Wrocław, dnia 24.05.2018 r.

Dane zamawiającego:

UNITY SYSTEMS SP. Z O.O.
Ul. Przedmiejska 6-10
54-201 Wrocław
NIP: 894-28-56-366

UnitySystems spółka z o.o.
ul. Przedmiejska 6-10, 54-201 WROCŁAW
tel. +48 71 35 84 100, fax: +48 71 35 84 101
www.unity.pl
REGON: 020234490

Dotyczy : wyboru wykonawcy na realizację zadań w projekcie RPDS.01.03.02-02-0009/17

Szanowni Państwo,

W związku z planowaną realizacją projektu w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020, Oś priorytetowa 1, Przedsiębiorstwa i innowacje, Działanie 1.3 „Rozwój przedsiębiorczości", Poddziałanie 1.3.2 Rozwój przedsiębiorczości ZIT WrOF,

w ramach **procedury rozeznania rynku,** prosimy o złożenie nam oferty na wykonanie usługi doradczej pn.:

Doradztwo w zakresie przygotowania do wdrożenia systemu zarzadzania bezpieczeństwem informacji zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2017-06 oraz zgodnie z wymaganiami rozporządzenia PE i Rady (UE) 2016/679 (RODO).

I. Podstawowe parametry techniczne i opis przedmiotu zamówienia:

Usługa doradcza ma polegać na:

Przedmiotem grantu jest wykonanie usługi doradczej w zakresie spełnienia wymagań przepisów prawa i opracowania dokumentacji systemu zarzadzania bezpieczeństwem informacji zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2017-06 oraz zgodnie z wymaganiami 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).

Zakres usługi doradczej:

Etap 1: *wykonanie audytu w zakresie bezpieczeństwa informacji w celu oceny stopnia spełnienia przez Spółkę wymogów*

- *normy **EN ISO/IEC 27001:2017***
- *Generalnego Rozporządzenia o Ochronie Danych Osobowych **(RODO)** (sprawdzenie jakie dane i na jakiej podstawie prawnej są przetwarzane oraz stosowanych zabezpieczeń)*

Etap 2: *Zapoznanie się z funkcjonującymi w Spółce dokumentami i sposobami postępowania w zakresie bezpieczeństwa informacji i opracowanie metodologii szacowania ryzyka utraty poufności, dostępności i integralności informacji zgodnie z normą ISO 27001:2017*

Etap 3: *Pomoc w przeprowadzeniu procesu szacowania ryzyka utraty poufności, dostępności i integralności informacji wg opracowanej metodologii, i określeniu „akceptowalnego poziomu ryzyka"*

Etap 4: *Zapoznanie się z funkcjonującymi w Spółce dokumentami i sposobami postępowania w zakresie bezpieczeństwa informacji i opracowanie procedur/y dotyczącej „ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy **przetwarzaniu mobilnym i pracy na odległość**" oraz procedur/y dotyczącej „ustalenia zasad postępowania z*

informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych"

Etap 5: *Zapoznanie się z funkcjonującymi w Spółce dokumentami i sposobami postępowania w zakresie bezpieczeństwa informacji i opracowanie* ***niezbędnej dokumentacji*** *normy* ***EN ISO/IEC 27001:2017*** *a w szczególności „DEKLARACJI STOSOWANIA" zgodnie z załącznikiem A do normy* ***EN ISO/IEC 27001:2017*** *szczegółowo w każdym punkcie (klauzuli) odnoszącej się do funkcjonujących w Spółce dokumentów oraz do przyjętych w Spółce metod postępowania i nowo opracowanych dokumentach/zarządzeniach. Zakres prac obejmuje m.in.:*

1. *umowy powierzenia dostosowane do wymogów rozporządzenia*
2. *klauzule zgód dostosowane do wymogów rozporządzenia*
3. *klauzule informacyjne dostosowane do wymogów rozporządzenia*
4. *umowy powierzenia dostosowane do wymogów rozporządzenia*
5. *Polityka/i bezpieczeństwa - identyfikacja i opis: natury, zakresu, kontekstu i celów przetwarzania (wspomagająca* „zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania" *oraz stosowanie ochrony prywatności jako ustawienia domyślnego (**privacy by default**))*
6. Deklaracja stosowania zabezpieczeń w odniesieniu do wymagań aktualnego załącznika do normy ISO/IEC 27001 *(wspomagająca „zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania")*
7. *Jeżeli to konieczne opracowanie procedur/y określających/cej* „pseudonimizację i szyfrowanie danych osobowych", postępowanie ze sprzętem przenośnym, postępowanie z danymi, postępowanie z pocztą elektroniczną, hasłami etc.
8. *Jeżeli to konieczne Procedury oceny ryzyka (skutków) przewidywanych operacji przetwarzania danych osobowych (**privacy impact assessment**)* (wynikającego(ych) z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) – **zobacz etap 2**
9. *Jeżeli to konieczne Raportu/ów z analizy ryzyka (PIA/DPIA) lub udokumentowana/e analiza/y, że dany rodzaj przetwarzania nie stwarza ryzyka dla praw i wolności i PIA/DPIA nie jest wymagana.* – **zobacz etap 3**
10. *Rejestr czynności przetwarzania danych osobowych (zgodnie z art. 30 RODO)*
11. *Procedura/y dotycząca zapewniania ochrony prywatności w fazie projektowania (**privacy by design**)*
12. *Procedura dotycząca szkoleń i uświadamiania*
13. *Procedura/y dotycząca/e monitorowania bezpieczeństwa (wspomagająca* „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania") *- Opracowanie metodologii pomiaru skuteczności SZBI oraz wdrożonych zabezpieczeń (zgodnie z ISO/IEC 27004)*
14. *Procedura/y nadawania i odbierania uprawnień oraz zarządzania dostępem (służąca* „zapewnieniu, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego")
15. *Opracowanie wzorcowych planów ciągłości działania (wspomagających* „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego")
16. Procedura/y monitorowania i postępowania w przypadku naruszenia ochrony danych wraz z Rejestrem naruszeń ochrony danych *(w tym regulujących „Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych oraz Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu") (zgodnie z ISO/IEC 27035 i **RODO**)*

Etap 7: *Pomoc w podnoszeniu świadomości*

Etap 8: *Pomoc we wdrożeniu zasad RODO w organizacji w szczególności w wypełnieniu wymagań wynikających z opracowanej dokumentacji*

Etap 9: *Ocena stopnia przygotowania organizacji na realizację* ***wniosków*** *ze strony osób, których dane są przetwarzane, dotyczących np. przeniesienia danych czy prawa do bycia zapomnianym itd. (np. opracowanie procedury)*