Tomaszów Lubelski; 30 kwietnia 2021 r.

ZAMAWIAJĄCY:
Sąd Rejonowego w Tomaszowie Lubelskim
ul. Lwowska 55
22-600 Tomaszów Lubelski

DOTYCZY:
Adm-263-15/21
Zaproszenia do składania ofert *na wykonywanie kompleksowej usługi z zakresu ochrony danych osobowych oraz pełnienia funkcji Inspektora Ochrony Danych dla Prezesa, Dyrektora i Sądu Rejonowego w Tomaszowie Lubelskim.*

W związku z wpłynięciem zapytania do oferty *na wykonywanie kompleksowej usługi z zakresu ochrony danych osobowych oraz pełnienia funkcji Inspektora Ochrony Danych dla Prezesa, Dyrektora i Sądu Rejonowego w Tomaszowie Lubelskim* uprzejmie udzielam wyjaśnień.

Pytanie 1
Czy weryfikacja (co najmniej raz na kwartał) zabezpieczeń funkcjonujących u Zamawiającego w zakresie przetwarzania danych winna być świadczona w zakresie o którym mowa w art.32 ust.1 lit. d) i dotyczyć także zabezpieczeń technicznych? W szczególności czy Wykonawca (raz na kwartał) winien wykonywać testy podatności zasobów IT?
Odpowiedź do pytania 1:
Zgodnie z art. 32 ust.1 lit. d *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)* administrator podzielił środki zabezpieczenia na dwie grupy: środki techniczne i środki organizacyjne. Pierwsza grupa odnosi się do rozwiązań technicznych (np. zamki w drzwiach, systemy alarmowe, zabezpieczenie dostępu hasłem w systemie informatycznym, szyfrowanie danych zawartych na dysku itp.), natomiast druga grupa dotyczy rozwiązań w zakresie organizacji przetwarzania danych (np. wyodrębnienie stref ograniczonego dostępu, kontrola dostępu do zasobów informatycznych, do kluczy, odpowiednie ustawienie monitora komputerowego, prawa dostępu itp.). W przypadku odporności systemu chodzi o uniemożliwienie ingerencji w systemy informatyczne Zamawiającego (dostępu osób nieupoważnionych), w szczególności uodpornienie systemów informatycznych lub procesów przetwarzania na ataki z zewnątrz (na przykład z użyciem oprogramowania postrzeganego przez systemy antywirusowe jako szkodliwe). Ogólne rozporządzenie o ochronie danych wymaga, aby w przypadku naruszenia fizycznego lub technicznego ochrony danych (jako efektu zastosowanych odpowiednio środków organizacyjnych i technicznych), ich integralności i/lub poufności – środki techniczne i organizacyjne zapewniały zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich. Chodzi więc o jak najszybsze przywrócenie możliwości dostępu do danych osobom upoważnionym, jak również przywrócenie im możliwości dokonywania operacji na danych. Analogicznie administrator ma również obowiązek zapewnienia odpowiednich środków technicznych i organizacyjnych,

o których mowa w art. 32 ust. 1 RODO, które mają charakter dynamiczny, gdyż ustawodawca unijny wymaga regularnego testowania, mierzenia i oceniania skuteczności zastosowanych środków dla zapewnienia bezpieczeństwa w stopniu, odpowiadającym ryzyku. Mając na uwadze powyższe w zakresie zapewniającym bezpieczeństwo danych osobowych Administrator Systemów Informatycznych (ASI) dokonuje permanentnej kontroli systemu informatycznego (mierzy, testuje i ocenia skuteczność środków technicznych w zakresie software jak i hardware oraz dba o zapewnienie organizacyjnych rozwiązań zmierzających do skutecznej ochrony poprzez politykę nadawania uprawnień dostępu, backup-y, szkolenia, stosowania polityk bezpieczeństwa ustalonych dla sądów powszechnych mających swoją rangę w strukturze sądownictwa powszechnego w zależności od potencjalnego ryzyka).

Dalego też, powyższy zapis w §3 ust. 2 pkt 3 wzoru umowy tj. „*Weryfikacja (co najmniej raz na kwartał) zabezpieczeń funkcjonujących u Zamawiającego w zakresie przetwarzania danych w celu doprowadzenia do stanu zgodnego z obowiązującym prawem*" należy rozumieć jako weryfikowanie opisanych powyżej stosowanych środków zabezpieczenia technicznego i organizacyjnego u Zamawiającego przez Wykonawcę przy ścisłej współpracy z ASI i prowadzenie w tym zakresie dokumentacji oraz zgłaszaniu wniosków o zmiany rozwiązań technicznych lub organizacyjnych pozwalających utrzymać zabezpieczenia techniczne i organizacyjne na odpowiednim poziomie zgodne z normami prawnymi, dobrymi praktykami i wytycznymi w tym zakresie, jak również wytycznymi jednostek nadrzędnych Zamawiającego nawet, jeżeli te wytyczne znacznie wykraczają poza minimalne wymagania ustawowe. Sposób wykonywania zapisów §3 ust. 2 pkt 3 wzoru umowy przez Wykonawcę musi być zgodny z normami prawnymi, dobrymi praktykami i nie naruszać Polityk bezpieczeństwa obowiązujących u Zamawiającego, a jednocześnie prowadzić do realizacji art. 32 ust.1 lit. d RODO.

Co do ostatniej części pytania Zamawiającego „*W szczególności czy Wykonawca (raz na kwartał) winien wykonywać testy podatności zasobów IT?*" Wykonawca nie posiada informacji od Pytającego jakie mają być to testy „podatności zasobów IT". Mając na uwadze brak precyzyjnej informacji na czym miałyby polegać te testy nie może udzielić w tym zakresie odpowiedzi. Jednakże Zamawiający chce zwrócić uwagę, że art. 32 ust.1 lit. d RODO nakazuje „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania" a nie wykonywanie testów penetracyjnych.

Pytanie 2:

Proszę o określenie jaka ilość infrastruktury informatycznej winna być okresowo testowana i oceniane jej zabezpieczania (ilość serwerów, baz danych, aplikacji, urządzeń sieciowych, stron www, etc)?

Odpowiedź do pytania 2:

Wszystkie zasoby techniczne (nie tylko urządzenia informatyczne) powinny być weryfikowane. Z racji bezpieczeństwa nie udzielamy szczegółowych informacji, co do zasobów sprzętowych oraz wykorzystywanego oprogramowania przez Zamawiającego. Niezbędne informacje w tym zakresie zostaną udzielona Zamawiającemu po podpisaniu umowy wykonawczej i wyznaczeniu IOD. Do oszacowania należy przyjąć, że ze sprzętu informatycznego korzysta w sposób ciągły około 75 pracowników oraz 5 stażystów/absolwentów.

Pytanie 3:

Proszę o określenie ilu pracowników Państwo zatrudniają?

Odpowiedź do pytania 3:

75 pracowników.

Pytanie 4:
Proszę o doprecyzowanie na czym winna polegać usługa „Doradzanie przy administrowaniu systemami i infrastrukturą informatyczną w zakresie ochrony informacji.”?
Odpowiedź do pytania 4:
IOD po zapoznaniu się z procedurami bezpieczeństwa związanymi z ochroną danych osobowych u Zamawiającego powinien kreować wspomniane procedury oraz doradzać pracownikom Zamawiającego jak powinni postępować, aby nie doszło do naruszeń związanych bezpieczeństwem danych osobowych, np.:

- Kreowanie procedury haseł do systemy (złożoność, długość, okres obowiązywania),
- Reglamentacja zasobów technicznych i uprawnień,
- Szyfrowanie, wykorzystywanie sprzętu mobilnego i stacjonarnego,
- Lokalizacja baz danych zawierających dane osobowe,
- Częstotliwość i zakres beckupów, aktualizacji oprogramowania,
- itd.

Nadmieniam, że usługa powinna być prowadzona kompleksowo zgodnie z zaproszeniem ofertowym tj. wykonanie **kompleksowej** usługi *z zakresu ochrony danych osobowych oraz pełnienia funkcji Inspektora Ochrony Danych dla Prezesa, Dyrektora i Sądu Rejonowego w Tomaszowie Lubelskim*. Osoba wyznaczona przez Wykonawcę do pełnienia funkcji IOD powinna w tym zakresie posiadać odpowiednią wiedzę, co jest niezbędnym wymogiem opisanym w Rozdziale V zaproszenia ofertowego.

Nadto informuję wszystkich zainteresowanych, że:

Zaproszenie do składania ofert na wykonywanie kompleksowej *usługi z zakresu ochrony danych osobowych oraz pełnienia funkcji Inspektora Ochrony Danych dla Prezesa, Dyrektora i Sądu Rejonowego w Tomaszowie Lubelskim* prowadzone jest w trybie poza ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019) zgodnie z art. 2 ust. 1 pkt 1 o wartości szacunkowej zamówienia poniżej równowartości kwoty 130 000 złotych.

Krzysztof Kowalski; S.R. Tomaszów Lub.
Elektronicznie podpisany przez Krzysztof Kowalski; S.R. Tomaszów Lub.
Data: 2021.04.30 10:01:56 +02'00'