

Warszawa, 18 kwietnia 2018 r.

Dotyczy postępowania na **wykonanie usługi związanej z dostosowaniem dokumentacji i procedur 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 („RODO”) w Grupie Kapitałowej Polskiego Holdingu Nieruchomości S.A.**

W związku z ogłoszeniem powyższego postępowania Zamawiający otrzymał następujące pytania od Podmiotów uczestniczących w postępowaniu:

Pytania:

1. Jakie spółki będą objęte projektem?
2. Czy prace projektowe obejmować będą Centralę czy również jednostki terenowe? (Jeżeli prace obejmą również jednostki terenowe prosimy o informację, gdzie są zlokalizowane.)
3. Jaka jest preferowana data startu projektu?
4. Czy w ramach utrzymania wdrożonych zmian oczekują Państwo przejęcia obowiązków IOD od 25.05.2018 r.?

Uwaga! Jeżeli projekt obejmuje więcej niż jedną spółkę, prosimy o udzielenie odpowiedzi na poniższe pytania w miarę możliwości w podziale na poszczególne spółki

5. Ile szacunkowo osób ma dostęp do przetwarzanych danych osobowych? (W praktyce jest to liczba pracowników)
6. Ile jest wewnętrznych departamentów/biur/działów?

7. Czy w ramach grupy kapitałowej (o ile istnieje) spółki wymieniają pomiędzy sobą dane osobowe? (Jeśli tak, prosimy o podanie liczby spółek.)
8. Czy powołano funkcję ABI lub osobę odpowiedzialną za bezpieczeństwo informacji? Jeśli tak, to czy funkcja outsorcowana do zewnętrznej firmy?
9. Czy zostały wdrożone wymagania normy ISO 27001 lub czy standardy bazują na wytycznych tej normy?
10. Jakie polityki i procedury funkcjonują obecnie w obszarze ochrony danych osobowych? Ile takich procedur wdrożono?

Przykładem może być polityka bezpieczeństwa, instrukcja, zarządzania systemem informatycznym, procedury dotyczące bezpieczeństwa informacji, zarządzania dokumentacją, roli inspektora ochrony danych etc.

11. Ile szacunkowo jest wzorów umów lub zapisów o powierzeniu przetwarzaniu danych osobowych?
12. Ile szacunkowo jest aktywnych umów z zewnętrznymi podmiotami, którzy przetwarzają dane osobowe?
13. Ile szacunkowo jest wykorzystywanych rodzajów klauzul Informacyjnych oraz zgód na przetwarzanie danych osobowych? Rodzaje klauzul i zgód mogą być różne w zależności:
 - zakresu, celu i kategorii przetwarzania danych osobowych,
 - liczby oferowanych produktów i usług
 - zmian w prawie na przestrzeni lat.
14. Ile szacunkowo jest procesów, w których mogą być przetwarzane dane osobowe?

Przykładem procesu jest proces zatrudnienia nowego pracownika lub sprzedaż konkretnego produktu, usługi

15. Ile szacunkowo jest systemów informatycznych używanych do przetwarzania danych osobowych?

Przykładem są systemy CMR, HR, finansowo-księgowe.

16. Czy przetwarzane dane są wrażliwe?

Poprzez dane wrażliwe rozumiemy szczególne kategorie danych (np. przekonania religijne, poglądy polityczne, stan zdrowia; więcej kategorii w dokumencie RODO) oraz dane dotyczące wyroków skazujących i naruszeń prawa

17. Czy dane osobowe są transferowane do państw spoza Europejskiego Obszaru Gospodarczego?

Dotyczy to również przypadków hostingu danych na serwerach zlokalizowanych w takich państwach.

18. Czy prowadzą Państwo aktywny marketing lub e-marketing?

19. Czy oczekują Państwo przeprowadzenia szkoleń dla pracowników? Jeśli tak, to dla jakiej liczby osób, mają zostać przeprowadzone?

20. Prosimy o informację czy szkolenia miałyby być przeprowadzone dla:

- Zespołu uczestniczącego we wdrożeniu wymagań RODO?

- Członków Zarządu i kadry kierowniczej?

- Wszystkich pracowników?

Prosimy o wskazanie przewidywalnej liczby osób, w podziale na wyżej wymienione grupy.

21. Czy oczekują Państwo przygotowania materiałów szkoleniowych do wykorzystania np. w formie e-learningu?

22. Adres siedziby i innych lokalizacji prowadzenia działalności

23. Liczba pracowników w podziale na główne grupy (np. administracja, pracownicy IT, eksploatacja, biuro obsługi Klienta)

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

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

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

27. Czy Klient posiada dokumentację ochrony danych osobowych zgodną z UODO (politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym)?
28. Czy został powołany Administrator Bezpieczeństwa Informacji odpowiedzialny za nadzór nad przestrzeganiem zasad przetwarzania danych osobowych ?
29. Liczba zidentyfikowanych zbiorów danych osobowych
30. Czy Klient zgłosił bazy danych do GIODO (jeśli tak, jakie to były bazy) ?
31. Czy Klient przechodził kiedykolwiek audyt informatyczny lub prawny ochrony danych i czy jest w posiadaniu dokumentacji z audytu (raport, rekomendacje itp.)?
32. Czy zarządzanie IT jest scentralizowane? Jeśli nie, prosimy o opisanie, które elementy IT są zarządzane lokalnie w poszczególnych lokalizacjach.
33. Czy występuje outsourcing usług IT? Jeśli tak, to jakie funkcje IT i jakie systemy są outsourcowane?
34. Liczba systemów IT , w ramach których przetwarzane są dane osobowe
35. Jakie firmy zewnętrzne przetwarzają dane osobowe (np. zewnętrzne biuro rachunkowe, zewnętrzne wsparcie IT)? Proszę podać szacunkową liczbę takich podmiotów.
36. Czy zawarto umowy powierzenia przetwarzania danych osobowych z firmami zewnętrznymi ? Liczba takich umów.
37. Czy audytowi oraz wdrożeniu mają podlegać również spółki zależne Holdingu czy tylko spółka dominująca?
38. Jeśli audytowi oraz wdrożeniu mają podlegać również spółki zależne, prosimy o udzielenie odpowiedzi na pytania 1-15 dla każdej ze spółek, która ma podlegać ocenie.
39. Jaka jest ilość wewnętrznych aktów normatywnych? OPZ Pkt I.1
40. Jaka ilość roboczogodzin/roboczości Zamawiający zamierza wykorzystać na bieżące doradztwo w trakcie trwania umowy? OPZ III.4
41. Czy Zamawiający uzna za spełniające wymagania referencje otrzymane od instytucji publicznych na poziomie ministerstwa?

42. Czy Zamawiający uzna za spełniające wymagania referencje otrzymane z rynku komercyjnego?
43. Czy Zamawiający uzna za spełniające wymagania referencje nie związane bezpośrednio z RODO, a dotyczące bezpieczeństwa danych i systemów informatycznych?
44. Prosimy o wydłużenie terminu składania ofert do 24.04.2018 r.

Odpowiedzi

1. Zakres Zapytania Ofertowego obejmuje wszystkie spółki z Grupy Kapitałowej Polski Holding Nieruchomości S.A.
2. Zakres prac opisanych w Zapytaniu Ofertowym obejmuje spółki zlokalizowane w Warszawie, Gdyni i Wrocławiu
3. Zamawiający wymaga aby prace rozpoczęły się niezwłocznie po podpisaniu umowy
4. Nie, zamawiający nie oczekuje przejęcia obowiązków IOD od 25.05.2018
5. Zamawiający szacuje, że dostęp do przetwarzanych danych osobowych ma 170 osób.
6. W strukturze organizacyjnej Spółki dominującej wyodrębniono 10 biur
7. W skład Grupy Kapitałowej wchodzi 46 Spółek pomiędzy którymi następuje wymiana danych osobowych
8. Tak, w Spółce powołany jest Administrator Bezpieczeństwa Informacji
9. Nie, w Spółce nie wdrożono normy ISO 27001
10. Spółka posiada kompletną dokumentację wymaganą przez obowiązujące przepisy w zakresie ochrony danych osobowych
11. Zamawiający w Zapytaniu Ofertowym wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu obowiązujących wewnętrznych aktów normatywnych
12. Zamawiający w Zapytaniu Ofertowym wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom

13. Zamawiający w Zapytaniu Ofertowym wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu obowiązujących wewnętrznych aktów normatywnych w tym także weryfikacji zgód na przetwarzanie danych osobowych, weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom, weryfikacji procedur realizacji praw osób których dane są przetwarzane.
14. Zamawiający w Zapytaniu Ofertowym wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu procesów, w których dochodzi do przetwarzania danych osobowych
15. Zamawiający w Zapytaniu Ofertowym wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu rozwiązań technicznych, organizacyjnych i informatycznych w zakresie ochrony danych osobowych dotyczących funkcjonalności i zastosowanych sposobów zabezpieczeń danych osobowych w systemach informatycznych
16. Zamawiający nie przetwarza danych wrażliwych
17. Dane osobowe nie są transferowane do państw spoza Europejskiego Obszaru Gospodarczego
18. Zamawiający prowadzi działania marketingowe i e-marketingowe.
19. Tak. Szkolenia powinny objąć od 20 - 30 pracowników Zamawiający w Zapytaniu Ofertowym wymaga aby Wykonawca przeprowadził certyfikowane szkolenie w siedzibie Zamawiającego dla co najmniej 20 osób z zakresu zasad przetwarzania i zabezpieczania danych osobowych w tym omówienie zmian wynikających z nowego rozporządzenia o ochronie danych osobowych.
20. Zamawiający w Zapytaniu Ofertowym wymaga aby Wykonawca przeprowadził certyfikowane szkolenie w siedzibie Zamawiającego dla co najmniej 20 osób z zakresu zasad przetwarzania i zabezpieczania danych osobowych w tym omówienie zmian wynikających z nowego rozporządzenia o ochronie danych osobowych.
21. Zamawiający nie oczekuje przygotowania materiałów do wykorzystania w formie e-learningu
22. Polski Holding Nieruchomości S.A. z siedzibą w Warszawie, przy ul. Jana Pawła II 12, prowadzi działalność na terenie całego kraju
23. Wszelkie informacje niezbędne do przedstawienia oferty i podlegające udostępnieniu są zawarte w Zapytaniu Ofertowym. Zamawiający na tym etapie postępowania nie przewiduje możliwości

informowania Oferentów o szczegółach dotyczących struktury organizacyjnej. Dane takie zostaną udostępnione Wykonawcy po podpisaniu umowy o zachowaniu poufności

24. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu wszystkich procesów, w których dochodzi do przetwarzania danych osobowych, w tym w szczególności: określenia podstaw przetwarzania danych osobowych, weryfikacji w zakresie obowiązków informacyjnych realizowanych przez PHN, weryfikacji zgód na przetwarzanie danych osobowych, weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom, weryfikacji procedur realizacji praw osób których dane są przetwarzane;
25. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu wszystkich procesów, w których dochodzi do przetwarzania danych osobowych, w tym w szczególności: określenia podstaw przetwarzania danych osobowych, weryfikacji w zakresie obowiązków informacyjnych realizowanych przez PHN, weryfikacji zgód na przetwarzanie danych osobowych, weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom, weryfikacji procedur realizacji praw osób których dane są przetwarzane;
26. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu wszystkich procesów, w których dochodzi do przetwarzania danych osobowych, w tym w szczególności: określenia podstaw przetwarzania danych osobowych, weryfikacji w zakresie obowiązków informacyjnych realizowanych przez PHN, weryfikacji zgód na przetwarzanie danych osobowych, weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom, weryfikacji procedur realizacji praw osób których dane są przetwarzane;
27. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu obowiązujących wewnętrznych aktów normatywnych;
28. W Spółce jest powołany Administrator Bezpieczeństwa Informacji
29. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał identyfikacji zbiorów danych osobowych oraz weryfikacji obszarów przetwarzania danych.

30. Zamawiający wypełnił spoczywający na nim obowiązek i dokonał zgłoszenia zbiorów danych osobowych do GIODO.
31. Wszelkie informacje niezbędne do przedstawienia oferty i podlegające udostępnieniu są zawarte w Zapytaniu Ofertowym. Zamawiający na tym etapie postępowania nie przewiduje możliwości informowania Oferentów o przeprowadzanych audytach. Informacje w tym zakresie mogą zostać udzielone Wykonawcy po podpisaniu umowy o zachowaniu poufności.
32. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu rozwiązań technicznych, organizacyjnych i informatycznych w zakresie ochrony danych osobowych dotyczących funkcjonalności i zastosowanych sposobów zabezpieczeń danych osobowych w systemach informatycznych;
33. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu rozwiązań technicznych, organizacyjnych i informatycznych w zakresie ochrony danych osobowych dotyczących funkcjonalności i zastosowanych sposobów zabezpieczeń danych osobowych w systemach informatycznych;
34. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu rozwiązań technicznych, organizacyjnych i informatycznych w zakresie ochrony danych osobowych dotyczących funkcjonalności i zastosowanych sposobów zabezpieczeń danych osobowych w systemach informatycznych;
35. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom.
36. Zgodnie z treścią Zapytania Ofertowego Zamawiający wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał weryfikacji w zakresie powierzenia przetwarzania danych osobowych innym podmiotom.
37. Tak, zakres czynności opasanych w Zapytaniu Ofertowym dotyczy wszystkich spółek z GK
38. Zakres czynności opisanych w Zapytaniu Ofertowym dotyczy wszystkich spółek z GK. Wszelkie informacje niezbędne do przedstawienia oferty i podlegające udostępnieniu są zawarte w Zapytaniu Ofertowym.

39. Zamawiający w Zapytaniu Ofertowym wymaga aby w ramach analizy stanu bezpieczeństwa to Wykonawca dokonał przeglądu obowiązujących wewnętrznych aktów normatywnych.
40. Przez „bieżące doradztwo z zakresu ochrony danych osobowych w trakcie wykonywania umowy” Zamawiający rozumie udzielanie rekomendacji wynikających z Raportu z przeprowadzonej analizy stanu bezpieczeństwa dotyczącego obszarów, które wymagają zapewnienia zgodności z rozporządzeniem o ochronie danych osobowych. Zamawiający nie jest w stanie oszacować liczby roboczogodzin bez Raportu z przeprowadzonej analizy stanu bezpieczeństwa.
41. Zamawiający zgodnie z treścią Zapytania Ofertowego uznaje referencje od instytucji publicznych na poziomie ministerstwa. Jednocześnie zgodnie z Zapytaniem Ofertowym dodatkowe punkty przyznawane są za podpisanie umowy odpowiadającej zakresem niniejszemu postępowaniu tj. w zakresie przygotowania dokumentacji i procedur dotyczących Ochrony Danych Osobowych lub RODO z podmiotem będącym Grupą Kapitałową Spółek Skarbu Państwa
42. Zamawiający zgodnie z treścią Zapytania Ofertowego uznaje referencje z rynku komercyjnego. Jednocześnie zgodnie z Zapytaniem Ofertowym dodatkowe punkty przyznawane są za podpisanie umowy odpowiadającej zakresem niniejszemu postępowaniu tj. w zakresie przygotowania dokumentacji i procedur dotyczących Ochrony Danych Osobowych lub RODO z podmiotem będącym Grupą Kapitałową Spółek Skarbu Państwa
43. Nie, Zamawiający wymaga aby Wykonawca posiadał doświadczenie w realizacji wdrożeń związanych z wymogami 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 „RODO”).
44. Zamawiający nie przewiduje zmiany terminu składania ofert.