ZARZĄD TRANSPORTU MIEJSKIEGO
ul. Żelazna 61, 00-848 Warszawa, tel. 22 459 41 00, faks. 22 459 42 43
ztm@ztm.waw.pl, www.ztm.waw.pl

ZTM-NZ.2610.101.2018.DMA

Warszawa, dnia 22.02.2018 r.

Sz. Wykonawcy

Dotyczy: **przetarg nieograniczony nr 21/2018 na usługę polegającą na kompleksowym wsparciu w procesie wdrożenia przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.**

Zamawiający, Zarząd Transportu Miejskiego w Warszawie, działając na podstawie rozdziału III pkt 4 Specyfikacji Istotnych Warunków Zamówienia(dalej w skrócie: „SIWZ"), udziela odpowiedzi na pytania, które wpłynęły do treści SIWZ:

Pytanie 1
Ile Zamawiający posiada zwartych umów powierzenia przetwarzania danych osobowych?
Odpowiedź: Zarząd Transportu Miejskiego posiada ok 550 umów powierzenie przetwarzania danych osobowych, zaznaczając że ok 500 umów stanowi ten sam rodzaj usługi.

Pytanie 2
Czy "dostosowanie systemów informatycznych w sposób umożliwiający realizowanie praw osób nałożonych RODO" oznacza wykonanie zmian w oprogramowaniu czy tylko wskazanie niezbędnych zmian funkcjonalności systemów?
Odpowiedź: Oznacza rekomendacje wskazujące niezbędne zmiany jakie muszą zostać wykonane.

Pytanie 3
Ile systemów informatycznych przetwarzających dane osobowe posiada Klient?
Odpowiedź: ZTM wykorzystuje 14 systemów informatycznych.

Pytanie 4
Ile procesów biznesowych, w których dochodzi do przetwarzania danych osobowych posiada Klient?
Odpowiedź: ZTM posiada ok 43 procesy biznesowe w których przetwarzane są dane osobowe.

Pytanie 5
Ile formularzy posiadają aplikacje webowe o których mowa w kontekście testów penetracyjnych?
Odpowiedź: Każda z aplikacji webowych wykorzystuje 1 formularz.

Pytanie 6
Jakie systemy informatyczne posiada Zamawiający?
Odpowiedź: Odpowiedzi na to pytanie możemy udzielić po rozstrzygnięciu przetargu i podpisaniu umowy.

Pytanie 7
Czy wyszczególnione systemy (które) są outsourcingowane?
Odpowiedź: Nie posiadamy systemów outsourcingowych.

Pytanie 8
Jakie bazy danych wykorzystuje organizacja?
Odpowiedź: Wykorzystujemy standardowe bazy danych dostępne na rynku tj.np. Oracle, MSSQL.

Pytanie 9
Czy zamawiający posiada wdrożone zasady nadawania dostępów użytkownikom do systemów informatycznych i czy jest wdrożony system klasy PAM?
Odpowiedź: Posiadamy wdrożone zasady nadawania dostępów użytkownikom do systemów informatycznych.

Pytanie 10
Czy w organizacji zamawiającego są prowadzone przeglądy weryfikujące do jakich systemów i aplikacji mają dostęp pracownicy?
Odpowiedź: Odpowiedzi na to pytanie możemy udzielić po rozstrzygnięciu przetargu i podpisaniu umowy.

Pytanie 11
Czy organizacja stosuje zasady zakazujące wykorzystywania tych samych loginów i haseł przez różnych pracowników?
Odpowiedź: Tak.

Pytanie 12
Czy pracownicy muszą zalogować się do systemów, by móc z nich skorzystać?
Odpowiedź: Tak.

Pytanie 13
Czy w siedzibie firmy jest dostępna dedykowana i odseparowana sieć dla gości?
Odpowiedź: Odpowiedzi na to pytanie możemy udzielić po rozstrzygnięciu przetargu i podpisaniu umowy.

Pytanie 14
Czy dostępu do brzegu sieci chroni rozwiązanie służące do blokowania nieautoryzowanego dostępu z sieci Internet?
Odpowiedź: Tak.

Pytanie 15
Czy zamawiający udostępnia aplikację / usługę internetową dla swoich Klientów lub pracowników dostępną z Internetu?
Odpowiedź: Tak

Pytanie 16
Czy w organizacji stosuje się zabezpieczenia przed szkodliwym oprogramowaniem, np. wirusami i nowymi formami ataku?
Odpowiedź: Tak

Pytanie 17
Czy w organizacji jest stosowane oprogramowanie niewspierane przez dostawców wskazanych systemów?
Odpowiedź: Odpowiedzi na to pytanie możemy udzielić po rozstrzygnięciu przetargu i

podpisaniu umowy.

Pytanie 18
Czy Zamawiający tworzy własne oprogramowanie?
Odpowiedź: Tak.

Pytanie 19
Czy tworząc nowe oprogramowanie lub kupując oprogramowanie zwracana jest uwaga na kwestie bezpieczeństwa danych osobowych (privacy by design" oraz „privacy by default)?
Odpowiedź: Tak

Pytanie 20
Czy zamawiający posiada dedykowane rozwiązanie służące do zbierania informacji o działaniu systemów IT i ich użytkowników oraz analizowaniu tych informacji pod kątem wystąpienia incydentu bezpieczeństwa IT?
Odpowiedź: Zamawiający posiada rozwiązania służące do zbierania informacji o działaniu systemów IT.

Pytanie 21
Czy jest proces zgłaszania incydentów IT?
Odpowiedź: Tak w Zarządzie Transportu Miejskiego jest wdrożony proces zgłaszania incydentów do działu IT.

Pytanie 22
Czy w organizacji zamawiającego jest wdrożony system zarządzania bezpieczeństwem informacji?
Odpowiedź: Tak w Zarządzie Transportu Miejskiego jest wdrożony system zarządzania bezpieczeństwem informacji.

Pytanie 23
Uprzejmie proszę o doprecyzowanie warunków udziału w postępowaniu punkt 1.2
1.2.1 posiada co najmniej 5 letnie doświadczenie w zakresie prawa ochrony danych osobowych;
1.2.2. w okresie ostatnich 5 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie lub wykonuje należycie:

- co najmniej 5 audytów z zakresu ochrony danych osobowych;
- co najmniej 5 audytów prawnych;
- co najmniej 3 kompleksowe testy penetracyjne (black-box i gay-box) systemów teleinformatycznych.

Punkt 1.2.2 mówi, że podmiot w okresie ostatnich 5 lat lub jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wykonała następujące usługi....
Natomiast punkt 1.2.1 mówi, że posiada co najmniej 5 letnie doświadczenie i brakuje informacji jeżeli okres działalności jest krótszy - w tym okresie posiada x lat doświadczenia.
Czy firma działająca od 2015 roku i od początku zajmująca się ochroną danych osobowych spełnią punkt 1.2.1?

Odpowiedź:
Kwestie zawarte w punkcie w brzmieniu: 1.2.1 posiada co najmniej 5 letnie doświadczenie w zakresie prawa ochrony danych osobowych oznaczają, że podmiot powinien posiadać minimum pięcioletnie udokumentowane doświadczenie w pracach (w szczególności: wdrożeniu, utrzymywaniu systemów ochrony, pełnienia funkcji ABI) w zakresie ochrony danych osobowych o których mowa w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

(Dz.U.2016 r. poz. 922) oraz aktach wykonawczych do niej (w tym: Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024)),
Co do punktu 1.2.2. - warunki dotyczą:

1. Ad. przeprowadzenie audytów prawnych - badania zgodności przetwarzanej dokumentacji wewnętrznej (w szczególności: umów, przepisów i innych) z przepisami ogólnie obowiązującymi.
2. Ad. przeprowadzenie audytów danych osobowych – podobnie jak wyżej, ale z skonkretyzowaniem na ochronę danych osobowych, o których mowa w przepisach obecnie obowiązujących, tj. w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016 r. poz. 922) oraz aktach wykonawczych do niej, jak również w przepisach zawartych w Rozporządzeniu 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.
3. Odnośnie testów penetracyjnych - black-box i gray-box systemów teleinformatycznych - całej infrastruktury teleinformatycznej mającej wpływ na bezpieczeństwo informacji.

Ocena spełniania warunków udziału w postępowaniu będzie dokonana przez komisję przetargową na podstawie dokumentów złożonych wraz z ofertą.

DYREKTOR
Zarządu Transportu Miejskiego
Wiesław Witek