

Warszawa, \$data r.

BP-SWK.261.1.2026.MO

## Opis Przedmiotu Zamówienia

### I. Informacje ogólne dotyczące przedmiotu zamówienia

**1.** Przedmiotem zamówienia jest świadczenie usługi polegającej na umożliwieniu składania, przyjmowania i obsługi zgłoszeń wewnętrznych i zewnętrznych o naruszeniach prawa, dokonywanych przez tzw. sygnalistów, za pośrednictwem systemu teleinformatycznego, który zapewni Wykonawca, zwanego dalej „Systemem”.

**2.** 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” oraz ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (D.U. z 2024 r. poz. 928), zwanej dalej „ustawą”

**3.** Okres świadczenia usługi przez Wykonawcę wynosi 12 miesięcy. Szczegółowe terminy dotyczące realizacji przedmiotu zamówienia zostały wskazane w Projektowanych postanowieniach umowy (zwanym dalej „Umową”) w sprawie zamówienia publicznego, stanowiących załącznik nr 3 do Zapytania ofertowego.

**4.** System powinien spełniać wymagania określone w przepisach powszechnie obowiązującego prawa unijnego i krajowego, w szczególności dyrektywy (UE) 2019/1937 oraz w ustawie. W przypadku zmiany przepisów prawa, Wykonawca w ciągu 14 dni od dnia ich ogłoszenia dostosuje System do wymagań wynikających z tych przepisów.

#### **5. Ochrona danych osobowych:**

**a)** 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),

**b)** dane osobowe przechowywane przez System nie mogą być przetwarzane (w tym przechowywane, kopiowane, przesyłane) poza obszarem Europejskiego Obszaru Gospodarczego,

**c)** 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).

**6.** W terminie uzgodnionym przez Strony, lecz nie później niż w ciągu 3 dni roboczych od rozpoczęcia okresu wskazanego w § 2 ust. 1 Umowy, Wykonawca przeprowadzi krótkie szkolenie instruktażowe (w formie on-line lub w siedzibie Zamawiającego) dotyczące obsługi Systemu i jego poszczególnych funkcjonalności.

## **II. Wymagania dotyczące funkcjonalności Systemu.**

- 1.** System powinien umożliwiać składanie przez sygnalistę zgłoszeń wewnętrznych i zewnętrznych o naruszeniu prawa drogą elektroniczną, poprzez wypełnienie przez sygnalistę szablonu zgłoszenia i wysłanie go w sposób umożliwiający zapoznanie się z treścią zgłoszenia przez osoby wskazane przez Zamawiającego, o których mowa w pkt 8 lit. a.
- 2.** System powinien w jasny i klarowny sposób rozróżniać niezależne od siebie szablony zgłoszenia na wewnętrzny i zewnętrzny. Sygnalista musi mieć możliwość wyboru danego typu zgłoszenia.
- 3.** System powinien być zaprojektowany w sposób zapewniający jednoznaczne i intuicyjne rozróżnienie szablonów do zgłoszeń, aby zminimalizować ryzyko błędnego wyboru przez sygnalistów. Interfejs powinien mieć zaimplementowane wyraźne oznaczenia wizualne oraz elementy identyfikacyjne, które skutecznie pozwolą rozróżnić dany szablon do zgłoszeń.
- 4.** System musi zawierać panel logowania dla dwóch administratorów wewnętrznych oraz dwóch administratorów zewnętrznych. System rozróżniać musi uprawnienia do kontroli nad zgłoszeniami wysłanymi w trybie wewnętrznym oraz zewnętrznym. Administratorzy odpowiedzialni za zgłoszenia wewnętrzne mają mieć podgląd wyłącznie do zgłoszeń i danych wysłanych w trybie wewnętrznym, natomiast administratorzy odpowiedzialni za zgłoszenia zewnętrzne mają mieć podgląd wyłącznie do zgłoszeń i danych wysłanych w trybie zewnętrznym.
- 5.** Zgłaszanie powinno następować za pomocą dedykowanej, indywidualnej strony dla sygnalistów z logo Zamawiającego oraz możliwością podpięcia własnej domeny.
- 6.** System powinien umożliwiać przyjmowanie zgłoszeń przez cały rok – 7 dni w tygodniu, 24 godziny na dobę.
- 7.** 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.
- 8.** 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).
- 9.** Dostęp do Systemu i obsługa zgłoszeń:
  - a)** ze strony Zamawiającego za obsługę zgłoszeń sygnalistów przy pomocy Systemu (tj. przyjmowanie, obsługę zgłoszeń, korespondencję z sygnalistą) odpowiedzialne będą maksymalnie cztery osoby wskazane przez Zamawiającego (dwie do zgłoszeń wewnętrznych i dwie do zgłoszeń zewnętrznych), które będą miały dostęp do Systemu po zalogowaniu się (indywidualny login i hasło dla każdej z nich),
  - b)** przyjęty sposób przekazywania dostępu do Systemu dla osób, o których mowa w lit. a, powinien gwarantować poufność tych informacji – nikt poza osobą wskazaną przez Zamawiającego nie powinien mieć dostępu do hasła przekazywanego danej osobie (przekazanie powinno odbywać się bezpośrednio pomiędzy Wykonawcą a wskazaną przez Zamawiającego osobą),
  - c)** wskazana przez Zamawiającego osoba po otrzymaniu hasła powinna mieć także możliwość jego samodzielnej zmiany,

**d)** 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 danej osobie, a także przekazać je innej osobie, wskazanej przez Zamawiającego,

**e)** każda z osób wskazanych przez Zamawiającego powinna mieć dostęp do Systemu (treści zgłoszeń, ich rejestru, korespondencji z sygnalistami) za pomocą panelu zarządzania zgłoszeniami,

**f)** Zamawiający powinien mieć możliwość dostosowania treści szablonu zgłoszenia do swoich potrzeb (np. możliwość określania jakie kategorie informacji powinno zawierać zgłoszenie),

**g)** tworzenie szablonów zgłoszeń powinno być możliwe z panelu administracyjnego dostępnego dla osoby, o której mowa w lit. a. Powinno być możliwe łatwe tworzenie pól formularzy oraz kategorii zgłoszeń.

**10.** W sytuacji, w której sygnalista wyśle zgłoszenie, System powinien generować natychmiastowe powiadomienie o otrzymaniu zgłoszenia na adres e-mail tych dwóch osób ze wskazanych przez Zamawiającego, które upoważnione są do obsługi danej kategorii zgłoszeń (wewnętrzne lub zewnętrzne – opcjonalnie również telefonicznie, ale nie jest to wymóg obligatoryjny).

**11.** System powinien umożliwiać dalszą komunikację sygnalisty z osobą, o której mowa w pkt 8 lit. a (możliwość wysyłania przez tę osobę 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 osobą, o której mowa w pkt 8 lit. a, 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 osoby, o których mowa w pkt 8 lit. a, będą miały pewność, że korespondują z osobą, od której pochodziło zgłoszenie).

**12.** 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 wewnętrznych regulaminów rozpatrywania zgłoszeń przyjętych przez Zamawiającego).

**13.** Zgłoszenia, załączniki, dane osobowe i korespondencja sygnalisty z osobami, o których mowa w pkt 8 lit. a, powinny być przechowywane na serwerach Wykonawcy znajdujących się na terenie państw należących do Europejskiego Obszaru Gospodarczego. Poza osobami, o których mowa w pkt 8 lit. a, nikt z organizacji Zamawiającego nie będzie miał dostępu do danych osobowych sygnalisty i informacji wprowadzonych do Systemu.

**14.** System powinien umożliwiać tworzenie zestawień zgłoszeń, w tym w podziale na zestawienie zgłoszeń wewnętrznych i zewnętrznych (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.

**15.** System powinien zapewniać pełny rejestr wszystkich zgłoszeń, w tym w podziale na rejestr zgłoszeń wewnętrznych i zewnętrznych, wraz ze ścieżką audytu.

**16.** System powinien zapewniać możliwość importowania zgłoszeń z aktualnego systemu obsługi zgłoszeń sygnalistów, którym posługuje się Zamawiający lub możliwość ręcznego wprowadzenia treści zgłoszenia dokonanego za pomocą dotychczasowego systemu do obsługi zgłoszeń sygnalistów z możliwością kontynuacji sprawy od etapu, na którym się znajduje w ramach Systemu.

**17.** System powinien zapewniać kompletność, poufność i integralność danych, w tym ich zabezpieczenie przed dostępem osób nieupoważnionych.

### **III. Wymagania techniczne dotyczące Systemu:**

System powinien zapewniać:

1. możliwość obsługi za pośrednictwem ogólnodostępnych przeglądarek internetowych, w tym m. in.: 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, w tym w podziale na rejestr zgłoszeń wewnętrznych i zewnętrznych, 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 w szczególności o wpłynięciu zgłoszenia, w tym terminy zgodne z dyrektywą UE 2019/1937 oraz ustawą,
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 i ustawą):
  - a) anonimowo
  - b) z ujawnieniem tożsamości (e-mail/nazwisko)
19. zarządzania zgłoszeniami,
20. zabezpieczenia logowania poprzez uwierzytelnianie wielopoziomowe, np. 2FA,
21. możliwość ustawiania statusów zgłoszeń,
22. możliwość odesłania odpowiedzi wraz załącznikami,
23. możliwość zachowania korespondencji wraz z treścią i tematami,
24. możliwość tworzenia formularzy zgłoszeń z panelu administracyjnego dla zarządzających,

**25.** spełnianie standardów WCAG (Web Content Accessibility Guidelines).

\$IMIE\_NAZWISKO\_PODPISUJACEGO

\$STANOWISKO\_PODPISUJACEGO

\$DEPARTAMENT\_PODPISUJACEGO

/ – podpisany cyfrowo/