Szczecin, dnia 13.04.2018 r.

**ODPOWIEDZI NA ZAPYTANIE OFERTOWE DOTYCZĄCE**

 ***Audytu zgodności i dostosowanie Pomorskiego Uniwersytetu Medycznego w Szczecinie do wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.***

1. Czy i jakie działania związane z przetwarzaniem danych osobowych są  outsourcowane (realizowane przez firmy zewnętrzne)? Np. wydruk faktur, mailing marketingowy, kadry / płace.

*Doradztwo prawne, usługi poligraficzno-wydawnicze,częściowe zabezpieczenie obiektów, wspieranie usług IT, badania laboratoryjna w ramach badań naukowych.*

1. Ile  mniej  więcej  osób  jest  zaangażowanych  w przetwarzanie danych osobowych w PUM.

*Ilość osób iorących udział w procesie przetwarzania danych - ok. 2000 osób*

1. Ile jest zarejestrowanych upoważnień do przetwarzania danych osobowych?

*Ok. 2000*

1. W ilu systemach są przetwarzane dane osobowe?

*Zidentyfikowanych ok. 26*

1. Czy wszystkie jednostki w których ma zostać przeprowadzony audyt zlokalizowane są na terenie miasta Szczecina (z wyjątkiem ośrodka wczasowego znajdującego się w Barlinku)?

*Zamawiający posiada także jednostki znajdujące się na terenie miasta Police*

1. Ile jest tzw. obszarów przetwarzania danych osobowych?

*Zamawiający posiada 23 lokalizacje, jednakże procesy przetwarzania odbywają się we wszystki jednostkach organizacyjnych, których jest duzo więcej.*

1. Czy istnieje możliwość zapoznania się ze wzorem umowy, która miałaby zostać zawarta?

*W chwilii obecnej Zamawiający nie opracował jeszcze wzoru umowy*

1. Czy PUM posiada dokumentację ochrony danych osobowych zgodną z  UODO (politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym)?

*Tak, Zamawiający posiada opracowana Politykę danych osobowych i Instrukcję zarządzania systemem informatycznym.*

1. Na ile godzin miałoby być przewidziane szkolenie?

*Co najmniej 4 godziny*

1. W ilu fizycznych lokalizacjach umieszczono zasoby informatyczne?

*7 lokalizacji*

1. Czy w PUM są zawarte umowy powierzenia danych osobowych?

*Tak*

1. Jakie dane przetwarza PUM? Pracownicze, handlowe?

*dane pracowników, studentów, doktorantów, słuchaczy, kontrahentów, byłych pracowników, absolwentów, kandydatów do pracy, uczestników badań naukowych, dane klientów*

1. Czy PUM przetwarza dane osobowe wrażliwe?

*Tak*

1. Czy PUM ma wdrożoną politykę bezpieczeństwa i System Zarządzania Bezpieczeństwem Informatycznym?

*Zamawiający nie posiada SZBI ani dokumentacji wynikającej z PN-ISO/IEC 27001, poza jedną jednostką organizacyjną która posiada Certyfikat Systemu Zarzadzania Bezpieczeństwem Informacji.*

1. Czy istnieje udokumentowany system nadawania upoważnień do przetwarzania danych osobowych?

Tak

1. Jaki jest sposób udostępniania aplikacji? (np. poprzez przeglądarkę internetową użytkownika, inne). Czy system udostępniania informacji został sformalizowany?

*przeglądarka internetowa, twardy klient, zasób sieciowy. System nadawnia upranień do systemów został sformalizowany.*

1. Jaki jest sposób uwierzytelniania użytkowników aplikacji?

*Login i hasło*

1. Czy zakres prac audytowych ma również obejmować zgodność z krajowymi przepisami prawa?

*Jeżeli mówimy o obowiązujących przepisach to nie. Usługa ma obejmowac zgodność z RODO, wytycznymi Grupy Art. 29.*

1. Na czym ma polegać doradztwo powdrożeniowe w zakresie zmian w przepisach i wytycznych z zakresu ochrony danych osobowych, w terminie do 31 grudnia 2018r.? Czy doradztwo to ma obejmować bieżące aktualizacje we wdrożonej dokumentacji?

*Jeżeli zmiany w przepisach i wytycznych będą wymagały zmian w prowadzonej dokumentacji, to wykonawca swoją wiedzą i doświadczeniem jest zobowiązanych udzielić pomocy i zaproponować jak najlepsze i zgodne z przepisami rozwiązanie*.

1. Czy Zamawiający w ramach usługi będzie wymagał przeprowadzenia testów penetracyjnych?

*Nie*

1. Odnośnie informacji „W ramach wdrożenia, Wykonawca po uzgodnieniu z Zamawiającym dokona sprawdzenia w wytypowanych jednostkach organizacyjnych PUM, sposóbu skuteczności zaimplementowanych rozwiązań z zakresu ochrony danych osobowych, a w razie potrzeby, wprowadzi stosowne modyfikacje tych rozwiązań” proszę o sprecyzowanie na czym polegałaby rola Wykonawcy w modyfikacji tych rozwiązań? Rozumiem, że usługa miała by polegać na przedstawieniu rekomendacji, później zweryfikowania czy zostały faktycznie wprowadzone w organizacji. Sformułowanie takie może oznaczać, że to na Wykonawcy będzie ciążyło wprowadzenie stosownych modyfikacji podczas gdy wdrożenie tych rekomendacji powinno spoczywać na Zamawiającym.

*Zapis ten dotyczy sprawdzenia zaimplementowanych rozwiązań, a jeżli ich wykonanie nie jest jednak skuteczne i możliwe do realizacji przez Zamawiąjącego, należy wprowadzić ich modyfikację*

1. Czy Zamawiający szacunkowo przewiduje czas zakończenia audytu? Czy w przypadku nie zakończenia wdrożenia audytu w terminie do dnia 31 grudnia 2018 r. wykonawca będzie zobowiązany do świadczenia usługi doradztwa powdrożeniowego w późniejszym czasie?

*Zamawiający wskazałał minimalne terminy na przeprowadzenie audytu i wdrożenia. Jednakże Zamawiający zastrzega że wykonanie usługi musi zostac zakończone do dnia 15 października 2018r.*

1. Jakie  są  możliwe  daty  oraz  godziny  przeprowadzenia  prac  w  siedzibie  Zamawiającego, a także zdalna dostępność?

*W chwilli obecnej Zamawiający nie jest w stanie określić dat i godzin przeprowadzenia prac. Zamawiający nie przewiduje wykonania usługi w sposób zdalny.*

1. Wielkość firmy w liczbach:
2. zatrudnienie - *pracownicy na umowy o prace i umowe zlecenie - ok. 1650, doktoranci ok 350,*
3. Oddziały – *Zamawiający nie posiada oddziałów*
4. ilość struktur wewnętrznych (biura, działy, departamenty) - *informacja zawarta w zapytaniu ofertowym. tj. struktura według Regulaminu organizacyjnego i Wykaz jednostek naukowo-dydaktycznych.*
5. ilość spółek zależnych - *spółki nie sa objete usługą*
6. konieczność przekazywania danych osobowych za granicę oraz poza EOG (ile i jakie kraje) – *przekazywanie danych w ramach EOG tj. w ramach projektów Erasmus, współpracy pomiędzy Uczelniami, przekazywanie danych w ramach projektów naukowych.*
7. obecna ilość zidentyfikowanych zbiorów danych osobowych – *70*
8. profil działalności - *działalność dydaktyczno-wychowawcza, działalność naukowo-badawcza, działalność usługowa, administracja*
9. Ogólna charakterystyka działu IT – stan osobowy, zakres obowiązków, ilość systemów - w tym o charakterze krytycznym, stosowane technologie, etc.

*Dział IT - ilość osób na chwile obecną - 9. Dodatkowo są 2 osoby zajmujące się konfiguracją stanowisk  na jednostkach organizacyjnych poza Rektoratem PUM. W 3 jednostkach istnieją odrębni Administratorzy dla tych jednostek. Ilość zidentyfikowanych systemów - 26, w tym 5 najważniejszych krytycznych. Zamawiający używa rożnych technologi w zakresie baz danych, stron www, systemów operacyjnych itd.*

1. 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).

*Zamawiający korzysta z właśnej infrastruktury. Co do informacji w zakresie formy komunikacji z innymi systemami i, używanych technologi, Zamawiający nie udostępni tych informacji na tym etapie postępowania.*

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

*7 lokalizacji, nie istnieje centrum zapasowe.*

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

*Zamawiający nie udostępni tych informacji na tym etapie postępowania.*

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

*Tak*

1. 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?

*Doradztwo prawne, usługi poligraficzno-wydawnicze,częściowe zabezpieczenie obiektów, wspieranie usług IT, badania laboratoryjna w ramach badań naukowych. Zamawiający podpisał umowy powierzenia lub jest w trakcie ustalania warunków w zakresie zdiagnozowanych usług.*

1. Jakie dane firma przetwarza

*Dane pracowników, studentów, doktorantów, słuchaczy, kontrahentów, byłych pracowników, absolwentów, kandydatów do pracy, uczestników badań naukowych, w ramach usługówki dane klientów, dane w ramach umów cywilnoprawnych.*

1. Ile osób należy przeszkolić?- *Zamawiający wskazał ilość w zapytaniu ofertowym*
2. W ilu lokalizacjach należy przeprowadzić badanie? Czy wszystkie lokalizacje znajdują się na terytorium Polski, jeżeli nie - to gdzie?

*Zamawiający wskazał w zapytaniu ofertowym miejsca i sposób przeprowadzenia usługi tj. wszystkie jednostki organizacyjne, domy studenckie i ośrodek wypoczynkowy w formie wskazanej na kazym etapie usług tj. wizji lokalnych, wywiadów, ankiet i opracowywaniu otrzymanej dokumentacji. Zamawiający nie dopuszcza wykonania Usługi metodą reprezentatywną, za wyjątkiem sprawdzenia w wytypowanych jednostkach organizacyjnych PUM, sposóbu skuteczności zaimplementowanych rozwiązań z zakresu ochrony danych osobowych*.

1. Czy organizacja ma wdrożony System Zarządzania Bezpieczeństwem Informacyjnym
 W szczególności, czy wdrożono podstawowe składniki dokumentacji przetwarzania danych osobowych (Polityka bezpieczeństwa, wymagane instrukcje)?

*Zamawiający nie posiada wdrożonego SZBI, poza jedna jednostką organizacyjną, która posiada Certyfikat Systemu Zarzadzania Bezpieczeństwem Informacji. Zamawiający posiada dokumentację przetwarzania tj. Politykę danych osobowych i Instrukcję zrządzania systemem*.

1. Prosimy o informację ilu podmiotom zewnętrznym są udostępniane dane osobowe?

*Według posiadanej wiedzy ok. 20*

1. 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.

*Zakres prac ma obejmować wszystkie procesy przetwarzania danych osobowych w sposób kompleksowy. Dotyczy to przeglądu własnych rozwiązań i opracowania nowych procedur.*

1. Prosimy o informację czy raport będzie przygotowywany tylko w języku polskim.

*Tak*

 .................................................

*Zatwierdzam*