zaradcze, umożliwiający organowi nadzorczemu weryfikację przestrzegania art. 33 RODO (33.5)
2.1.33. Dokument zgłoszenia naruszenia ochrony danych osobowych (art. 33.3)
2.1.34. Dokument zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych (34.1)
2.1.35. Dokument uzasadniający dlaczego nie zawiadomiono osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, uzasadniający brak zawiadomienia (34.3)
2.1.36. Dokument uzasadniający dlaczego nie zawiadomiono osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, uzasadniający brak zawiadomienia i użycie innej metody poinformowania (34.3.c)
2.1.37. Dokument wyznaczenia IOD (37.1)
2.1.38. Umowa powierzenia przetwarzania danych osobowych (28)
2.1.39. Zgoda na podpowierzenie przetwarzania danych osobowych (jeśli zachodzi podpowierzenie) (28.1)
2.1.40. Opracowanie formularzy do zbierania danych osobowych z klauzulami informacyjnymi dla wszystkich przypadków zbierania danych przez Zamawiającego (13).

2.2. Dokumenty wynikające z KRI oraz PN-ISO/IEC 27001:2014:

2.2.1. Księga systemu zarządzania bezpieczeństwem informacji,
2.2.2. Instrukcja zarządzania systemami informatycznymi,
2.2.3. Procedury bezpieczeństwa w obszarach:
- organizacji wewnętrznej,

- urządzeń mobilnych,
- bezpieczeństwa zasobów ludzkich przed zatrudnieniem, podczas zatrudniania i zakończanie lub zmiana zatrudniania,
- odpowiedzialności za aktywa informacyjne i usługi informatyczne,
- klasyfikacji i postępowania z informacjami i jej nośnikami,
- kontroli dostępu fizycznego, technicznego i logicznego do aktywów informacyjnych w tym zarządzanie użytkownikami,
- zarządzania i pracy w obszarach bezpiecznych,
- bezpieczeństwa sprzętu,
- rejestrowania i monitorowania zdarzeń związanych z bezpieczeństwem informacji,
- monitorowania podatności technicznych i ochrony przed szkodliwym oprogramowaniem,
- obsługi incydentów i zgłaszanych słabości w zakresie bezpieczeństwa informacji,
- zarządzania bezpieczeństwem sieci,
- nadawania i kontroli uprawnień,
- planowania, wdrażania, weryfikowania, przeglądu i oceny ciągłości działania,
- ochrony danych osobowych.

3. Szkolenie

3.1 Wykonawca po zakończeniu audytu i opracowaniu dokumentacji SZBI zobowiązany jest do:
a) przeprowadzenia szkolenia (w siedzibie Zamawiającego) dla wszystkich pracowników POSiR z tematyki ochrony danych osobowych i informacji w kontekście RODO, KRI oraz opracowanej dokumentacji SZBI w wymiarze 8 godzin (2 grupy po 4 godziny zegarowe);
b) przeprowadzenia specjalistycznego szkolenia (w siedzibie Zamawiającego) dla pracowników działu kadr POSiR z tematyki ochrony danych osobowych i informacji w procesach związanych z obsługą stosunku pracy w kontekście RODO, KRI oraz opracowanej dokumentacji SZBI w wymiarze 8 godzin (2 grupy po 4 godziny zegarowe).