**Opis Przedmiotu Zamówienia**

1. **Informacje ogólne dotyczące przedmiotu zamówienia**
2. Przedmiotem zamówienia jest świadczenie usługi polegającej na umożliwieniu składania, przyjmowania i obsługi zgłoszeń o naruszeniach prawa, dokonywanych przez tzw. sygnalistów, za pośrednictwem systemu teleinformatycznego, który zapewni Wykonawca, zwanego dalej „Systemem”.
3. Przedmiot zamówienia dotyczy zgłoszeń o naruszeniach prawa, o których mowa w przepisach dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. *w sprawie ochrony osób zgłaszających naruszenia prawa Unii* (Dz. Urz. UE. L Nr 305, str. 17), zwanej dalej „dyrektywą (UE) 2019/1937”.
4. Okres świadczenia usługi przez Wykonawcę wynosi12 miesięcy. Szczegółowe terminy dotyczące realizacji przedmiotu zamówienia zostały wskazane w Projektowanych postanowieniach umowy w sprawie zamówienia publicznego, stanowiących załącznik nr 1 do Zapytania ofertowego.
5. System powinien spełniać wymagania określone w przepisach powszechnie obowiązującego prawa unijnego i krajowego, w szczególności dyrektywy (UE) 2019/1937. W przypadku zmiany przepisów prawa, w tym wejścia w życie przepisów prawa krajowego implementujących dyrektywę do krajowego porządku prawnego, Wykonawca w ciągu 14 dni od dnia ich ogłoszenia dostosuje System do wymagań wynikających z tych przepisów (w przypadku niedostosowania Systemu Zamawiający będzie uprawniony do wypowiedzenia umowy ze skutkiem natychmiastowym).
6. Ochrona danych osobowych:
   1. System powinien zapewniać rozwiązania zgodne z rozporządzeniem 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), (Dz. Urz. UE L 119 z 04.05.2016, str. 1),
   2. dane osobowe przechowywane przez System nie mogą być przetwarzane (w tym przechowywane, kopiowane, przesyłane) poza obszarem Europejskiego Obszaru Gospodarczego,
   3. w związku z przetwarzaniem danych osobowych Zamawiający powierzy Wykonawcy przetwarzanie danych osobowych, których Zamawiający jest administratorem   
      (tj. danych osobowych zawartych w zgłoszeniach i niezbędnych do obsługi zgłoszeń, wprowadzanych do Systemu). W tym celu niezbędne jest zawarcie z Wykonawcą umowy powierzenia przetwarzania danych osobowych.
7. Przed rozpoczęciem korzystania z Systemu przez Zamawiającego, Wykonawca zapewni wskazanej przez Zamawiającego osobie (Pełnomocnikowi ds. zgłoszeń) krótkie szkolenie instruktażowe (w formie on-line) dotyczące obsługi Systemu i jego poszczególnych funkcjonalności.

1. **Wymagania dotyczące funkcjonalności Systemu.**
2. System powinien umożliwiać składanie przez sygnalistę zgłoszeń o naruszeniu prawa drogą elektroniczną, poprzez uzupełnienie przez sygnalistę szablonu zgłoszenia i wysłanie go w sposób umożliwiający zapoznanie się z treścią zgłoszenia przez Pełnomocnika ds. zgłoszeń.
3. Zgłaszanie powinno następować za pomocą dedykowanej, indywidualnej strony dla sygnalistów z logo Zamawiającego oraz możliwością podpięcia własnej domeny.
4. System powinien umożliwiać przyjmowanie zgłoszeń przez cały rok – 7 dni w tygodniu, 24 godziny na na dobę. Ewentualne nieprawidłowości w działaniu Systemu, w szczególności przerwy w dostępie do Systemu dla sygnalistów (brak możliwości skutecznego składania zgłoszeń, komunikacji między sygnalistą a Pełnomocnikiem ds. zgłoszeń) nie mogą przekroczyć 2% czasu realizacji przedmiotu zamówienia.
5. System powinien umożliwiać dokonywanie zgłoszeń zarówno anonimowo jak i z podaniem danych osobowych przez sygnalistę, przy czym Zamawiający powinien mieć możliwość wyłączenia możliwości przyjmowania zgłoszeń anonimowych, albo przynajmniej ich łatwego wyodrębnienia „jednym kliknięciem” (tak, by – w zależności od przepisów krajowych oraz wewnętrznych regulacji Zamawiającego – zgłoszenia anonimowe mogły zostać łatwo wyselekcjonowane i pozostawione bez rozpatrzenia, usunięte z Systemu). W przypadku zgłoszeń, które zostaną podpisane przez sygnalistę imieniem i nazwiskiem, przyjęte rozwiązania powinny zapewniać poufność danych osobowych.
6. System powinien umożliwiać sygnaliście dołączanie do zgłoszenia załączników (maksymalna objętość jednego pliku załącznika, jaką może dołączyć do wiadomości sygnalista, nie może być mniejsza niż 5 MB, łączna maksymalna objętość plików stanowiących załączniki do jednego zgłoszenia nie może być mniejsza niż 20 MB).
7. Dostęp do Systemu i obsługa zgłoszeń:
   1. ze strony Zamawiającego za obsługę zgłoszeń sygnalistów przy pomocy Systemu (tj. przyjmowanie, obsługę zgłoszeń, korespondencję z sygnalistą) odpowiedzialna będzie osoba wskazana przez Zamawiającego, tj. Pełnomocnik ds. zgłoszeń – 1 osoba, która dostęp do Systemu będzie miała po zalogowaniu się (indywidualny login i hasło),
   2. na udokumentowany wniosek Zamawiającego Wykonawca przyzna i odbierze wskazanej przez Zamawiającego osobie (Pełnomocnikowi ds. zgłoszeń) dostęp do Systemu (np. przekazanie loginu i hasła/zresetowanie hasła),
   3. przyjęty sposób przekazywania dostępu do Systemu dla Pełnomocnika ds. zgłoszeń powinien gwarantować poufność tych informacji – nikt poza Pełnomocnikiem ds. zgłoszeń nie powinien mieć dostępu do hasła przekazywanego Pełnomocnikowi ds. zgłoszeń (przekazanie powinno odbywać się bezpośrednio pomiędzy Wykonawcą a wskazanym przez Zamawiającego Pełnomocnikiem ds. zgłoszeń),
   4. Pełnomocnik ds. zgłoszeń po otrzymaniu hasła powinien mieć także możliwość jego samodzielnej zmiany,
   5. Zamawiający powinien mieć swobodę w decydowaniu o tym, kto ma dostęp do systemu – tj. na wniosek Zamawiającego Wykonawca powinien niezwłocznie (tj. nie później niż po upływie 8 h od zgłoszenia żądania) odebrać uprawnienia Pełnomocnikowi ds. zgłoszeń, a także przekazać je innej, wskazanej przez Zamawiającego osobie (nowemu Pełnomocnikowi ds. zgłoszeń),
   6. Pełnomocnik ds. zgłoszeń powinien mieć dostęp do Systemu (treści zgłoszeń, ich rejestru, korespondencji z sygnalistami) za pomocą panelu zarządzania zgłoszeniami,
   7. Zamawiający powinien mieć możliwość dostosowania treści szablonu zgłoszenia do swoich potrzeb (np. możliwość określania jakie kategorie informacji powinno zawierać zgłoszenie),
   8. tworzenie szablonów zgłoszeń powinno być możliwe z panelu administracyjnego dostępnego dla Pełnomocnika ds. zgłoszeń. Powinno być możliwe łatwe tworzenie pól formularzy oraz kategorii zgłoszeń.
8. W sytuacji, w której sygnalista wyśle zgłoszenie, System powinien generować natychmiastowe powiadomienie o otrzymaniu zgłoszenia na adres e-mail Pełnomocnika ds. zgłoszeń (opcjonalnie również telefonicznie, ale nie jest to wymóg obligatoryjny).
9. System powinien umożliwiać dalszą komunikację sygnalisty z Pełnomocnikiem ds. zgłoszeń (możliwość wysyłania przez Pełnomocnika ds. zgłoszeń do sygnalisty wiadomości, informacji, wniosków o dowolnej treści, wraz z załącznikami, możliwość odpowiadania na te wiadomości przez sygnalistę) – po uprzedniej weryfikacji przez System, że osoba korespondująca z Pełnomocnikiem ds. zgłoszeń jest osobą, która wcześniej wysłała dane zgłoszenie. System powinien w związku z tym np. generować dla sygnalisty login i hasło lub identyfikator zgłoszenia, który sygnalista powinien wpisać do Systemu w celu uwierzytelnienia tożsamości (dzięki temu Pełnomocnik ds. zgłoszeń będzie mieć pewność, że koresponduje z osobą, od której pochodziło konkretne zgłoszenie).
10. System powinien umożliwiać monitorowanie obsługi poszczególnych wniosków (alarmowanie o wnioskach, na które nie udzielono odpowiedzi pomimo zbliżającego się czasu na jej udzielenie, Zamawiający powinien mieć możliwość ustawiania warunków monitów, tak by były one dostosowane do terminów określonych w przepisach prawa oraz wewnętrznym regulaminie rozpatrywania zgłoszeń przyjętym przez Zamawiającego).
11. Zgłoszenia, załączniki, dane osobowe i korespondencja sygnalisty z Pełnomocnikiem ds. zgłoszeń, powinny być przechowywane na serwerach Wykonawcy znajdujących się na terenie państw należących do Europejskiego Obszaru Gospodarczego. Poza Pełnomocnikiem ds. zgłoszeń wskazanym przez Zamawiającego, nikt z organizacji Zamawiającego nie będzie miał dostępu do danych osobowych sygnalisty i informacji wprowadzonych do Systemu.
12. System powinien umożliwiać tworzenie zestawień zgłoszeń (w tym m.in. zgłoszenia, które wpłynęły od początku, w określonym przedziale czasowym), a ponadto wyeksportowanie utworzonego zestawienia do pliku „pdf.” lub „doc./docx.” i jego wydruk.
13. System powinien zapewniać pełny rejestr wszystkich zgłoszeń wraz ze ścieżką audytu.
14. **Wymagania techniczne dotyczące Systemu:**

**System powinien zapewniać:**

1. możliwość obsługi za pośrednictwem ogólnodostępnych przeglądarek internetowych, w tym m.in.: Internet Explorer, Mozilla Firefox, Google Chrome, Opera,
2. responsywność i gotowość do użycia na każdym urządzeniu mobilnym (tak by składanie zgłoszeń było możliwe i wygodne również za pomocą smartfonu, tabletu),
3. rozwiązanie typu SaaS,
4. mechanizmy ograniczające dokonywanie zgłoszeń przez boty, wysyłanie spamu (np. potwierdzanie wysłania zgłoszenia poprzez CAPTCHA),
5. natychmiastowe powiadomienia o otrzymaniu zgłoszeń (email i/lub sms),
6. opcję anonimowego zgłaszania i dwukierunkowej anonimowej komunikacji ze zgłaszającym,
7. zintegrowany system zarządzania zgłoszeniami z automatyzacją procesów oraz szczegółowym raportowaniem,
8. pełny rejestr wszystkich zgłoszeń wraz ze ścieżką audytu,
9. panel zarządzania zgłoszeniami sygnalistów dla wielu użytkowników,
10. indywidualną stronę dla sygnalistów z logo firmy oraz możliwością podpięcia własnej domeny,
11. komunikację przez stronę www,
12. zachowanie ciągłości korespondencji,
13. powiadomienia e-mail dla osób zarządzających zgłoszeniami w tym zgodne terminy z dyrektywą,
14. szyfrowanie treści zgłoszenia wraz z załącznikami,
15. archiwizowanie szyfrowanych zgłoszeń na koncie firmowym,
16. komunikację pomiędzy stronami bez ujawniania tożsamości sygnalisty poprzez serwer,
17. możliwość przypisania zgłoszenia do odpowiedniej osoby w celu odebrania zgłoszenia,
18. możliwość zgłoszenia sygnalisty na dwa dozwolone sposoby (Zgodnie z dyrektywą UE 2019/1937):
19. anonimowo
20. z ujawnieniem tożsamości (email/nazwisko)
21. zarządzania zgłoszeniami,
22. zabezpieczenia logowania poprzez uwierzytelnianie wielopoziomowe, np. 2FA,
23. możliwość ustawiania statusów zgłoszeń,
24. możliwość odesłania odpowiedzi wraz załącznikami,
25. możliwość zachowania korespondencji wraz z treścią i tematami,
26. możliwość tworzenia formularzy zgłoszeń z panelu administracyjnego dla zarządzających.