Wszyscy Wykonawcy

Zamawiający informuje, że w zapytaniu cenowym dotyczącym udzielenia zamówienia na dostosowanie warunków działania Stowarzyszenia Gmin i Powiatów Aglomeracji Wrocławskiej do 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), wpłynęły niżej wymienione zapytania o wyjaśnienie treści Opisu Przedmiotu Zamówienia. Niniejszym Zamawiający z przekazuje treść zapytań wraz z wyjaśnieniami:

1. Czy w firmie były już prowadzone prace, mające na celu dostosowanie organizacji do wymagań RODO? Jeżeli tak, prosimy wymienić ich zakres?

   Nie, nie było wcześniej prowadzonych prac w tym zakresie.

2. Jaka jest struktura organizacyjna firmy (działy / departamenty)? Czy wdrożenie będzie realizowane w więcej niż jednej spółce? Czy któreś z podstawowych funkcji wspierających są w całości zlecane na zewnątrz firmy? (kadry, płace, IT, marketing)

   Z uwagi na liczbę pracowników w strukturze Stowarzyszenia brak jest wydzielonych komórek organizacyjnych typu działy/departamentu (płaska struktura).

   Stowarzyszenie zleca na zewnątrz usługę obsługi informatycznej, tj. zarządzanie replikacją mobilnych katalogów użytkowników (profile użytkowników), przestrzenią dyskową serwera, plikami i folderami sieciowymi, monitorowanie zdarzeń dotyczących zabezpieczeń w obrębie sieci informatycznej, konfigurowanie oraz zarządzanie systemem DNS oraz protokołem TCP/IP, nadzór nad funkcjonowaniem bazy danych, zarządzanie prawami dostępu do bazy danych, aktualizowanie dokumentacji technicznej sieci LAN, bieżąca optymalizacja wydajności sieci komputerowej, pracy bazy danych, wykrywanie sprawiających problemy zapytań oraz aplikacji, zarządzanie zasobami (przestrzeń dyskowa, czas procesorów, przydziały pamięci, itp.), zarządzanie urządzeniami sieciowymi, bieżąca kontrola wykorzystania zasobów (prowadzenie nadzoru nad eksploatacją urządzeń aktywnych), określanie zasad wewnętrznego /zewnętrznego dostępu do usług, nadzór nad sprzętem informatycznym, instalowanie systemów operacyjnych wraz z aktualizacjami, reinstalacja systemów operacyjnych, optymalizacja pracy komputerów, instalowanie komputerów, terminali, drukarek (fizyczne podłączenie do sieci teletechnicznej oraz instalacja właściwych sterowników), instalowanie oprogramowania podstawowego (biurowego, antywirusowego), bieżące dostosowywanie środowiska do potrzeb użytkowników (konfiguracja drukarek, połączeń sieciowych, udostępnianie zasobów, itp.), pomoc pracownikom Zamawiającego

w korzystaniu z dostępnego oprogramowania, doradztwo w zakresie planów modernizacji sprzętu oraz oprogramowania wraz z wydawaniem orzeczeń technicznych dotyczących sprzętu komputerowego, usuwanie awarii i przywrócenie prawidłowej pracy infrastruktury informatycznej, odtwarzanie systemu po awarii, utworzenie i wdrożenie procedur tworzenia kopii zapasowych oraz nadzór nad ich przestrzeganiem, wykonywanie bieżących kopii bezpieczeństwa danych oraz kontrola procesu odtwarzania (okresowe odtwarzanie danych w środowisku testowym), współpraca z firmami dostarczającymi sprzęt w zakresie egzekwowania zobowiązań gwarancyjnych, itp., zabezpieczanie łączności z Internetem przez wykupione przez Zamawiającego łącze (instalacje i konfiguracje urządzeń dostępowych), zarządzanie pocztą elektroniczną.

3. Czy firma posiada własną serwerownię, czy wykorzystuje usługi zewnętrznych dostawców (kolokacja / hosting)? Prosimy o wskazanie ilości centrów danych, (w przypadku outsourcingu) wybranych dostawców oraz wskazanie, jeśli któraś lokalizacja pełni funkcję zapasowej.

   Stowarzyszenie wykorzystuje własny jeden serwer lokalny oraz korzysta z usług zewnętrznych w zakresie strony internetowej oraz poczty elektronicznej.
4. Czy dotychczas istniały w Państwa firmie procesy, standardy i polityki odpowiedzialne za bezpieczeństwo informacji? Jeżeli tak, prosimy wskazać nadrzędne dokumenty.
   Jeżeli posiadane rozwiązania bazowały na powszechnie stosowanej metodyce, lub firma posiada certyfikaty bezpieczeństwa – prosimy je wskazać.

   Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw.

5. Kto w firmie (stanowisko / rola) jest odpowiedzialny za funkcje związane z bezpieczeństwem informacji (infrastruktura, aplikacje, operacje, zarządzanie ryzykiem).
   Jeżeli istnieje dedykowany zespół, czy firma posiada opisany model operacyjny funkcji bezpieczeństwa?
   Jeżeli nie istnieje odrębny zespół bezpieczeństwa, można wskazać osoby pracujące w dziale IT odpowiedzialne za administrowanie siecią i aplikacjami.

   Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw. Z uwagi na liczbę pracowników w strukturze Stowarzyszenia brak jest wydzielonych komórek organizacyjnych typu działy/departamentu (płaska struktura).

6. Ilu zewnętrznych dostawców przetwarza na zlecenie Państwa firmy dane osobowe klientów lub pracowników? Ilu dostawców zewnętrznych posiada potencjalny dostęp do tych danych? Prosimy wskazać usługi, które świadczą

   0 (zero) dostawców.

7. Prosimy wskazać, czy w przedsiębiorstwie zostały wdrożone procesy: zarządzania incydentami, zarządzania zmianą, zarządzania ryzykiem operacyjnym, zarządzania konfiguracją, monitorowania operacyjnego. Jeżeli tak, czy zostały opracowane w oparciu o znaną metodykę (ITIL, COBIT, SABSA)?

   Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw. Wskazane procesy nie są istotną częścią działalności Stowarzyszenia i nie zostały jako takie wdrożone.

8. Czy w ramach projektu będzie potrzeba abyśmy zinwentaryzowali zbiory danych osobowych przetwarzanych w Państwa firmie?

   Nie ma takiej konieczności.

9. Prosimy wskazać orientacyjną liczbę procesów biznesowych funkcjonujących w Państwa firmie. Jaka część z nich została opisana? (pozostałą część będziemy musieli zmapować w trakcie wspólnych warsztatów)

   Działalność Stowarzyszenie ma charakter publiczny, wspierający działalność jednostek samorządu terytorialnego. Brak jest procesów biznesowych.

10. Czy w firmie istnieje opis architektury IT pozwalający zmapować grupy danych osobowych na poszczególne aplikacje i lokalizacje sieciowe, w których są przetwarzane/ przechowywane? Ile aplikacji przetwarza te dane – czy są to rozwiązania „pudełkowe”, czy projektowane na zamówienie Państwa firmy?

    Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw. W Stowarzyszeniu nie funkcjonują aplikacje projektowane na zamówienie. Używane jest standardowe oprogramowanie biurowe oraz aplikacje dedykowane do obsługi księgowości, kadr oraz systemu kancelaryjnego.

11. Czy istnieją oddziały, przedstawicielstwa, pracownicy (przedstawiciele) terenowi?

    Nie, Stowarzyszenie nie posiada wskazanych elementów struktury. Istnieje jedna siedziba instytucji.

12. Jaka jest orientacyjna łączna liczba pracowników (również współpracowników)?

    9 osób.

13. Czy przetwarzacie Państwo dane dotyczące stanu zdrowia, historii karalności, orientacji seksualnej lub zapatrywań politycznych? (obejmuje to również informacje wykorzystywane w działach windykacji)

    Uczniowie szkół podstawowych biorący udział w obozach sportowych organizowanych przez Stowarzyszenie dostarczają zaświadczenia o braku przeciwskazań zdrowotnych. Osoby wykonujące zadania o charakterze edukacyjnym (trenerzy, edukatorzy) są weryfikowani w rejestrze sprawców przestępstw na tle seksualnym.

14. Czy macie Państwo wyznaczonego Administratora Bezpieczeństwa Informacji?

    Dotychczas nie było konieczności powołania administratora. Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw.

15. Czy dane są powierzane poza Polskę/ czy dane są transferowane poza obszar EOG/ ?

    Nie.

16. Czy spółka była kontrolowana przez GIODO, czy aktualnie toczą się jakiekolwiek postępowania przed GIODO?

    Nie.

17. Kluczowe procesy biznesowe (np. kadry, płace, biuro obsługi Klienta, IT, administracja, eksploatacja):

    Projekty edukacyjne, obozy sportowe, obsługa kadrowa i księgowa.

18. Lista procesów biznesowych, które są outsourcowane np. kadry, płace, rachunkowość

    Usługi informatyczne, zgodnie z pyt. nr 2.

19. Jaki jest cel, zakres i kontekst przetwarzania danych osobowych (prosimy o krótki opis)

    Stowarzyszenie przetwarza dane osobowe uczniów szkół podstawowych biorących udział w działaniach edukacyjnych celem możliwości dopuszczenia ich do udziału w obozach sportowych lub w celu sprawozdawczości dla instytucji udzielających dotacji na realizację tych działań. Dane pracowników Stowarzyszenia przetwarzane są zgodnie z ogólnie przyjętymi zasadami kadrowymi.

20. Czy Klient posiada dokumentację ochrony danych osobowych zgodną z UODO (politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym)?

    Zgodnie z odpowiedzą na pyt. nr 7.

21. Liczba zidentyfikowanych zbiorów danych osobowych

    Dane dotyczące pracowników Stowarzyszenia, dane osób zaangażowanych w realizację projektów Stowarzyszenie (edukatorzy, trenerzy), dane uczestników zajęć organizowanych przez Stowarzyszenie.

22. Czy Klient zgłosił bazy danych do GIODO (jeśli tak, jakie to były bazy) ? Czy Klient przechodził kiedykolwiek audyt informatyczny lub prawny ochrony danych i czy jest w posiadaniu dokumentacji z audytu (raport, rekomendacje itp.)?

    Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw. Stowarzyszenie nie było podmiotem kontroli, o jakiej mowa z pytaniu.

23. Czy zarządzanie IT jest scentralizowane? Jeśli nie, prosimy o opisanie, które elementy IT są zarządzane lokalnie w poszczególnych lokalizacjach.

    Zgodnie z pyt. nr 2.

24. Czy występuje outsourcing usług IT? Jeśli tak, to jakie funkcje IT i jakie systemy są outsourcowane?

    Zgodnie z pyt. nr 2.

25. Liczba systemów IT , w ramach których przetwarzane są dane osobowe.

    Zgodnie z pyt. nr 10.

26. Jakie firmy zewnętrzne przetwarzają dane osobowe (np. zewnętrzne biuro rachunkowe, zewnętrzne wsparcie IT)? Proszę podać szacunkową liczbę takich podmiotów.

    Zgodnie z pyt. nr 2.

27. Czy zawarto umowy powierzenia przetwarzania danych osobowych z firmami zewnętrznymi? Liczba takich umów.

    Stowarzyszenie przewiduje, że usługa będące przedmiotem zamówienia zostanie wdrożona/przeprowadzona od podstaw. Nie zawierano umów dotyczących powierzenia danych osobowych.

28. Czy jest to RFI, na podstawie którego szacujecie Państwo budżet na docelowe zapytanie ofertowe ?

Jest to docelowe zapytanie ofertowe.

29. W odniesieniu do przedmiotu zamówienia. Mam rozumieć, że zależy Państwu na audycie pod kątem KRI oraz RODO (pkt.7)?

    Przedmiotem zamówienia nie jest audyt. Stowarzyszenie wyłoni w ramach zapytania cenowego Wykonawcę, który wdroży stosowne procedury i zweryfikuje konieczność zatrudnienia Inspektora danych osobowych w kontekście RODO, zgodnie z treścią zapytania.

30. Jaka ilość stacji roboczych będzie objęta wdrożeniem RODO?

    W Stowarzyszeniu 8 osób posiada stanowiska komputerowe.

31. Czy przekazują Państwo dane osobowe innym podmiotom?

    Zgodnie z pyt. nr 19.

32. Czy wiedzą Państwo, w jakim kraju znajdują się serwery, na których przechowywane są dane osobowe przetwarzane przez Państwa w tym m.in. w tzw. chmurze (dotyczy to również korzystania z usług podmiotów trzecich)? Czy znajdują się one poza obszarem Unii Europejskiej?

    Serwer Stowarzyszenia znajduje się na terenie kraju (wspólny serwer lokalny). Na zewnątrz realizowana jest usługa poczty elektronicznej oraz strony www.

33. Proszę o wymienienie całej dokumentacji, którą Państwo posiadają w zakresie bezpieczeństwa danych, również polityki wejść i wyjść lub polityki kluczy, jeżeli taka funkcjonuje, czy posiadają Państwo instrukcję zgłaszania incydentów, procedurę dostępu do zakładów itp.?

    Zgodnie z pyt. nr 4.

34. Czy mają Państwo wdrożone normy z rodziny ISO 27000, ISO 29100, ISO 31000? Nie

    Zgodnie z pyt. nr 7.

35. W jakich systemach, programach przetwarzają Państwo dane osobowe (np. CRM), czy mają Państwo informację, czy systemy te są zgodne z aktualnie obowiązującą ustawą o ochronie danych?

    Zgodnie z pyt. nr 10.

36. Czy mają Państwo wdrożone zabezpieczenia własnej sieci (Firewall, systemy antywirusowe czy też IPS, oprogramowanie anti malware)?

    Tak, funkcjonuje firewall oraz system antywirusowy.

37. Czy mają Państwo własny dział IT, czy też korzystają Państwo z zewnętrznej firmy? Zewnętrza firma.

    Zgodnie z pyt. nr 2.

38. Czy mają Państwo opracowane procesy związane z monitorowaniem stanu bezpieczeństwa sieci i systemów?

    Zgodnie z pyt. nr 2.

39. Czy wdrożono procedurę tworzenia kopii zapasowych?

    Tak, zgodnie z pyt. nr 2.

40. Czy mają Państwo wdrożone procedury dotyczące ciągłości działania lub faktycznie stosują Państwo rozwiązania zapewniające ciągłość działania sprzętu IT pomimo np. braku zasilania?

    Zgodnie z pyt. nr 2. Dwa stanowiska pracy wyposażone są w UPS, reszta pracowników posługuje się komputerami przenośnymi wyposażonymi w baterie.

41. Czy dysponujecie Państwo projektem umowy dot. realizacji ww. zlecenia.

    Wraz z odpowiedziami na pytania przedstawiamy istotne postanowienia umowy.

42. Czy współpracuje Państwo ze specjalistami z zakresu IT w zakresie obsługi wykorzystywanego sprzętu informatycznego, programów itd., którzy będą w stanie podjąć współpracę ze zleceniobiorcą w zakresie wdrożenia RODO (konieczność przekazania stosownych informacji technicznych na potrzeby opracowania i wdrożenia dokumentacji RODO).

    Tak, zgodnie z pyt. nr 2.