Chorzów, dnia 05.02.2018 r.

Dotyczy: postępowania o udzielenie zamówienia sektorowego - nr sprawy: DL/155/2018.

W związku z pytaniami Wykonawcy do postępowania sektorowego prowadzonego w formie przetargu pisemnego pn.: Wykonanie audytu funkcjonującej w spółce Tramwaje Śląskie S.A. ochrony danych osobowych oraz przygotowanie dokumentacji zgodnej 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") - nr sprawy: DL/155/2018, wyjaśniam:

Pytanie nr 1

Wielkość firmy w liczbach:

a. zatrudnienie
b. oddziały
c. ilość struktur wewnętrznych (biura, działy, departamenty)
d. ilość spółek zależnych
e. konieczność przekazywania danych osobowych za granicę oraz poza EOG (ile i jakie kraje)
f. obecna ilość zidentyfikowanych zbiorów danych osobowych
g. profil działalności

Odpowiedź:

a. Zamawiający zatrudnia aktualnie 1650 osób, w tym na stanowiskach nierobotniczych 285 osób.
b-c Strukturę organizacyjną Spółki prezentuje schemat, który dostępny jest pod adresem:
http://www.tram-silesia.pl/www/wp-content/uploads/2009/12/Schemat-organizacyjny2.pdf

Dodatkowo każdy Rejon od nr 1 do nr 4 (odpowiednio Będzin, Katowice, Bytom, Gliwice) posiada wewnętrzną strukturę organizacyjną w skład, której wchodzą po 3 wewnętrzne komórki organizacyjne podległe właściwemu Kierownikowi Rejonu. Zakłady posiadają również wewnętrzną strukturę i tak: ZUR – 5 wewnętrznych komórek organizacyjnych podległych Kierownikowi ZUR, natomiast ZTS – 3 wewnętrzne komórki organizacyjne podległe Kierownikowi ZTS, wewnętrzną strukturę organizacyjną posiada także Dział Zamówień Publicznych i Zaopatrzenia (FZ) - 7 wewnętrznych komórek organizacyjnych podległych Kierownikowi FZ w tym 5 magazynów.

d. Zamawiający nie posiada spółek zależnych.

e. Dotychczas Zamawiający nie był zobowiązany do przekazywania danych osobowych poza granicę oraz poza EOG.

f. Identyfikacja zbiorów danych osobowych jest dokonywana przez Zamawiającego przy zachowaniu podziału na zbiory danych osobowych przetwarzanych w tradycyjnej formie papierowej i w systemie informatycznym. W odniesieniu do zbiorów danych osobowych przetwarzanych w tradycyjnej formie papierowej Zamawiający identyfikuje 8 zbiorów danych. Z kolei w odniesieniu do zbiorów danych osobowych przetwarzanych w systemie informatycznym Zamawiający identyfikuje 5 zbiorów danych.

g. Profil (przedmiot) działalności Spółki określony jest szczegółowo w KRS a także pod adresem:
http://www.tram-silesia.pl/www/index.php/bip/przedmiot/

Pytanie nr 2

Ogólna charakterystyka działu IT – stan osobowy, zakres obowiązków, ilość systemów - w tym o charakterze krytycznym, stosowane technologie, etc.,

Odpowiedź:

Dział Obsługi Informatycznej realizuje na rzecz Zamawiającego całokształt zadań związanych z zagadnieniami informatyki oraz łączności telefonicznej stacjonarnej i mobilnej, a także organizuje i realizuje, całość zagadnień i prac związanych z komputeryzacją Spółki. Do zakresu Działu Obsługi Informatycznej należy również

administrowanie serwerami systemów, zarządzanie infrastrukturą sieciową oraz archiwizacja baz danych systemów informatycznych.

Kierownik Działu Obsługi Informatycznej wykonuje jednocześnie funkcję ASI.

W Dziale zatrudnionych jest aktualnie 8 osób, których zakres obowiązków wynika wprost z zadań realizowanych przez ten Dział. Spółka pracuje na dwóch wielomodułowych systemach informatycznych (IMPULS, MUNICOM) przetwarzających dane osobowe oraz na systemie PŁATNIK. Jednocześnie zamawiający informuje, iż nie użytkuje systemów krytycznych, tzn. takich których awaria lub nieprawidłowe działanie może skutkować śmiercią lub poważnymi obrażeniami ludzi, utratą bądź poważnymi uszkodzeniami urządzeń albo zanieczyszczeniem środowiska.

Pytanie nr 3

Czy firma korzysta z własnej infrastruktury IT? Z iloma systemami zewnętrznymi firma się komunikuje i za pomocą jakich technologii, kanałów, itp.? (chodzi o oszacowanie zewnętrznych systemów, z których mogą być pozyskiwane lub eksportowane dane).

Odpowiedź:

Zamawiający wyjaśnia, że jedynym elementem infrastruktury IT, który podlega dzierżawie jest łącze światłowodowe. Pozostałe elementy infrastruktury IT stanowią własność Zamawiającego.
Poza systemem PŁATNIK zamawiający nie komunikuje się z systemami zewnętrznymi umożliwiającymi migrację lub udostępnianie danych osobowych.

Pytanie nr 4

W ilu fizycznych lokalizacjach umieszczono zasoby informatyczne? Czy istnieje Centrum zapasowe, a jeśli tak, to w jakiej miejscowości jest zlokalizowane?

Odpowiedź:

Zasoby informatyczne wykorzystywane do przetwarzana danych osobowych zlokalizowane są w ośmiu tzw. obszarach przetwarzania danych osobowych. Zamawiający nie posiada Centrum zapasowego.

Pytanie nr 5

Jakie są podstawowe funkcje biznesowe poszczególnych aplikacji i jakie operacje można na nich wykonywać?

Odpowiedź:

Zamawiający wyjaśnia, że wielomodułowy system IMPULS (system ERP) gromadzi i integruje bazy danych z obszarów kadr, płac, gospodarki magazynowej, księgowości, gospodarowania środkami trwałymi, z kolei system MUNICOM gromadzi dane z zakresu planowania i realizacji zadań przewozowych.

Pytanie nr 6

Prosimy o informację czy w organizacji został wyznaczony ABI i ASI oraz czy ustanowiono role odpowiedzialne za bezpieczeństwo informacji?

Odpowiedź:

Tak. U Zamawiającego wyznaczone zostały osoby pełniące obowiązki ABI i ASI jak również upoważniono właściwe osoby do przetwarzania danych osobowych.

Pytanie nr 7

Prosimy o informację, czy i jakie działania związane z przetwarzaniem danych osobowych są outsourcowane (realizowane przez firmy zewnętrzne)? Np. wydruk faktur, mailing marketingowy, kadry / płace, IT, recepcja, bezpieczeństwo obiektowe i osobowe). Czy z tymi firmami zostały podpisane umowy przetwarzania?

Odpowiedź:

Zamawiający jako Administrator Danych nie powierzył innemu podmiotowi przetwarzania danych w drodze umowy, o której mowa jest w art. 31 ustawy o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 z późn.zm.).

Pytanie nr 8

Czy w związku z działaniami określonymi w pkt. 7 zostały zawarte umowy powierzenia danych osobowych?

Odpowiedź:
Por. odpowiedź na pytanie 7.

Pytanie nr 9
Jakie dane firma przetwarza - pracownicze, handlowe, produkcyjne inne?
Odpowiedź:
Przetwarzane przez Zamawiającego dane osobowe mają głownie charakter pracowniczy (np. akta osobowe pracowników) i handlowy (np. rejestr umów i kontrahentów).

Pytanie nr 10
Czy firma przetwarza dane osobowe wrażliwe?
Odpowiedź:
Zamawiający nie przetwarza danych osobowych wrażliwych, o których mowa jest w art. 27 ustawy o ochronie danych osobowych.

Pytanie nr 11
Czy zakres prac ma obejmować przegląd zgodności z wymaganiami RODO, czy tylko z obecnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych?
Odpowiedź:
Tak. Zgodnie z opisem przedmiotu zamówienia zakres prac powinien obejmować przegląd zgodności funkcjonującej w spółce Tramwaje Śląskie S.A. ochrony danych osobowych oraz przygotowanie dokumentacji zgodnej 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").

Pytanie nr 12
Ile osób należy przeszkolić, jeśli jest taka potrzeba?
Odpowiedź:
Zgodnie z ust. 1 pkt. 6 opisu przedmiotu zamówienia szczegółowy zakres zamówienia obejmuje przeprowadzenie w miejscu uzgodnionym z Zamawiającym certyfikowanego szkolenia dla grupy 15 osób wyznaczonych przez Zamawiającego z zakresu zasad przetwarzania i zabezpieczania danych osobowych, w tym na tle zmian wynikających z RODO.

Pytanie nr 13
W ilu lokalizacjach należy przeprowadzić badanie? Czy wszystkie lokalizacje znajdują się na terytorium Polski, jeżeli nie - to gdzie?
Odpowiedź:
Zamawiający oczekuje od Wykonawcy przedstawienia metodologii i założeń badania audytowego, przy czym dane osobowe przetwarzane są przez Zamawiającego z użyciem tradycyjnej formy jak również stacjonarnego lub przenośnego sprzętu komputerowego w ośmiu tzw. obszarach przetwarzania danych osobowych. Wszystkie lokalizacje w których Zamawiający przetwarza dane osobowe znajdują się na terytorium Polski.

Pytanie nr 14
Czy organizacja ma wdrożony System Zarządzania Bezpieczeństwem Informacyjnym?
W szczególności, czy wdrożono podstawowe składniki dokumentacji przetwarzania danych osobowych (Polityka bezpieczeństwa, wymagane instrukcje)?
Odpowiedź:
Tak. Zamawiający posiada wdrożoną dokumentację dotyczącą przetwarzania danych osobowych, na którą składają się: Polityka bezpieczeństwa danych osobowych w Tramwajach Śląskich S.A. oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Pytanie nr 15
Czy istnieje udokumentowany system nadawania upoważnień do przetwarzania danych osobowych?

Odpowiedź:
Tak. Zamawiający ustalił zasady nadawania upoważnień do przetwarzania danych osobowych.

Pytanie nr 16
Jaki jest sposób udostępniania aplikacji? (np. poprzez przeglądarkę internetową użytkownika, inne). Czy system udostępniania aplikacji został sformalizowany?
Odpowiedź:
Zamawiający wyjaśnia, że aplikacje mogą być udostępniane za pomocą technologii zdalnego pulpitu albo też poprzez udostępnienie skrótu do danej aplikacji. Nadawanie uprawnień do konkretnej aplikacji odbywa się na podstawie indywidualnych loginów i haseł dostępu.

Pytanie nr 17
Jaki jest sposób uwierzytelniania użytkowników w aplikacji?
Odpowiedź:
Uwierzytelnienie użytkowników w aplikacjach (programach komputerowych) odbywa się na podstawie indywidualnych loginów i haseł dostępu.

Pytanie nr 18
Prosimy o informację, ile mniej więcej osób dotychczas jest zaangażowanych w przetwarzanie danych osobowych w jednostce?
Odpowiedź:
Zamawiający upoważnił 309 osób do przetwarzania danych osobowych.

Pytanie nr 19
Prosimy o informację ilu podmiotom zewnętrznym są udostępniane dane osobowe?
Odpowiedź:
W ocenie Zamawiającego pytanie jest nieprecyzyjne. Co do zasady pomijając wewnętrzne udostępnienia danych, Zamawiający udostępnia dane osobowe pracowników na zewnątrz wyłącznie na wezwanie uprawnionych organów lub instytucji.

Pytanie nr 20
Czy zakres prac ma obejmować kompleksowy przegląd zgodności z wymaganiami RODO, przegląd własnych rozwiązań, czy opracowanie projektów nowych procedur? Czy przegląd ma obejmować regulacje wyłącznie w zakresie, w jakim dotyczą one danych osobowych? Prosimy o potwierdzenie.
Odpowiedź:
Zgodnie z opisem przedmiotu zamówienia zakres prac ma obejmować przegląd zgodności funkcjonującej w spółce Tramwaje Śląskie S.A. ochrony danych osobowych oraz przygotowanie dokumentacji zgodnej 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").

Pytanie nr 21
Jakie są możliwe daty oraz godziny przeprowadzenia prac w siedzibie Zamawiającego, a także zdalna dostępność?
Odpowiedź:
Zamówienie powinno być wykonane w terminie do dnia 16.04.2018 r. Z kolei wszelkie prace audytowi powinny być prowadzone w dni robocze tj. od poniedziałku do piątku, po wcześniejszym uzgodnieniu z Zamawiającym. Zamawiający dopuszcza możliwość wzajemnego kontaktowania się z wykorzystaniem elektronicznych środków komunikowania.

Pytanie nr 22
Prosimy o informację czy raport będzie przygotowywany tylko w języku polskim.
Odpowiedź:
Tak. Raport z audytu oraz dokumentacja RODO powinny być przygotowane w języku polskim.