Orzysz, 25.11.2020 r.

Znak: WOR. 271.5.1/2.2020.MST.

dot. zapytania ofertowego na świadczenie kompleksowej obsługi w zakresie ochrony danych osobowych w tym pełnienie funkcji Inspektora Ochrony Danych oraz wykonanie audytu bezpieczeństwa informacji w Urzędzie Miejskim w Orzyszu.

Nazwa oraz adres zamawiającego: **Gmina Orzysz – Urząd Miejski w Orzyszu**

reprezentowany przez Burmistrza Orzysza, ul. Rynek 3, 12 - 250 Orzysz - znak sprawy:

WOR. 271.5.2020.MST.

Pytania do treści zapytania skierowane do Zamawiającego w dn. **24.11.2020 r.** wraz

z odpowiedziami:

1. **Pytanie:** Z czego wynika powołanie się na normę ISO 27001 , proszę o podanie podstawy prawnej i uzasadnienie formalne tego kryterium

Odpowiedź:
Zgodnie z art. 32 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; Dz. U. UE. L. 2016, poz. 119.1), zwanego dalej „RODO" administrator jest zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Treść ust. 2 w/w przepisu stanowi natomiast, iż oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Przepisy te - dotyczące bezpieczeństwa przetwarzania danych - nadają regulacji ochrony danych techniczne i organizacyjne ramy. Przepis art. 32 RODO stanowi bowiem konkretyzację wskazanej w art. 5 ust. 1 lit. f RODO zasady integralności i poufności, zgodnie z którą dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Jest to szczególnie widoczne w sformułowaniu przesłanki ocennej, na podstawie której dokonuje się ustalenia odpowiedniego stopnia bezpieczeństwa, a ujętej w art. 32 ust. 2 RODO.
Przepisy RODO nie zawierają wprost wytycznych w zakresie wyboru norm ISO, natomiast praktycy i znawcy przepisów z zakresu ochrony danych osobowych (prof. Paweł Fajgielskie [w:] *Komentarz do rozporządzenia nr 2016/679 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) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, art. 32., oraz była Prezes Urzędu Ochrony danych Osobowych w publikacji Edyta Bielak-Jomaa (red.), Dominik Lubasz (red). *[w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, Warszawa 2018, art. 32.)* zalecają się ich stosowanie

ze względu na fakt, iż normy te bazują na międzynarodowo uznanych wartościach podstawowych, tj. poufności, integralności i dostępności, do których odwołuje się także prawodawca unijny w art. 32 ust. 2 lit. b RODO. W płaszczyźnie organizacyjnej przewidują one stworzenie systemu, którego głównym zadaniem jest opracowanie adekwatnych koncepcji zarządzania bezpieczeństwa informacji, ich wdrożenie, weryfikowanie i ostatecznie stałe dopasowywanie, w tym rozwijanie. Jest to szczególnie istotne wobec podmiotów odpowiadających za istotne bezpieczeństwo informacji dotyczące danych zawartych m.in. w publicznych rejestrach dostępnych jedynie jednostkom administracji publicznej.
Norma ISO 27001 stanowi międzynarodową normę systemu zarządzania bezpieczeństwem informacji, określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji oraz obejmuje wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb tej organizacji. Jej posiadanie przez podmiot obsługujący gwarantuje wysoki standard realizacji usługi poprzez zapewnienie poufności informacji, integralności informacji i dostępności informacji przy realizacji usługi, co podlega cyklicznej certyfikacji przeprowadzanej przez jednostkę nadzorującą, akredytowaną przez Polskie Centrum Akredytacji.
Posiadanie normy ISO 27001 dokumentuje utrzymywanie odpowiednich zabezpieczeń technicznych i organizacyjnych wymaganych przepisami RODO, podnosząc ich standard i zapewniając ciągłość działania wykonywanych usług publicznych. Jest to niezmiernie istotne, szczególnie w czasach epidemii COVID-19, gdzie zdecydowana większość pracy wykonywanej przez podmioty publiczne odbywa się w sposób zdalny poza ich siedzibami i miejscami przeznaczonymi do codziennego wykonywania obowiązków pracowniczych, biorąc przy tym pod uwagę w czasie obecnych okoliczności pandemicznych często prywatne okoliczności jej realizowania przez niektórych pracowników. Zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania jest wymogiem określającym cechy (funkcje), jakie powinny spełniać systemy i usługi związane z przetwarzaniem danych osobowych. Równocześnie stanowią też realizację zasad przetwarzania wskazanych w art. 5 RODO, zwłaszcza zasady poufności i integralności (art. 5 ust. 1 lit. f) oraz minimalizacji danych (art. 5 ust. 1 lit. c).
Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
Posiadana przez potencjalnego Wykonawce usługi norma ISO 27001 pomaga stworzyć odpowiednie warunki ochrony informacji, adekwatne do ryzyka utraty, zniszczenia lub odtajnienia informacji. Certyfikowany system zarządzania bezpieczeństwem informacji stanowi zapewnienie, że ochrona danych i informacji – w szczególności przez podmioty publiczne, których obowiązek wynikający z odpowiednich przepisów prawa stanowi przetwarzanie wielu istotnych danych o osobach fizycznych o znacznej doniosłości i wadze wpływających na prawa i wolności tych osób - jest priorytetowa, bowiem jednostka administracji publicznej przetwarza znaczne ilości informacji zawierających dane osobowe, w tym również dane osobowe szczególnych kategorii, a także tajemnic prawnie chronionych, wobec których jest zobowiązana do ich przetwarzania z zachowaniem wysokiej jakości i staranności oraz najwyższych zasad ich ochrony. Brak wyraźnych unormowań prawnych ujętych w RODO, określających rodzaje technicznych i organizacyjnych środków zabezpieczenia danych skłania do poszukiwania rozwiązań uznawanych przez administratora danych osobowych za najlepsze pod względem charakteru, zakresu, kontekstu, celów i ryzyka przetwarzania danych osobowych, które mogą być pomocne administratorom do spełnienia wymogów ogólnie uregulowanych w rozporządzeniu RODO, pozostawiając im swobodę w ich doborze. Zasadnym natomiast w dobrze pojętym interesie Zamawiającego, będącego jednostką administracji publicznej jest to, aby bezpieczeństwo danych, które zostaną powierzone Wykonawcy i z jego pomocą ochraniane, było na najwyższym poziomie i stwierdzone obiektywnie przez podmiot trzeci tj. niezależną jednostkę

certyfikującą. W ocenie Zamawiającego spełnienie tego warunku nie może być obiektywnie potwierdzone w inny sposób. Posiadanie i aktualizowanie certyfikacji ISO 27001 oznacza i daje Zamawiającemu gwarancję, że Wykonawca usługi spełnia trzy zasadnicze atrybuty ochrony informacji obejmujące poufność – czyli zapewnienie dostępu do informacji wyłącznie dla osób uprawnionych do ich dostępu; integralność – czyli zagwarantowanie dokładności i kompletności informacji, oraz metod ich przetwarzania; oraz dostępność – czyli zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami. Spełnienie przez Wykonawcę warunku posiadania certyfikatu normy ISO 27001 daje Zamawiającemu rękojmię, iż kontrahent ten wdrożył w swojej działalności przewidziany normą system zabezpieczeń danych do których uzyskuje dostęp w tym określone procedury, procesy, funkcje oprogramowania i sprzętu, a także posiada adekwatną do realizowanej usługi wiedzę i praktykę z tego zakresu.

2. Pytanie: Proszę o wyjaśnienie braku punktu kontaktowego do pytań ze strony oferentów – brak osoby wyznaczonej do prowadzenia sprawy/kontaktu

Odpowiedź: Zapytanie ofertowe zostało zamieszczone na oficjalnej stronie Biuletynu Informacji Publicznej Urzędu Miejskiego w Orzyszu na której widnieją dane kontaktowe Zamawiającego obejmujące telefon, adres skrzynki mailowej oraz adres skrzynki epuap. Obowiązujace u Zamawiającego zasady udzielania zamówień publicznych poniżej progów wynikających z ustawy Prawo zamówień publicznych nie obejmują obowiązku zamieszczania w zapytaniu ofertowym danych kontaktowych osób wyznaczonych do prowadzenia sprawy.

Wszelkie zapytania dotyczące postępowania można kierować na adres um@orzysz.pl

3. Pytanie: Proszę o wyjaśnienie dlaczego organ nie dokonuje obowiązku informacyjnego wynikającego z 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 (Dz.U.UE.L.2016.119.1)

Odpowiedź: Brak załączonej klauzuli informacyjnej wynika z niedopatrzenia przez osobę publikującą zapytanie na stronie BIP. Niezwłocznie po otrzymaniu Pańskiej uwagi, w dniu 25.11.2020 r. informacja ta została zamieszczona przy zapytaniu ofertowym pod adresem : http://www.bip.orzysz.pl/index.php?wiad=10730

4. Pytanie: Dlaczego Urząd ujął jako wymaganie wobec Inspektora Ochrony Danych ubezpieczenia na kwote 4 mln złotych. Taki wymóg jest niewspółmierny do wartości zamówienia i dotyczy tylko Urzędu. Posiadam ubezpieczenie do kwoty 100000 zl i jest to współmierne gdyż na sektor publiczny można nałożyć max kwote 100 000 zl. Kwota ubezpieczenia na taka kwotę wynosi ok 3 tys zl rocznie i oferta jaka można złożyć będzie bardzo wysoka i Urzad będzie musiał ponieść dużo wysze koszty niż planuje. Dlatego proszę o poinformowanie czy kwota ubezpieczenia na kwote 100 000 zł będzie dopuszczalna i z zachowaniem uczciwej konkurencji.

Odpowiedź: ustalonym przez Zamawiającego warunkiem udziału w postępowaniu podmiotu który nie tylko będzie pełnił funkcje Inspektora Ochrony Danych Osobowych ale także będzie wykonywał audyt bezpieczeństwa informacji zgodnie z Rozporządzeniem ws prawie Krajowych Ram Interoperacyjności… jest wymóg posiadania polisy ubezpieczeniowej . Kwota minimum 4 mln zlotych jest podyktowana ochroną Zamawiającego głównie przed roszczeniami osób fizycznych związanych z potencjalnym naruszeniem ich danych osobowych. Mając na uwadze, że potencjalnie mogą zostać naruszone dane osobowe osób

fizycznych będące w posiadaniu Gminy Orzysz i osoby te mogą wystąpić z roszczeniem odszkodowawczym (lub też zadośćuczynieniem) wobec gminy, tak określona kwota polisy ubezpieczeniowej daje, w ocenie Zamawiającego, gwarancję ewentualnego zabezpieczenia tych roszczeń.Odpowiedzialność Urzędu o której Państwo piszą tj. kwoty 100.000 zł dotyczy jedynie kar jakie mogą zostać nałożone na Urząd z tytułu naruszenia przepisów o ochronie danych, niestety nie dotyczą one w żaden sposób limitów odpowiedzialności finansowej wobec osób fizycznych z roszczeń indywidualnych ustalanych przez sąd na skutek powództwa cywilnego. Posiadanie takiej polisy jest ustalonym warunkiem udziału w postępowaniu, niespełnienie tego warunku spowoduje odrzucenie oferty.

Zamawiający informuje, że pytania oraz odpowiedzi na nie stają się integralną częścią zapytania i będą wiążące przy składaniu ofert.

W związku z faktem, że udzielone odpowiedzi nie powodują modyfikacji treści zapytania, Zamawiający nie dokonuje zmiany terminu składania i otwarcia ofert w przedmiotowym postępowaniu.

BURMISTRZ

(-) mgr Zbigniew Włodkowski