

Wrocław, 21 lutego 2020

Do Zainteresowanych

Dotyczy: postępowania prowadzonego w trybie przetargu nieograniczonego o udzielenie zamówienia publicznego, którego przedmiotem jest: ZAWARCIE UMOWY RAMOWEJ NAUSŁUGI DOSTĘPU DO ZEWNĘTRZNEJ PLATFORMY ZAKUPOWEJ, znak postępowania: CUI-ZZ.3201.1.2020

W związku z otrzymaniem pytań do treści Specyfikacji Istotnych Warunków Zamówienia, działając w trybie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019r. poz. 1843, z późn. zm.), dalej „ustawa Pzp” wyjaśniam co następuje:

Pytanie 1

Aby wycenić Państwa usługę w zakresie zakupów regulaminowych z art. 4 ust. 8 potrzebujemy skany sprawozdań do Prezesa UZP (za 2018 lub 2019 w zależności, który jest dostępny).

Poza tym w Państwa pytaniu zabrakło informacji dot. bezpieczeństwa systemu, dlatego poniżej wysyłamy istotne wg nas informacje. Chcę budować bezpieczny system do obsługi zamówień wdrożyliśmy ISO 27001, które determinuje nas do tego, aby umowy miały jednolity charakter, tak aby procedura postępowania była identyczna dla każdego Klienta, gdyż tylko w ten sposób można świadczyć usługi na wysokim poziomie.

Nasze mocne strony to:

- największa ilość obsługiwanych Klientów w Zamówieniach Publicznych w Polsce (919 Klientów , 16.865 Zamawiających procedujących postępowania i 134.050 wykonawców),
- Zero odwołań do KIO wykonawców z tytułu źle działającego systemu,
- Ponad 95% więcej ofert w przetargach napl niż średnia w kraju (4,28 oferty na przetarg napl wobec 2,19 oferty na przetarg w Polsce w 2018, czytaj więcej).

Bezpieczeństwopl

Posiadamy Certyfikatu ISO 27001 , co daje pewność należytego wykonania usługi przez Zamawiającego przy wyborze systemu. Jeżeli bezpieczeństwo przechowywanych danych jest dla Państwa ważne i chcecie dochować należytej staranności przy wyborze systemu (to Zamawiający odpowiada za błędy systemu) to ISO 27001 daje Państwu pewność i zlecenie jednostce certyfikującej sprawdzanie zgodności deklaracji z działaniami. W innym wypadku to Państwo powinniście audytować operatora, czy jego procedury są bezpieczne. W innym wypadku można zarzucić Państwu wybór rozwiązania przy niezachowaniu należytej staranności, ponieważ to Zamawiający odpowiada za rozwiązanie jakie wybrał. W naszym przypadku instytucją certyfikującą, która posiada akredytację do tego typu audytów jest Wojskowa Akademia Techniczna.

Proszę zadać sobie pytanie w jaki sposób chcecie sprawdzać operatora platformy, czy spełnia restrykcyjne wymagania w zakresie bezpieczeństwa? Na pewno przyjdzie Państwu audytować osobiście operatora, jeżeli nie będzie miał wdrożonego systemu, który jest audytowany przez akredytowane jednostki zewnętrzne. Co zrobicie Państwo jeżeli po audycie operator nie będzie się zgadzał z Państwa zastrzeżeniami? Rozwiążecie Państwo umowę? Jak chcecie dochować należytej staranności nie uwzględniając w procesie kwestii bezpieczeństwa? Wg nas w niedalekiej przyszłości operatorzy platform zostaną włączeni w infrastrukturę krytyczną Państwa. Wymagania w zakresie podmiotów wpisanych na tę listę są bardzo zbieżne z ISO 27001. Co jeżeli wybierze operatora, a okaże się, że nie przejdzie on obowiązkowej certyfikacji, gdyż nie spełnia założeń bezpieczeństwa?

ISO 27001 nie jest łatwo wdrożyć, gdyż przystosowanie się do nowych procedur zajmuje nawet 2 lata. Główne serwery platform zakupowa.pl są zlokalizowane w Polsce oraz spełniają restrykcyjne wymogi bezpieczeństwa TIER III of Constructed Facility, przyznana po serii rygorystycznych testów infrastruktury obiektu, przeprowadzonych przez niezależną amerykańską agencję Uptime Institute.

Naszą siłą jest wybór najlepszych dostawców jak choćby serwerownia spełniająca TIER III of Constructed Facility. Zdajemy sobie sprawę, że niekiedy operatorzy platform nie chcą płacić za dużo wyższy poziom bezpieczeństwa, jednak jest to w Państwa interesie, aby taki komfort bezpieczeństwa posiadać, dlatego główna nasza serwerownia jest zlokalizowana w Polsce, a Spółka zarządzająca serwerownią należy do Toruńskiej Agencji Rozwoju Regionalnego.

Posiadamy najwyższy certyfikat szyfrowania danych TSL 1.3. TLS to Secure Socket Layer zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta. Opiera się na szyfrowaniu asymetrycznym oraz certyfikatach. Jako jedni z nielicznych systemów przeglądarkowych w Polsce przeszliśmy na certyfikat TLS 1.3 z najwyższymi standardami bezpieczeństwa.

Liczymy na odpowiedź w zakresie pisma. Ważne jest dla nas, czy dopuszczają Państwo złożenie oferty na naszych warunkach wraz ze wzorcem umowy. W innym wypadku rozważymy złożenie oferty, jednak będziemy musieli oszacować ryzyka i szacujemy że wycenia wzrośnie min 50%.

Odpowiedź:

Zamawiający informuje, że w specyfikacji istotnych warunków zamówienia zawarto szereg wymogów związanych z zapewnieniem bezpieczeństwa informacji m.in.

- w załączniku nr 1 do projektu umowy - OPZ punkt 1.1. a) - wymóg zapewnienia zgodności z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r., poz. 2247 z późn. zm.) w obszarze zarządzania bezpieczeństwem informacji;
- w załączniku nr 1 do projektu umowy - OPZ punkt 4 - wymagania techniczne dla platformy, w tym m.in. kwestie przywołane w zadanym pytaniu dotyczące lokalizacji serwerów, nakazu stosowania protokołu TLS 1.3. oraz szereg innych wymogów wymienionych w punkcie 4.8
- w załączniku nr 2 do projektu umowy – umowa PPDO – określono szczegółowe regulacje dotyczące zasad przetwarzania w systemie danych osobowych zgodnie z obowiązujących w tym obszarze przepisami prawa
- w załączniku nr 6 do projektu umowy – wymagania dotyczące dokumentacji systemu informatycznego, którą wykonawca przekaze zamawiającemu, w szczególności dotyczące przetwarzania danych osobowych w systemie.

Ponadto względy bezpieczeństwa informacji są brane pod uwagę również w ocenie ofert. Zamawiający w treści SIWZ określił minimalny próg bezpieczeństwa danych osobowych, którego niespełnienie przez system lub wykonawcę skutkuje nieważnością oferty.

Przywołane fakty dowodzą, że kwestia zachowania bezpieczeństwa informacji została uwzględniona w niniejszym zamówieniu, tym samym Zamawiający zachował w tym obszarze należytą staranność.

W chwili obecnej nie ma regulacji, które nakazują Zamawiającemu aby wymagał certyfikatu ISO 27001 od dostawcy zamawianego rozwiązania. Taki wymóg mógłby ograniczyć konkurencję co pozostaje w sprzeczności z ustawą Pzp.

Jeżeli pomimo określenia licznych wymogów związanych z bezpieczeństwem informacji dojdzie do naruszenia, zgłoszenia zastrzeżeń w audycie bezpieczeństwa lub zostanie dla wykonawcy narzucony

obowiązek certyfikacji wówczas zamawiający podejmie działania zgodne z zapisami zawartej przez strony umowy oraz aktualnie obowiązującym przepisami prawa – adekwatne do zaistniałej sytuacji.

Zamawiający nie dopuszcza do złożenia oferty na Państwa warunkach i z Państwa wzorcem umowy. Oferta musi zostać złożona zgodnie z wymaganiami zawartymi w Specyfikacji Istotnych Warunków Zamówienia i jej załącznikach (w tym projektem umowy).

Zamawiający informuje, że w Jednostce Zamawiającego zgodnie z przekazanym do Prezesa UZP sprawozdaniem za 2018r. łączną wartość udzielonych zamówień bez podatku od towarów i usług w zamówieniach, których wartość nie przekracza wyrażonej w złotych równowartości kwoty, o której mowa w art. 4 pkt. 8 ustawy wynosiła 2 406 174,55 złotych.

Tymoteusz Przybylski

Dyrektor CUI

Dokument podpisano podpisem elektronicznym w dniu: 21-02-2020

Sprawę prowadzi:
Marta Kozyra
Sporządziła:
Magdalena Anuszkiewicz
Do wiadomości:
aa