Kraków, dnia 11.04.2024

**Zapytanie ofertowe**

**Szanowni Państwo,**

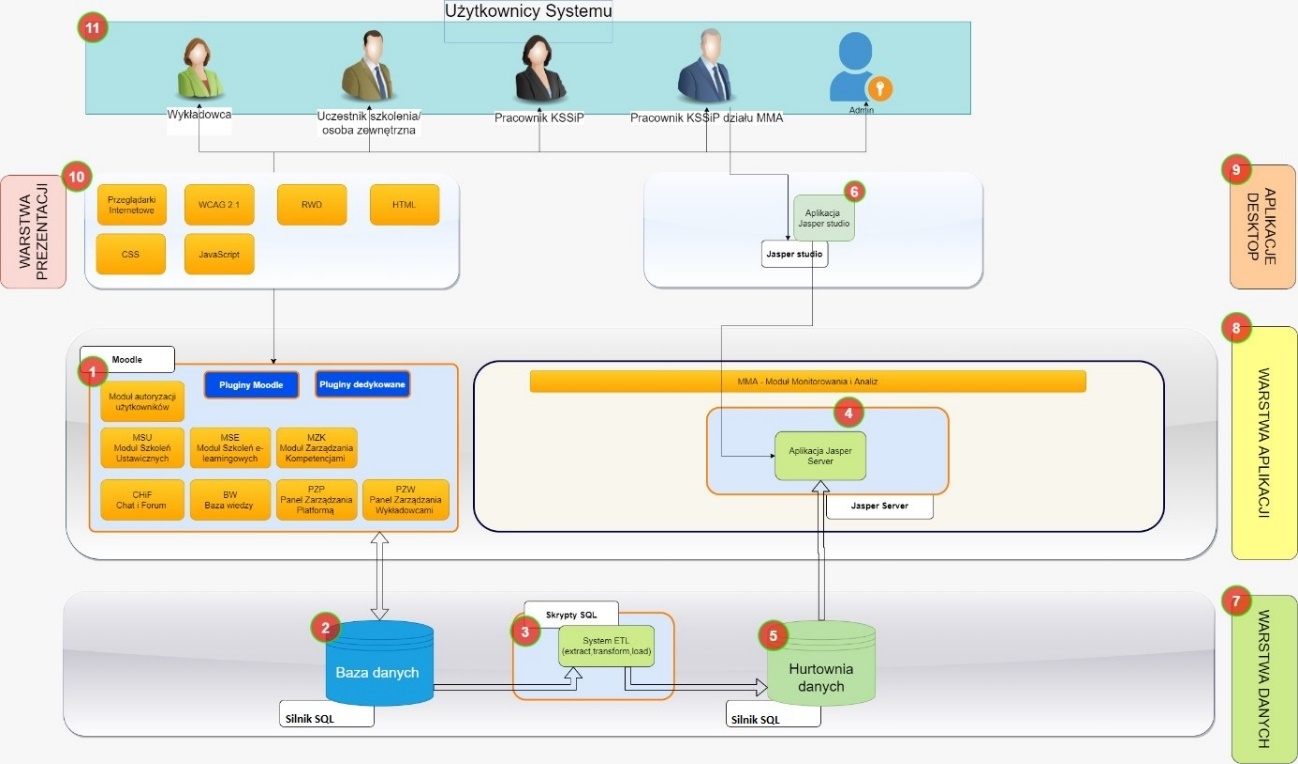
Krajowa Szkoła Sądownictwa i Prokuratury (dalej: KSSiP) zaprasza Państwa do złożenia oferty cenowej na usługę **przeprowadzenia** **audytu bezpieczeństwa systemu informatycznego, bezpieczeństwa informacji** **w narzędziu e-KSSiP wraz ze środowiskiem sieciowym hostingodawcy oraz sporządzenie raportu.**

Serwer pocztowy jest oparty na systemie pracy grupowej Zimbra.

Narzędzie e-KSSiP to nowoczesne narzędzie o budowie modułowej zawierającej: Moduł Szkoleń Ustawicznych (MSU), Moduł Szkoleń E-learningowych (MSE), Moduł Monitorowania i Analiz (MMA), Moduł Zarządzania Kompetencjami (MZK), Chat i Forum (CHiF), Baza wiedzy (BW), w tym także Panel Zarządzania Platformą (PZP), Panel Zarządzania Wykładowcami (PZW), z systemem wzajemnych powiązań pomiędzy modułami, umożliwiających korzystanie za pośrednictwem jednego konta z zaprojektowanych funkcji zgodnie z przydzielonymi uprawnieniami. W jego ramach będą przetwarzane dane osobowe użytkowników.

Narzędzie e-KSSiP zostało wdrożone na wybranej platformie hostingowej.

Audyt bezpieczeństwa systemu informatycznego ma na celu wykrycie potencjalnych zagrożeń i nieprawidłowości oraz ocenę bezpieczeństwa przetwarzania danych i zgodności z aktualnie obowiązującymi aktami prawnymi. Audyt powinien zawierać analizę podatności oraz zabezpieczeń systemu (rozumianego jako serwer pocztowy i narzędzie e-KSSiP) oraz środowiska sieciowego przed nieuprawnionym działaniem, nieuprawnionym dostępem kradzieżą, uszkodzeniami lub zakłóceniami oraz złośliwym oprogramowaniem. Audyt powinien być przeprowadzony najnowocześniejszymi narzędziami i zgodnie z metodologią, która gwarantuje rzetelność oceny bieżącego stanu bezpieczeństwa systemów informatycznych. Audyt bezpieczeństwa informacji polegać będzie na analizie ochrony danych, w szczególności osobowych pod kątem zapewnienia ich poufności, integralności i dostępności oraz na weryfikacji zgodności bezpieczeństwa z aktualnymi przepisami o ochronie danych osobowych. Obejmować będzie dane przechowywane fizycznie oraz informatycznie.



1. **Opis przedmiotu zamówienia**

**1.1 Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytu bezpieczeństwa systemu informatycznego, bezpieczeństwa informacji** **w narzędziu e-KSSiP wraz ze środowiskiem sieciowym hostingodawcy oraz sporządzenie raportu., o którym mowa w 1.3.**

1. Przedmiotowe usługi powinny zostać zrealizowane w szczególności zgodnie z następującymi dokumentami:

* Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r. ;
* Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
* Rozporządzenie 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 119 z 4.05.2016).
* Norma PN-ISO/IEC 27001 - „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania” lub równoważna;
* Norma PN-ISO/IEC 27002 - „Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczenia informacji” lub równoważna;
* PN-ISO/IEC 27005 - „Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji” lub równoważna;
* PN-ISO/IEC 24762 - Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie

1. W ramach zadań audytowych należy uwzględnić metodologię lub zasady określone w:

* PN-EN ISO 19011 – „Wytyczne dotyczące audytowania systemów zarządzania”
* ISO/IEC TR 13335 (PN-I-13335-1) - "Technika informacyjna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych”
* ISO 9001 - Systemy zarządzania jakością -- Wymagania
* ISO/IEC 29100 - Ramy prywatności
* PN-ISO 15408-1 – Kryteria oceny zabezpieczeń informatycznych
* PN-ISO/IEC 18045 – Metodyka oceny zabezpieczeń informatycznych
* PN-EN ISO 22301 Systemy zarzadzania ciągłością działania

Audyt środowiska sieciowego zostanie wykonany jako analiza wszelkich zabezpieczeń narzędzia e-KSSiP realizowanych po stronie hostingodawcy oraz jako analiza wdrożenia norm ISO rodziny 27000 (określonych w rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności) oraz ewentualnie innych, dodatkowych norm i certyfikatów stosowanych w zakresie świadczenia usługi hostingu w zakresie narzędzia e-KSSiP, w szczególności celem zapewnienia bezpieczeństwa i jego ciągłości działania.

Wykonawca przed przystąpieniem do realizacji Zamówienia jest zobowiązany do podpisania klauzuli informacyjnej oraz umowy powierzenia przetwarzania danych osobowych i jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni dotyczących Zamawiającego, a w szczególności danych osobowych, technicznych, ekonomicznych lub organizacyjnych.

Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie, drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań audytowych i jest bezterminowe.

**1.2 Obszary kontroli**

* Przetwarzanie i ochrona danych w systemach informatycznych.
* Bezpieczeństwo systemów informatycznych.
* Zasoby informatyczne.

**Szczegółowy zakres usług w zakresie audytu bezpieczeństwa systemu informatycznego oraz bezpieczeństwa informacji** **w narzędziu e-KSSiP wraz ze środowiskiem sieciowym:**

1. Przeprowadzenie testów penetracyjnych narzędzia e-KSSiP. W ramach wykonywania testów penetracyjnych wymagane jest wykorzystanie aktualnie obowiązujących standardów bezpieczeństwa udostępnionych przez organizację OWASP (Open Web Application Security Project) z uwzględnieniem OWASP Top 10 oraz OWASP ASVS (Application Security Verification Standard); podejście do testów penetracyjnych powinno być zgodne z wytycznymi przedstawionymi w dokumencie OWASP Testing Guide v4.2
2. Analiza podatności oraz zabezpieczeń przed niepowołanym dostępem osób trzecich, jakiejkolwiek nieuprawnionej ingerencji w działanie oraz w zasoby narzędzia e-KSSiP, w tym instalacji złośliwego oprogramowania, detekcji żądania niepowołanych informacji (usług sieciowych, typu oprogramowania).
3. Analiza zagrożeń utraty danych.
4. Analiza aktualności oprogramowania, systemu backupu.
5. Analiza systemu bezpieczeństwa po stronie firmy realizującej umowę hostingu na potrzeby narzędzia e-KSSiP, analiza wszelkich zabezpieczeń narzędzia e-KSSiP realizowanych po stronie hostingodawcy weryfikacja implementacji norm ISO rodziny 27000 (określonych w rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności) lub innych norm i certyfikatów, analiza zabezpieczeń fizycznych w kontekście zapewnienia bezpieczeństwa i ciągłości działania narzędzia e-KSSiP; Weryfikacja procedur i instrukcji w zakresie zapewnienia ciągłości działania systemów informatycznych oraz w zakresie zarządzania ryzykiem incydentu naruszenia bezpieczeństwa informacji.
6. Weryfikacja sposobu monitorowania bezpieczeństwa, wydajności i awarii infrastruktury informatycznej narzędzia e-KSSiP.

W ramach prac Wykonawca zidentyfikuje występujące problemy i ich prawdopodobne przyczyny, opracuje rekomendacje działań odnoszących się do zapewnienia zgodności działania Zamawiającego z wymaganiami dokumentów, o których mowa w rozdziale 1.1 a) przedmiotowego zapytania.

**W toku prac, w przypadku stwierdzenia wad lub błędów o charakterze krytycznym, Wykonawca niezwłocznie powiadomi o nich Zamawiającego, niezależnie od wymogów i terminów przewidzianych dla sporządzenia Raportu**

* 1. **Wymagane rezultaty audytu bezpieczeństwa systemu informatycznego oraz bezpieczeństwa informacji** **w narzędziu e-KSSiP wraz ze środowiskiem sieciowym.**

Dla audytu bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji Wykonawca sporządzi Raport, który będzie zawierać co najmniej:

* 1. Szczegółowy wykaz wszystkich obszarów poddanych audytowi (wraz z konkretnymi zabezpieczeniami), ich opis oraz ocenę stanu bezpieczeństwa – obejmujący narzędzie, środowisko sieciowe oraz usługodawcę hostingu
  2. Szczegółowy opis wykonanych testów wraz ich wynikami.
  3. Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń (prawdopodobieństwo wystąpienia i mechanizm zminimalizowania/eliminacji skutków).
  4. Zalecenia dotyczące sposobów usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyk

**Wszystkie dokumenty związane z przeprowadzonym audytem bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji Wykonawca dostarczy Zamawiającemu w wersji papierowej oraz w postaci elektronicznej na nośniku.**

Wykonawca pisemnie zobowiąże się, że dokumenty te będzie traktował, jako poufne i nie przekaże ani nie udostępni ich nikomu bez pisemnej zgody Zamawiającego.

Zamawiający przewiduje, że realizacja Zamówienia rozpocznie się w maju 2024 r.

**1.4 Warunki płatności**

Wypłata wynagrodzenia nastąpi na podstawie prawidłowo wystawionego przez Wykonawcę rachunku lub faktury, po stwierdzeniu wykonania Przedmiotu zamówienia (po przyjęciu Zamówienia, stwierdzonego Protokołem zdawczo-odbiorczym).

Płatność zostanie zrealizowana w terminie 21 dni od daty doręczenia Zamawiającemu prawidłowo wystawionego rachunku lub faktury przez Wykonawcę. Płatność będzie realizowana przelewem na rachunek bankowy Wykonawcy wskazany w umowie.

1. **Warunki udziału w postępowaniu**

Do udziału w niniejszym postępowaniu dopuszczeni będą Wykonawcy, spełniający warunki dotyczące bezstronności (brak konfliktu interesów) oraz posiadania wiedzy i doświadczenia.

* 1. **Warunek dotyczący bezstronności (brak konfliktu interesów):**

Wykonawca (oraz osoba wskazana w formularzu ofertowym) nie może być powiązany osobowo i kapitałowo z Zamawiającym, ani z wykonawcami narzędzia e-KSSiP (OPGK Rzeszów SA, NET-EXPRESS Teresa Jurkowska Lublin, SoftIQ sp. z o.o. Gliwice) ani z firmą realizująca usługę hostingu Flowberg It sp. z o.o., ul. Sucha 3, Wrocław).

**Przez powiązania kapitałowe lub osobowe z Zamawiającym** rozumie się wzajemne powiązania, między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami, wykonującymi w imieniu Zamawiającego czynności, związane z przygotowaniem i przeprowadzeniem procedury wyboru Wykonawcy, a Wykonawcą, polegające w szczególności na:

* + - * Uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej.
      * Posiadaniu, co najmniej 10 % udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa.
      * Pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika.
      * Pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze Wykonawcy, w szczególności pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Ponadto **przez powiązania kapitałowe lub osobowe z wykonawcą narzędzia e-KSSiP** rozumie się wzajemne powiązania, między wykonawcą narzędzia e-KSSiP lub osobami upoważnionymi do zaciągania zobowiązań w imieniu wykonawcy narzędzia e-KSSiP lub osobami, wykonującymi w imieniu wykonawcy narzędzia e-KSSiP czynności, polegające w szczególności na:

* + - * Uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej.
      * Posiadaniu, co najmniej 10 % udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa
      * Pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika.
      * Pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze Wykonawcy, w szczególności pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Ponadto przez **powiązania kapitałowe lub osobowe z hostingodawcą** rozumie się wzajemne powiązania, między hostingodawcą lub osobami upoważnionymi do zaciągania zobowiązań w imieniu hostingodawcy lub osobami, wykonującymi w imieniu hostingodawcy czynności, polegające w szczególności na:

* + - * Uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej.
      * Posiadaniu, co najmniej 10 % udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa
      * Pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika.
      * Pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze Wykonawcy, w szczególności pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Sposób oceny spełniania warunku:

Do oferty należy załączyć oddzielnie oświadczenie Wykonawcy i oddzielnie oświadczenie osoby wskazanej w formularzu ofertowym o braku powiązań z Zamawiającym, Wykonawcą narzędzia e-kssip oraz z hostingodawcą.

**2.2 Warunek dotyczący posiadania doświadczenia**

Zamawiający uzna, że Wykonawca, spełnia warunek doświadczenia, gdy w okresie ostatnich trzech lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie) wykonał **co najmniej po dwie usługi**, odpowiadające swoim rodzajem usługi stanowiące przedmiot zamówienia, przy czym wartość każdej ze wskazanych usług nie może być mniejsza niż10 000,00 złotych brutto (słownie złotych brutto: dziesięć tysięcy złotych). Nadto usługi wykazane jako doświadczenie Wykonawcy muszą wspólnie spełniać następujące kryteria:

* obejmować audyt bezpieczeństwa danych osobowych,
* być realizowane na rzecz sektora administracji publicznej,
* obejmować system zawierający minimum 1000 zarejestrowanych użytkowników.

Pod pojęciem „usług odpowiadających swoim rodzajem usługom stanowiącym przedmiot zamówienia” w zakresie zamówienia Zamawiający rozumie usługi przeprowadzania audytów lub testów informatycznych, mających w  swoim zakresie m.in. inwentaryzację zasobów sprzętowych i programowych systemów informatycznych, bezpieczeństwo systemów informatycznych i bezpieczeństwo przetwarzania informacji, w szczególności danych osobowych.

Na potwierdzenie spełnienia warunku w zakresie doświadczenia Wykonawca zobowiązany jest przedłożyć wykaz usług, zgodnie z wzorem zawartym w Załączniku nr 1 do zapytania ofertowego.Wykonanie lub wykonywanie usług zamieszczonych w wykazie musi być potwierdzone poświadczonymi za zgodność z oryginałem w szczególności: referencjami, zaświadczeniami, protokołami odbioru itp., że usługi te zostały wykonane lub są wykonywane należycie.

Sposób oceny spełniania warunku:

Warunek zostanie oceniony na podstawie informacji zawartych w Załączniku nr 1. Do oferty należy załączyć wymagane wskazane dokumenty potwierdzające posiadane doświadczenie w realizacji danej części zamówienia.

* 1. **Warunek dotyczący dysponowania osobami zdolnymi do wykonania zamówienia**

O udzielenie zamówienia dotyczącego - audytu bezpieczeństwa systemu informatycznego oraz bezpieczeństwa informacji mogą ubiegać się Wykonawcy, którzy wykażą, że dysponują lub będą dysponować osobą lub osobami, które będą uczestniczyć w wykonaniu zamówienia, spełniającymi wymagania określone w pkt 1) oraz posiadającymi przynajmniej 1 aktualny certyfikat z wymienionych poniżej w pkt 2) i 3). W przypadku wskazania jednej osoby, musi ona spełniać wymagania z pkt 1) oraz posiadać przynajmniej po aktualnym 1 certyfikacie z wymienionych poniżej w pkt 2) i 3).

* Szczegółowy wykaz warunków:
  + 1. wykształcenie wyższe,
    2. posiadać doświadczenie w zakresie przeprowadzania audytów/testów odpowiadających swoim zakresem przedmiotowi niniejszego zamówienia oraz **co najmniej jeden** aktualny certyfikat z przedstawionych poniżej:
       1. Certified Internal Auditor (CIA),
       2. Certified Information System Auditor (CISA),
       3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób,
       4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób,
       5. Certified Information Security Manager (CISM),
       6. Certified in Risk and Information Systems Control (CRISC),
       7. Certified in the Governance of Enterprise IT (CGEIT),
       8. Certified Information Systems Security Professional (CISSP),
       9. Systems Security Certified Practitioner (SSCP),
       10. Certified Reliability Professional,
       11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert,

lub równoważny,

* + 1. W zakresie testów osoba je wykonująca posiadać **co najmniej jeden** aktualny certyfikat z przedstawionych poniżej:
       1. OSCP (Offensive Security Certified Professional),
       2. OSCE (Offensive Security Certified Expert)
       3. GXPN (GIAC Exploit Researcher and Advanced Penetration Tester),
       4. CEH (EC-Council Certified Ethical Hacker),
       5. eLearnSecurity Web application Penetration Tester (eWPT),
       6. eLearnSecurity Web application Penetration Tester eXtreme (eWPTX), lub równoważny.

Sposób oceny spełniania warunku:

Warunek zostanie oceniony na podstawie informacji i oświadczeń zawartych w Załączniku nr 1. (formularz ofertowy) oraz na podstawie załączonych kopii potwierdzonych za zgodność z oryginałem certyfikatów wskazanych przez Wykonawcę w formularzu ofertowym.

Uwaga: dotyczy pkt. 2.1. – 2.3: Jako certyfikat równoważny zamawiający rozumie posiadanie certyfikatów analogicznych do zakresu wskazanych certyfikatów tj. dotyczących analogicznej dziedziny merytorycznej wynikającej z roli, której dotyczy certyfikat, analogicznego stopnia poziomu kompetencji, analogicznego poziomu doświadczenia zawodowego wymaganego dla otrzymania danego certyfikatu itp.

**NIESPEŁNIENIE POWYŻSZYCH WARUNKÓW UDZIAŁU W POSTĘPOWANIU BĘDZIE SKUTKOWAĆ ODRZUCENIEM OFERTY**

1. **Termin realizacji zamówienia**

14 dni kalendarzowych od daty zawarcia umowy.

1. **Kryteria oceny ofert**

Przy wyborze oferty najkorzystniejszej Zamawiający będzie stosował następujące kryteria i ich wagi:

Kryterium cena: Waga 100% (od 0 do 100 pkt)

Opis sposobu oceny kryterium oraz obliczania wartości punktowej kryterium:

Opis sposobu oceny:

Ocena złożonych ofert w zakresie kryterium „Cena” zostanie dokonana na podstawie podanej w ofercie przez Wykonawcę całkowitej ceny brutto za realizację usługi będącej przedmiotem niniejszego zamówienia.

Cena oferty musi zawierać wszystkie koszty i opłaty niezbędne dla realizacji zamówienia

Liczba punktów w tym kryterium zostanie obliczona wg następującego wzoru:

1. **Informacje dotyczące wyboru najkorzystniejszej oferty**

Zamawiający wybierze ofertę spełniającą wszystkie wymagania oraz warunki udziału w postepowaniu (o ile zostały określone w treści zapytania) oraz taką, która uzyska największą liczbę punktów zgodnie z wyżej przyjętymi kryteriami oceny ofert.

1. **Termin i sposób składania ofert**
2. Ofertę należy złożyć do dnia 19 kwietnia 2024
3. Określenie miejsca i sposobu składania ofert:
4. pocztą elektroniczną na adres (e-mail): [informatyka@kssip.gov.pl](mailto:informatyka@kssip.gov.pl)
5. osobiście lub za pośrednictwem poczty/kuriera na adres:

miejsce: Krajowa Szkoła Sądownictwa i Prokuratury

adres: ul. Przy Rondzie 5, 31-547 Kraków

godziny pracy kancelarii KSSIP: od 7:30 do 15:30 od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy,

1. **Informacje dodatkowe**
2. Ofertę należy sporządzić na załączonym do zapytania ofertowego załączniku - formularzu oferty i przekazać do Zamawiającego zgodnie ze sposobem określonym w ust. 6 pkt 2.
3. W ofercie należy wskazać cenę netto oraz brutto na określony w zapytaniu ofertowym przedmiot zamówienia.
4. **Wszelkich informacji udziela**

Bartosz Kuźma, tel.: 12 617 96 49, e-mail: [b.kuzma@kssip.gov.pl](mailto:b.kuzma@kssip.gov.pl)

Piotr Tomasikiewicz, tel. 12 617 96 48, e-mail: [p.tomasikiewicz@kssip.gov.pl](mailto:p.tomasikiewicz@kssip.gov.pl)

1. **Klauzula informacyjna dla Wykonawcy**

Administratorem danych osobowych zawartych w dokumentach postępowania, w tym w ofercie składanej przez Wykonawcę ubiegającego się o udzielenie zamówienia publicznego, a także w dokumentach podwykonawców oraz podmiotów trzecich udostępniających zasoby oraz w dokumentach związanych z realizacją udzielonego zamówienia jest Krajowa Szkoła Sądownictwa i Prokuratury (dalej: KSSiP), z siedzibą przy ul. Przy Rondzie 5, 31-547 Kraków.

Administrator informuje, że:

1) Kontakt z Inspektorem Ochrony Danych (IOD), również w zakresie realizacji praw, o których mowa w pkt. 5, realizowany jest za pośrednictwem adresu mailowego: iod@kssip.gov.pl.

2) Pani/Pana dane będą przetwarzane w celu udzielenia i realizacji zamówienia publicznego oraz jego rozstrzygnięcia, ponadto zawarcia umowy w sprawie zamówienia publicznego oraz jej realizacji, na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych– zgodnie z art. 6 ust. 1 c RODO.

3) Pani/Pana dane będą przetwarzane jedynie przez upoważnionych pracowników KSSiP zaangażowanych w proces udzielenia i realizacji zamówienia publicznego oraz mogą być udostępniane organom i osobom uprawnionym na mocy przepisów prawa.

4) Pani/Pana dane osobowe przetwarzane będą do czasu zakończenia procesu udzielenia i realizacji zamówienia publicznego. Po zakończeniu procesu dane będą przechowywane przez okres określony w przepisach prawa oraz wewnętrznych procedurach archiwizacyjnych KSSiP.

5) Przysługuje Pani/Panu, na zasadach określonych w RODO i przepisach prawa krajowego, prawo do żądania dostępu do swoich danych osobowych, ich sprostowania lub ograniczenia przetwarzania.

6) Wskazane w punkcie 5 prawa podlegają następującym ograniczeniom:

a) skorzystanie z uprawnienia do sprostowania lub uzupełnienia danych (art. 16 RODO) nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu postępowania oraz jego załączników;

b) prawo żądania od administratora ograniczenia przetwarzania danych osobowych (art. 18 RODO) nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania.

7) Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych osobowych.

8) Podanie danych w procesie udzielenia i realizacji zamówienia publicznego jest wymogiem ustawowym, jest niezbędne do skutecznego jego przeprowadzenia. Niepodanie danych skutkuje brakiem możliwości udziału w procesie.

9) Pani/Pana dane osobowe nie będą przetwarzane w celach związanych z automatycznym podejmowaniem decyzji, w tym w oparciu o profilowanie.

10) Pani/Pana dane nie będą przekazywane do państw trzecich, ani do organizacji międzynarodowych.

1. **Uwagi końcowe**

1) W przypadku, gdy w wyniku niniejszego postępowania wartość zamówienia wyniesie lub przekroczy kwotę 130 000 zł (bez VAT), złożone oferty posłużą wyłącznie do oszacowania wartości zamówienia w celu przeprowadzenia postępowania w trybie ustawy Pzp;

2) Zamawiający zastrzega sobie prawo do unieważnienia postępowania o udzielenie zamówienia bez podawania przyczyny na każdym etapie postępowania;

3) Zamawiający może unieważnić postępowanie, w szczególności, jeżeli:

a) cena lub koszt najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że, Zamawiający może zwiększyć tę kwotę do ceny lub kosztu najkorzystniejszej oferty;

b) Wykonawcy tak samo ocenieni, złożą oferty dodatkowe o takiej samej cenie lub koszcie;

c) wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć;

d) postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego;

4) Wszelkie koszty związane z przygotowaniem oferty oraz jej dostarczeniem ponosi Wykonawca.

5) Wykonawcom biorącym udział w postępowaniu nie przysługują żadne roszczenia z tytułu unieważnienia postępowania przez Zamawiającego.

6) Zamawiający zastrzega, że jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający może wezwać Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

7) Zamawiający zastrzega, że może podjąć negocjacje z Wykonawcą/Wykonawcami w zakresie ceny oferty.

8) Zamawiający dokona poprawy oczywistych omyłek rachunkowych polegających na błędnym przemnożeniu, zsumowaniu poszczególnych pozycji w formularzu ofertowym z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek.

9) Zamawiający może wezwać Wykonawcę do wyjaśnienia treści złożonej oferty. Nieprzedłożenie przez Wykonawcę wyjaśnień treści oferty w wyznaczonym przez Zamawiającego terminie skutkować będzie odrzuceniem oferty. Niedopuszczalne jest prowadzenie między Zamawiającym a Wykonawcą negocjacji dotyczących złożonej oferty, poza sytuacją opisaną w ust. 10 pkt. 7)

10) Zamawiający przewiduje możliwość jednokrotnego wezwania Wykonawcy do uzupełnienia dokumentów, wskazanych w zapytaniu ofertowym, w sytuacji ich niezłożenia wraz z ofertą. Nieprzedłożenie przez Wykonawcę uzupełnionych dokumentów w wyznaczonym przez Zamawiającego terminie skutkować będzie odrzuceniem oferty. Nie wzywa się Wykonawcy, jeżeli dokument służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert.

11) Oferty zawierające zapisy niezgodne z postanowieniami zapytania lub wniesione po terminie składania ofert pozostawia się bez rozpatrzenia.

**Załączniki**

* + - 1. Załącznik nr 1 - Formularz ofertowy
      2. Załącznik nr 2 - Klauzula Informacyjna dla podmiotów przystępujących do postępowania o udzielenie zamówienia publicznego
      3. Załącznik nr 3 - Wzór umowy
      4. Załącznik nr 4 – Wzór umowy powierzenia danych

..……….……………….. Bartosz Kuźma ..……………………………..

podpis pracownika sporządzającego zapytanie ofertowe