

Poznań, 13.01.2021 r.

**ODPOWIEDZI NA PYTANIA WYKONAWCÓW II
MODYFIKACJA TREŚCI WARUNKÓW ZAMÓWIENIA**

Sygnatura postępowania: 1100/AW00/ZD/KZ/2020/0000089728

Sygnatura pisma: DL/LZ/GM/2021/23

Dotyczy: Zawarcie umów ramowych na wykonanie testów bezpieczeństwa teleinformatycznego lub OT

Zamawiający na podstawie 1.12 Warunków Zamówienia (WZ) modyfikuje zapisy dokumentacji postępowania przedłużając termin składania ofert:

TREŚĆ MODYFIKACJI	
1.	<p>Zamawiający modyfikuje następujące zapisy Warunków Zamówienia:</p> <p><u>Rozdział I, pkt 11.1</u></p> <p>PO MODYFIKACJI Z 31.12.2020R. BYŁO</p> <p>„11.1. Ofertę należy złożyć w formie elektronicznej na adresy e-mail: adrianna.targalska@enea.pl oraz mikolaj.gorecki@enea.pl, w terminie do dnia 15 stycznia 2021 r. do godz. 10.00.</p> <p>WAŻNE! Hasło dostępu do pliku ze złożoną ofertą, Wykonawca przesyła Zamawiającemu na adresy email adrianna.targalska@enea.pl oraz mikolaj.gorecki@enea.pl, po upływie terminu składania ofert, jednak nie później niż w ciągu 2 godzin od upływu tego terminu, tj. 15 stycznia 2021 r. między godziną 10:00, a godziną 12:00.”</p> <p>JEST:</p> <p>„11.1. Ofertę należy złożyć w formie elektronicznej na adresy e-mail: adrianna.targalska@enea.pl oraz mikolaj.gorecki@enea.pl, w terminie do dnia 22 stycznia 2021 r. do godz. 10.00.</p> <p>WAŻNE! Hasło dostępu do pliku ze złożoną ofertą, Wykonawca przesyła Zamawiającemu na adresy email adrianna.targalska@enea.pl oraz mikolaj.gorecki@enea.pl, po upływie terminu składania ofert, jednak nie później niż w ciągu 2 godzin od upływu tego terminu, tj. 22 stycznia 2021 r. między godziną 10:00, a godziną 12:00.”</p>

Działając na podstawie pkt 1.9. – 1.11. Warunków Zamówienia (WZ) Zamawiający udziela wyjaśnień dokumentacji przedmiotowego postępowania:

LP	Treść pytania i odpowiedzi
1.	<p>PYT: (DOT. CZĘŚCI 1) § 2 ust 2 lit i) DPA – czy postanowienie dopuszcza przetwarzania danych osobowych w sposób zdalny spoza siedziby Procesora? Proponujemy doprecyzowanie wskazujące wprost na taką możliwość.</p> <p>ODP: Tak, dopuszczamy, ale tylko dla niektórych systemów i pod warunkiem, że stacje robocze osób wykonujących testy penetracyjne będą właściwie zabezpieczone, tzn. minimum VPN, zaszyfrowany dysk, a zgromadzone informacje podczas pentestów jeszcze dodatkowo zabezpieczone (np. spakowane i zabezpieczone hasłem), stacja robocza pentestera innym segmencie sieci wewnętrznej Wykonawcy niż nieuprawnionych do pentestów pracowników.</p>

2.	<p>PYT: (DOT. CZĘŚCI 1) § 2 ust 2 lit m) DPA – czy postanowienie to oznacza, że rejestr nie może być oprowadzony w formie elektronicznej?</p> <p>ODP: Jak wskazuje dr Marlena Sakowska-Baryła <i>bez wątplenia forma pisemna może zatem przybrać postać wskazaną w art. 78 § 1 KC lub odpowiednio w art. 78¹ § 1 KC (dla formy elektronicznej), gdyż podpis stanowiący część sporządzanego dokumentu będzie informował o osobie realizującej obowiązek prowadzenia rejestru lub zatwierdzającej poczynione wpisy.</i> Reasumując rejestr może być prowadzony w formie elektronicznej ważne żeby możliwe było złożenie pod nim podpisu elektronicznego z kwalifikowanym certyfikatem bezpieczeństwa.</p>
3.	<p>PYT: (DOT. CZĘŚCI 1) § 3 ust 2 DPA – czy postanowienie to oznacza, że Administrator może polecić Procesorowi wdrożenie wszelkich nowych środków bezpieczeństwa – bez względu na zasadność, konieczność, koszty? Kto ponosi koszt wdrażania takich środków? Czy w przypadku braku możliwości wdrożenia takich środków Procesor może odmówić ich wdrożenia lub wypowiedzieć umowę bez ponoszenia konsekwencji w tym zakresie? Proponujemy wprowadzenie zmiany do umowy adresującej powyższe wątpliwości celem zniwelowania nierównowagi stron.</p> <p>ODP: Administrator może polecić wdrożenie środków , które będą niezbędne do zapewnienia właściwego poziomu bezpieczeństwa i adekwatne do celu przetwarzania zgodnie z zasadami wskazanymi w art. 5 RODO. Koszty wdrożenia środków ponosi Procesor.</p>
4.	<p>PYT: (DOT. CZĘŚCI 1) § 4 ust 2 DPA – termin 24 h godzin na zgłoszenie jest bardzo krótki – w jaki sposób i od jakiego momentu należy go liczyć w przypadku podejrzenia naruszenia lub próby naruszenia? Czy te należy zgłaszać sukcesywnie – próba – podejrzenie – naruszenie – każde w 24 h? Proponujemy zmianę – 36 h godzin od momentu stwierdzenia naruszenia dla naruszenia ochrony danych; w pozostałych przypadkach zgłoszenie powinno być niezwłoczne, chyba że nie stanowi zagrożenia dla ochrony danych.</p> <p>ODP: Jest to nasza standardowa regulacja i nie ulega zmianie.</p>
5.	<p>PYT: (DOT. CZĘŚCI 1) § 4 ust 5 DPA – o jakie wytyczne i polecenia chodzi? Czy Procesor będzie je zobowiązany zrealizować w każdym przypadku bez względu na ich niezbędność, koszt? Proponujemy doprecyzowanie, iż Procesor realizuje ww. wytyczne i polecenia w zakresie w jakim jest niezbędne do zapewnienia odpowiedniej ochrony danych zgodnie z RODO. W pozostałym zakresie koszt realizacji wytycznych ponosić powinien Administrator.</p> <p>ODP : Chodzi o wszelki wytyczne i polecenia zgodne z RODO. Wykonawca zgłaszając się do udziału w postępowaniu powinien mieć świadomość że w celu zapewnienia właściwego poziomu bezpieczeństwa przetwarzanych danych konieczne może być poniesienie dodatkowych kosztów.</p>
6.	<p>PYT: (DOT. CZĘŚCI 1) § 5 ust 1 DPA – czy za sub-procesora Strony uznają także osoby stale świadczące usługi na rzecz Procesora w oparciu o umowy cywilnoprawne (osoby na zleceniu, osoby na B2B)? Proponujemy wyraźne wskazanie, że takie osoby nie są uznawane za sub-pocesorów a Procesor udostępnia im dane do przetwarzania na podstawie upoważnienia.</p> <p>ODP: To zależy, jeżeli osoba na zleceniu prowadzi działalność gospodarczą i w ramach tej działalności wykonuje usługi dla Procesora to jest z mocy prawa uznawana za sub-procesora. Natomiast, jeżeli Zleceniobiorca to osoba fizyczna, która nie prowadzi działalności gospodarczej, to można go zakwalifikować jako osobę zatrudnioną u Procesora, która ma dostęp do danych na podstawie upoważnienia.</p>
7.	<p>PYT: (DOT. CZĘŚCI 1) § 6 ust 5 DPA - o jakie wytyczne i polecenia chodzi? Czy Procesor będzie je zobowiązany zrealizować w każdym przypadku bez względu na ich niezbędność, koszt? Proponujemy doprecyzowanie, iż Procesor realizuje ww. wytyczne i polecenia w zakresie w jakim jest niezbędne do zapewnienia odpowiedniej ochrony danych zgodnie z RODO. W pozostałym zakresie koszt realizacji wytycznych ponosić powinien Administrator.</p> <p>ODP: Zamawiający informuje, że w tym paragrafie chodzi o realizację art. 28 ust 3 lit. h RODO udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych</p>

8.	<p>PYT: (DOT. CZĘŚCI 1) § 9 ust 2 DPA – czy wymienione w postanowieniu przyczyny uznaje się za ważne bez względu na ich wpływ na ochronę danych? Proponujemy zawężenie przyczyn do tych, które powodują naruszenie lub zagrożenie ochrony danych</p> <p>ODP: To nasze standardowe regulacje, które co do zasady nie podlegają zmianie. Zdarzenie może nie powodować naruszenia ale może doprowadzić do utraty zaufania po stronie ENEA.</p>
9.	<p>PYT: (DOT. CZĘŚCI 1) Prosimy o wyjaśnienie zapisu zawartego w Par. 12 Ochrona i powierzanie przetwarzania danych osobowych, ust. 1. Umowy ramowej w brzmieniu jak poniżej:</p> <p>1.W związku z realizacją przedmiotowej Umowy między stronami dochodzi do udostępnienia danych osobowych. Jeżeli w związku z realizacją niniejszej Umowy lub określonego Zlecenia zajdzie potrzeba powierzenia Wykonawcy przez Zamawiającego do przetwarzania danych osobowych, Koordynatorzy Umowy wskazani w § 15 Umowy ustalą niezbędny zakres danych osobowych podlegających powierzeniu oraz sporządzą pisemny protokół określający zakres danych osobowych i wskazujący administratorów tych danych.</p> <p>ODP: Strony nie przewidują aby w związku z ich współpracą miało dochodzić do powierzenia przetwarzania danych osobowych, jednak nie mogą tego wykluczyć. Wskazując na udostępnienie danych mamy na myśli dane przedstawicieli i personelu stron pracujących przy realizacji umowy. Udostępnienie danych od powierzenia przetwarzania różni się tym że nie wymaga zawierania umowy powierzenia przetwarzania, bo po dwóch stronach występują Administratorzy danych a nie Administrator i Procesor. Mając na względzie fakt, że umowa ma charakter umowy należy brać pod uwagę możliwość że na dalszym etapie współpracy może wystąpić zlecenie które będzie obejmowało swoim zakresem informacje kwalifikowane jako dane osobowe zgodnie z art. 4 RODO i wówczas konieczne będzie zawarcie umowy powierzenia przetwarzania zgodnie z art. 28 RODO</p>

Z poważaniem

Otrzymują:

- 1) strona internetowa
- 2) a/a