

## INSTRUKCJA ROZPATRYWANIA ZGŁOSZONYCH NARUSZEŃ

### I. Postanowienia ogólne

1. Niniejszy dokument stanowi praktyczną wskazówkę dla osób upoważnionych do przyjmowania zgłoszeń od sygnalistów, wykonywania działań następczych oraz komunikowania się z sygnalistą.
2. *Instrukcja rozpatrywania zgłoszonych naruszeń* jest załącznikiem do *Procedury przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*, która kompleksowo przedstawia wymagania dotyczące przyjmowania zgłoszeń zewnętrznych dotyczących naruszeń prawa.
3. Za wykonanie instrukcji odpowiedzialne są osoby wyznaczone do obsługi zgłoszeń, działające na podstawie pisemnego upoważnienia.
4. Z niniejszą instrukcją powinny zapoznać się wszystkie osoby upoważnione do obsługi zgłoszeń zewnętrznych.
5. Instrukcja opiera się na założeniach działania platformy do przyjmowania zgłoszeń SYGNALISTA24.info. Platforma ta umożliwia:
  - a) przyjmowanie zgłoszeń,
  - b) wymianę korespondencji z sygnalistą,
  - c) dokumentowanie wszelkich działań związanych ze zgłoszeniem,
  - d) prowadzenie rejestru zgłoszeń zewnętrznych,
  - e) całościowe zarządzanie zgłoszeniami– stąd wymagane jest wprowadzanie wszystkich otrzymanych zgłoszeń naruszeń prawa do tej platformy.

### II. Dostęp do platformy SYGNALISTA24.info

#### 1. Dostęp do platformy po stronie podmiotu przyjmującego zgłoszenia

- 1) Dostęp do platformy po stronie podmiotu przyjmującego zgłoszenia mają tylko osoby upoważnione, którym przypisano określone role.
- 2) Osoby wyznaczone do obsługi zgłoszeń mogą pełnić następujące funkcje:
  - a) główny odbiorca zgłoszeń – 1 osoba – pełniąca funkcję administratora; odpowiedzialna m.in. za zakładanie profilu podmiotu i jego aktualizację, a także nadająca uprawnienia pozostałym osobom (koordynatorom);
  - b) odbiorca zgłoszeń – co najmniej 1 osoba zgodnie z wykupionym pakietem – przyjmująca zgłoszenia od sygnalistów, wykonująca działania następcze oraz komunikująca się z sygnalistą.
- 3) Za nadawanie i odbieranie dostępów do systemu odpowiedzialny jest główny odbiorca zgłoszeń, który zobowiązany jest również do zabezpieczenia hasła master (hasła głównego) do platformy.

- 4) Powołani zgodnie z §6 Procedury przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych członkowie zespołu ds. obsługi zgłoszeń i podejmowania działań następczych nie otrzymują dostępu do platformy SYGNALISTA24.info. Nie są również zobowiązani do komunikacji z sygnalistą.
- 5) Osoby upoważnione do przyjmowania zgłoszeń lub podejmowania działań następczych otrzymują na podany adres e-mail powiadomienia, np. informacje o nowym zgłoszeniu, o nowej wiadomości lub zbliżających się terminach realizacji poszczególnych zadań.

## **2. Dostęp do platformy po stronie sygnalisty**

- 1) Dostęp do systemu po stronie sygnalisty ma osoba zgłaszająca.
- 2) Sygnalista dokonując zgłoszenia z wykorzystaniem dostępnej platformy otrzymuje unikatowy login i hasło, które powinien zabezpieczyć (zapisując lub zapamiętując), aby w przyszłości móc komunikować się w sprawie zgłoszenia.
- 3) Zgubienie lub zapomnienie podanego przy zgłoszeniu loginu i hasła uniemożliwi kontakt z osobą wyznaczoną do przyjmowania i obsługi zgłoszeń.
- 4) Sygnalista może przekazać wygenerowane poświadczenia innej osobie, jednak odpowiedzialność za wykorzystanie tych danych spoczywa na sygnaliście i osobie przez niego upoważnionej.
- 5) Sygnalista nie otrzymuje automatycznych powiadomień z systemu.

## **III. Schemat postępowania**

### **1. Założenie profilu podmiotu na platformie SYGNALISTA24.info**

- 1) Główny odbiorca zgłoszeń zakłada profil podmiotu wpisując m.in.
  - a) dane podmiotu i logotyp,
  - b) adres skrzynki dla sygnalistów,
  - c) swoje dane, tj. imię i nazwisko,
  - d) swój adres e-mail,
  - e) swoje hasło dostępowe,
  - f) hasło do odszyfrowywania wiadomości w systemie od sygnalistów,
  - g) dedykowane informacje dla sygnalistów.
- 2) Główny odbiorca zgłoszeń załącza klauzulę informacyjną dotyczącą ochrony danych osobowych dla sygnalisty zgodnie 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 65/46/WE (RODO).
- 3) Główny odbiorca zgłoszeń uzupełnia również dane innych użytkowników (odbiorców zgłoszeń), w tym imię i nazwisko oraz adres e-mail, jeżeli wykupiony pakiet systemu SYGNALISTA24.info dopuszcza taką możliwość.

### **2. Przyjęcie zgłoszenia od sygnalisty na platformie SYGNALISTA24.info**

- 1) Sygnalista korzystając z formularza udostępnionego w systemie poprzez dedykowaną stronę internetową przekazuje swoje dane osobowe oraz wszelkie posiadane informacje dotyczące naruszenia prawa, w tym również posiadane dowody. Sygnalista dodatkowo potwierdza zapoznanie się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych.
- 2) Jeżeli sygnalista poda w zgłoszeniu dane, w tym dane osobowe, które nie są istotne dla rozpatrywania zgłoszenia, należy je usunąć w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.
- 3) Jeżeli sygnalista korzystając z platformy SYGNALISTA24.info wyśle zgłoszenie anonimowe, a podmiot nie przyjmuje zgłoszeń o takim charakterze, należy poinformować o tym sygnalistę i poprosić go o podanie wymaganych danych osobowych zgodnie z §7 *Procedury przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*.
- 4) O każdym nowym zgłoszeniu lub nowej wiadomości, która zostanie przesłana do Organizacji przez sygnalistę osoba wyznaczona do obsługi zgłoszeń jest automatycznie informowana za pomocą podanego w systemie adres e-mail.
- 5) Osoba wyznaczona do obsługi zgłoszeń loguje się do swojego konta na platformie SYGNALISTA24.info za pomocą indywidualnych poświadczeń i odczytuje wiadomość po jej odszyfrowaniu.
- 6) W ciągu 7 dni od otrzymania informacji od sygnalisty należy potwierdzić wpłynięcie zgłoszenia. Odszyfrowanie i odczytanie wiadomości w systemie jest jednoznaczne z potwierdzeniem przyjęcia zgłoszenia.

### **3. Obsługa zgłoszenia**

- 1) Obsługa zgłoszenia polega na przyjęciu zgłoszenia, oceny zasadności zgłoszenia, wdrożeniu działań następczych, a następnie zamknięciu zgłoszenia i zarchiwizowaniu informacji o naruszeniu.
- 2) Po odszyfrowaniu wiadomości od sygnalisty należy zweryfikować czy zgłoszenie jest zasadne i wiarygodne, tzn. uzasadniające podjęcie działań następczych. Należy sprawdzić czy osoba zgłaszająca może być sygnalistą, jakiego obszaru dotyczy zgłoszenie oraz czy potencjalny sprawca naruszenia jest autentyczny.
- 3) Jeżeli jest taka potrzeba należy skontaktować się z sygnalistą w celu uzupełnienia brakujących informacji lub dodatkowych wyjaśnień. Kontaktując się z sygnalistą należy zawsze korzystać z platformy SYGNALISTA24.Info.
- 4) Jeżeli po weryfikacji zgłoszenia okaże się, że jest ono bezzasadne należy taką informację przekazać sygnaliście podając powód odrzucenia zgłoszenia.
- 5) Po weryfikacji przekazanych informacji należy nadać w systemie odpowiedni status zgłoszenia.
- 6) Jeżeli przekazane przez sygnalistę informacje i dowody są wystarczające do podjęcia działań następczych należy rozpocząć ich realizację.
- 7) Jeżeli sygnalista uzupełnił zgłoszenie o kolejne informacje mające wpływ na wynik działań następczych, należy weź je pod uwagę przy wykonywaniu tych działań.

- 8) Osoba upoważniona jest zobowiązana do spełnienia obowiązku informacyjnego względem osoby, która występuje w zgłoszeniu. Należy w takiej sytuacji dochować terminów wskazanych w Rozporządzeniu o ochronie danych osobowych (RODO).
- 9) Osoba upoważniona do obsługi zgłoszeń dochowuje terminów kontaktu z sygnalistą wskazanych w *Procedurze przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*.
- 10) Osoba upoważniona do obsługi zgłoszeń otrzymuje automatycznie na podanego e-maila informacje o zbliżających się terminach realizacji poszczególnych działań.
- 11) Jeżeli osoba wyznaczona do obsługi zgłoszeń nie jest w stanie dotrzymać terminu przekazania informacji zwrotnej sygnaliście zgodnie z zapisami wskazanymi w *Procedurze przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*, należy o tym fakcie poinformować sygnalistę z wyprzedzeniem, podając jednocześnie powód opóźnienia oraz wskazując realny termin przekazania informacji zwrotnej.

#### **4. Działania następcze**

- 1) Działania następcze wykonują osoby posiadające wiedzę i kompetencję odpowiednie do rozstrzygnięcia i oceniania kwestii zawartych w zgłoszeniu.
- 2) Działania następcze mogą wykonywać osoby upoważnione na stałe lub powołane do wykonywania tych działań w kontekście konkretnego zgłoszenia.
- 3) W sytuacji konieczności powołania zespołu ds. obsługi zgłoszeń należy postępować zgodnie z *Procedurą przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*.
- 4) Osoba wyznaczona do przyjmowania zgłoszeń zobowiązana jest do zebrania i przygotowania wszelkich posiadanych informacji istotnych dla określonego zgłoszenia. Informacje te należy udostępnić osobom upoważnionym do wykonania działań następczych, zachowując przy tym odpowiedni poziom bezpieczeństwa, np. poprzez zanonimizowanie danych, które nie będą miały wpływu na obiektywną ocenę zgłoszenia.
- 5) Osoby upoważnione do wykonywania działań następczych wykonują z należytą starannością wszystkie działania mające na celu potwierdzenie bądź nie, naruszeń prawa przedstawionych w zgłoszeniu.
- 6) Jeżeli w wyniku przeprowadzonego dochodzenia zewnętrznego i postępowania wyjaśniającego nie zostaną potwierdzone informacje o naruszeniu przedstawione w zgłoszeniu, takie zgłoszenie należy zamknąć bez podejmowania dalszych działań.
- 7) Jeżeli w wyniku przeprowadzonego dochodzenia zewnętrznego i postępowania wyjaśniającego zostaną potwierdzone informacje o naruszeniu przedstawione w zgłoszeniu, należy wykonać kolejne działania następcze mające na celu rozwiązanie i wyeliminowanie tego typu naruszeń.
- 8) Jeżeli okaże się, że posiadane informacje o naruszeniu prawa nie leżą w kompetencji podmiotu przyjmującego zgłoszenie osoba upoważniona zobowiązana jest do przekazania posiadanych informacji do określonego organu publicznego, którego zakres działania należy do dziedziny wskazanej w zgłoszeniu.

- 9) Osoba upoważniona do obsługi zgłoszeń przekazuje sygnaliście informację zwrotną o podjętych działaniach następczych w terminie wskazanym w *Procedurze przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*.
- 10) Po zakończeniu wszystkich działań następczych osoba wyznaczona do obsługi zgłoszeń zamyka zgłoszenie nadając odpowiedni status na platformie.

#### 5. Dokumentowanie i archiwizacja

- 1) Osoba wyznaczona do obsługi zgłoszeń dokumentuje wszelkie działania związane ze zgłoszeniem oraz archiwizuje posiadane informacje dotrzymując terminów ich przetwarzania zgodnie z *Procedurą przyjmowania zgłoszeń zewnętrznych oraz podejmowania działań następczych*.
- 2) Platforma SYGNALISTA24.info umożliwia archiwizację wszelkich działań podjętych w związku ze zgłoszeniem. Dodatkowo – jeżeli zachodzi taka konieczność – można archiwizować zapisy poprzez wygenerowanie z systemu dokumentu w formie pdf. W takiej sytuacji jednak należy zapewnić odpowiedni poziom bezpieczeństwa dla przetwarzanych w ten sposób informacji, np. poprzez nadanie hasła do dokumentu.
- 3) Rejestr zgłoszeń zewnętrznych prowadzony jest automatycznie na platformie SYGNALISTA24.info. Za prowadzenie i nadzór nad rejestrem odpowiedzialna jest osoba upoważniona do prowadzenia rejestru zgłoszeń zewnętrznych. Jeżeli zachodzi taka konieczność można ww. rejestr naruszeń wygenerować z systemu w formie pdf. Można również zabezpieczyć plik poprzez nadanie hasła do dokumentu.
- 4) Platforma SYGNALISTA24.info umożliwia również sporządzenie rocznego sprawozdania dla Rzecznika Praw Obywatelskich oraz wygenerowania go w formie pdf.

#### IV. Zasada działania platformy SYGNALISTA24.info. Pytania i odpowiedzi.

Pytanie	Odpowiedź
W jaki sposób sygnalista korzystając z platformy SYGNALISTA24.info może zgłosić naruszenie?	Formularz zgłoszeniowy dostępny jest na platformie SYGNALISTA24.info pod adresem dedykowanej skrzynki <a href="https://app.sygnalista24.info/umak">https://app.sygnalista24.info/umak</a> Do zgłoszenia można dodać załącznik w następujących formatach: .pdf,.xls,.xlsx,.doc,.docx,.ods,.odt,.jpg,.bmp,.png,.txt.
W jaki sposób realizowany jest obowiązek informacyjny wobec sygnalisty zgodny z RODO?	Podmiot umieszcza klauzulę informacyjną w postaci pliku pdf na platformie we wskazanym miejscu. Treść zamieszczonej klauzuli informacyjnej jest dostępna dla sygnalisty. Sygnalista przed wysłaniem naruszenia obowiązkowo potwierdza znajomość klauzuli informacyjnej podmiotu, do którego kieruje zgłoszenie.
Jakie pola zawiera formularz zgłoszenia? Czy tylko pole "treść zgłoszenia"?	Nie. Obok samej treści zgłoszenia sygnalista może dołączyć do zgłoszenia dowody w postaci plików w ww. formatach. W formularzu są również inne pola, np. miejsce i czas zdarzenia/naruszenia.
Czy zgłoszenia są realizowane wyłącznie anonimowo?	Platforma umożliwia obsługę zgłoszeń jawnych i anonimowych. Przy wykorzystaniu platformy kontakt z sygnalistą jest możliwy

Pytanie	Odpowiedź
	<p>bez potrzeby wykorzystywania jego danych osobowych i kontaktowych. To od sygnalisty będzie zależało, czy będzie chciał ujawnić swoją tożsamość. Zależy to również od zapisów procedury przyjmowania zgłoszeń zewnętrznych obowiązujących w danym podmiocie, które dopuszczają lub nie przyjmowanie zgłoszeń anonimowych.</p> <p>Jeżeli przepisy prawa o ochronie sygnalistów dopuszczają fakultatywne przyjmowanie zgłoszeń anonimowych, platforma SYGNALISTA24.info informuje o tym czy dany podmiot przyjmuje czy nie przyjmuje zgłoszeń anonimowych. Jest to indywidualne ustawienie pierwszego okna podmiotu, z informacją dla sygnalisty.</p>
<p>Czy system zapewnia możliwość przesłania/ przekazania/ pobrania potwierdzenia zgłoszenia?</p> <p>Czy i w jaki sposób zabezpieczony jest plik z potwierdzeniem zgłoszenia?</p>	<p>Tak. Sygnalista otrzymuje potwierdzenie dokonania zgłoszenia. Może go również pobrać w formacie pdf i zapisać z użyciem własnego hasła (wymóg systemu) lub wydrukować.</p>
<p>Czy system zapewnia możliwość generowania i zapisywania treści zgłoszenia do pliku pdf?</p>	<p>Tak. Sygnalista, jak również odbiorca zgłoszenia, mają możliwość wygenerowania do pliku pdf historii konkretnego zgłoszenia. Plik należy zabezpieczyć nadanym przez siebie hasłem (wymóg systemu). Można go również wydrukować.</p>
<p>Czy system służy wyłącznie zgłoszeniu naruszenia czy umożliwia także prowadzenie dalszej korespondencji?</p> <p>Jeżeli tak to:</p> <ul style="list-style-type: none"> <li>● w jaki sposób sygnalista będzie logował się do systemu?</li> <li>● jak zapewniono bezpieczeństwo danych do logowania?</li> <li>● jak zapewniono anonimowość sygnalisty?</li> <li>● kiedy i na jakich zasadach jest blokowany dostęp</li> </ul>	<p>Tak. Korespondencja między sygnalistą a podmiotem może być prowadzona w sposób ciągły.</p> <p>Po przesłaniu informacji przez sygnalistę odbiorca zgłoszenia otrzymuje powiadomienie na wskazany adres e-mail, informujące o tym, że na platformie SYGNALISTA24.info znajduje się nowa wiadomość. Dostęp odbiorcy do platformy możliwy jest po zalogowaniu indywidualnymi poświadczeniami.</p> <p>Sygnalista nie otrzymuje powiadomień. Aby sprawdzić korespondencję, musi zalogować się na platformę za pomocą kluczy (nr sprawy i hasło) generowanych automatycznie w momencie dokonania zgłoszenia. Bez nich nie będzie miał możliwości odczytania wiadomości od odbiorcy zgłoszenia.</p> <p>Bezpieczeństwo logowania jest zapewnione przez konieczność wejścia na platformę i użycia wygenerowanych przez system: numeru zgłoszenia i hasła. Można je zanotować lub zapisać</p>

Pytanie	Odpowiedź
<p>sygnalisty do treści zgłoszenia?</p>	<p>w formacie pdf na komputerze wyłącznie przy użyciu nadanego przez siebie hasła (wymóg systemu) lub wydrukować.</p> <p>Bezpieczeństwo sygnaliście zostaje zapewnione przez wymóg każdorazowego logowanie się za pomocą wygenerowanych podczas wysłania zgłoszenia kluczy oraz ograniczenia do 10 minut trwania jednej sesji z możliwością jej przedłużenia. Do każdego zgłoszenia generowany jest inny, własny numer zgłoszenia i niepowtarzalne hasło.</p> <p>Anonimowość sygnalisty zapewniona jest również przez usuwanie metadanych i szyfrowanie całej korespondencji (wraz z załącznikami). Dodatkowo po stronie podmiotu dostęp do platformy SYGNALISTA24.info, w tym całej zgromadzonej tam korespondencji mają tylko upoważnione osoby, logujące się do systemu z wykorzystaniem indywidualnych poświadczeń.</p> <p>Sygnalista ma dostęp do swojej skrzynki zgłoszeniowej przez cały okres toczących się wyjaśnień i działań następczych. Sygnalista otrzymuje informacje na platformie o każdej czynności związanej ze zgłoszeniem, w tym jego zakończeniem, archiwizacją lub usunięciem. Może on również pobrać całą historię korespondencji w formacie pdf i wydrukować lub zapisać używając własnego hasła. Dostęp sygnalisty do zgłoszenia blokowany jest po 12 miesiącach od momentu zamknięcia sprawy.</p>
<p>W jaki sposób system SYGNALISTA24.info zapewnia poufność komunikacji i ogranicza dostęp do zgłoszenia do osób uprawnionych?</p> <ul style="list-style-type: none"> <li>● kto nadaje dostępy dla poszczególnych odbiorców?</li> <li>● jaki jest zakres dostępu osób uprawnionych do przyjmowania zgłoszenia?</li> <li>● kto blokuje dostęp do zgłoszenia?</li> <li>● kto i jak definiuje zakres uprawnień dotyczących zgłoszenia (np. przeglądanie spraw, tworzenie notatek)?</li> </ul>	<p>Usługodawca nadaje uprawnienia głównego odbiorcy zgłoszeń (również zwanego administratorem) osobie wskazanej w umowie zawartej z podmiotem na świadczenie usługi. Główny odbiorca zgłoszeń rejestruje pozostałych użytkowników, nadaje i odbiera uprawnienia. W przypadku zmiany głównego odbiorcy zgłoszeń generowane są nowe uprawnienia dla nowego administratora wskazanego przez podmiot na piśmie.</p> <p>Główny odbiorca zgłoszeń ma również możliwość blokowania dostępu poszczególnym koordynatorom ze względu na lokalizację zgłoszenia. Usługodawca blokuje dostęp administratorowi na wyraźne, pisemne życzenie podmiotu.</p> <p>Zakres uprawnień dotyczących zgłoszenia, np. przegląd zgłoszeń, tworzenie notatek oraz uzupełnianie innych dostępnych na platformie pól, obejmują odbiorców zgłoszeń zgodnie z ustaleniami. Każda ww. czynność jest rejestrowana pod kątem terminu, jak i osoby wykonującej działanie.</p>

Pytanie	Odpowiedź
<ul style="list-style-type: none"> <li>● kto prowadzi korespondencję z sygnalistą?</li> <li>● czy system wprowadza separacje uprawnień ze względu na rolę osób upoważnionych?</li> <li>● czy system zapisuje logowanie: kto / kiedy / jakie dane wprowadził / zmodyfikował / usunął / pobrał po stronie rozpatrującej zgłoszenie?</li> <li>● jak i gdzie zabezpieczone są dane do logowania przez osoby uprawnione po stronie organizacji przyjmującej zgłoszenia?</li> </ul>	<p>Z sygnalistą korespondować mogą wszyscy upoważnieni odbiorcy zgłoszeń.</p> <p>System wprowadza separacje uprawnień ze względu na rolę osób upoważnionych (główny odbiorca zgłoszeń posiada większe uprawnienia).</p> <p>System odnotowuje każdą wykonywaną czynność: kto / kiedy / jakie dane wprowadził / zmodyfikował / pobrał / przesłał.</p> <p>Dane do logowania, tj. hasło do odszyfrowywania wiadomości oraz imienne maile służbowe oraz hasła własne odbiorców zgłoszeń są zabezpieczone przez osoby uprawnione po stronie podmiotu przyjmującego zgłoszenia.</p>
<p>W jaki sposób wykluczono możliwość identyfikacji sygnalisty poprzez mechanizmy śledzenia i profilowania? Np. systemy monitorujące stację roboczą? Śledzenie poprzez mechanizm <i>cookies</i>?</p>	<p>Nie ma możliwości identyfikacji sygnalisty poprzez mechanizmy śledzenia i profilowania pod warunkiem, że sygnalista nie korzysta z urządzeń firmowych udostępnionych przez pracodawcę. Platforma SYGNALISTA24.info usuwa wszelkie metadane związane z pochodzeniem plików oraz dotyczące samej wiadomości (cookies). Ponadto wiadomość jest szyfrowana hybrydowo i przesyłana bezpiecznym kanałem zgłoszeniowym do podmiotu. Wiadomość jest sprawdzana pod kątem obecności złośliwego oprogramowania.</p>
<p>Czy system daje możliwość tworzenia przez osoby uprawnione do przyjmowania / rozpatrywania zgłoszeń notatek / historii zgłoszenia?</p> <p>Jeżeli tak, to jak jest zapewniony wymóg poprawności i minimalizacji, a także ograniczenia przechowywania?</p>	<p>Tak. System daje możliwość tworzenia notatek przez osoby uprawnione do przyjmowania / rozpatrywania zgłoszeń oraz generowania historii danego zgłoszenia w formacie pdf zabezpieczonego nadanym hasłem.</p> <p>Odbiorca zgłoszenia ma dostęp do historii zgłoszenia:</p> <ul style="list-style-type: none"> <li>● usuniętego – przez 12 miesięcy po usunięciu,</li> <li>● zakończonego i zarchiwizowanego – przez minimum 3 lata po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami, chyba że przepisy stanowią inaczej.</li> </ul>



Pytanie	Odpowiedź
	Wygenerowany dokument podpisany cyfrowo, potwierdzający tym samym autentyczność pochodzenia.
Czy wdrożono dwuskładnikową (wieloskładnikową) autoryzację na poziomie osób uprawnionych do treści zgłoszenia?	<p>Tak. Jest to hasło oraz imienny mail. Dodatkowo kod autoryzacyjny przychodzi na wskazany mail. Każda wiadomość jest szyfrowana i dostępna dla odbiorcy oraz sygnalisty po odcodowaniu indywidualnymi poświadczeniami. Dla bezpieczeństwa czas trwania jednej sesji ograniczony jest do 10 minut, którą można przedłużyć.</p> <p>Hasło może być zmieniane przez obiorców zgłoszeń. Zmiana hasła odbiorcy zgłoszeń jest możliwa przy pomocy głównego odbiorcy zgłoszeń, który ponadto może dodać lub usunąć użytkownika.</p>
<p>Czy system daje możliwość <i>uploadu</i> treści? Np. przesłania skanu dokumentu?</p> <ul style="list-style-type: none"> <li>• jeżeli tak, to jak ten plik jest zabezpieczony?</li> <li>• jaki jest możliwy format pliku?</li> <li>• czy jest skanowany pod kątem złośliwego oprogramowania?</li> </ul>	<p>Tak. Platforma umożliwia wysyłanie załączników w następujących formatach: .pdf,.xls,.xlsx,.doc,.docx,.ods,.odt,.jpg,.bmp,.png,.txt.</p> <p>Z załączników usuwane są wszelkie metadane.</p> <p>Cała wiadomość wraz z załącznikami sprawdzana jest pod kątem obecności złośliwego oprogramowania.</p>
W jaki sposób i po jakim czasie usuwane są dane sygnalisty/ samego zgłoszenia?	<p>Decyzja co do statusu zgłoszenia należy do podmiotu. Osoby upoważnione do obsługi zgłoszeń decydują, czy zgłoszenie jest zamknięte, usunięte itd.</p> <p>Zgłoszenia zamknięte i zarchiwizowane – przechowywane przez 3 lata po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami, chyba że przepisy stanowią inaczej.</p> <p>Zgłoszenia usunięte – przechowywane do 12 miesięcy od momentu ich usunięcia.</p>
Czy system umożliwia prowadzenie rejestru zgłoszeń?	Tak. System umożliwia prowadzenie rejestru zgłoszeń, który jest zgodny z wymaganiami zawartymi w przepisach krajowych. Zestawienie naruszeń zawiera wszystkie niezbędne elementy, z możliwością pobrania w formacie pdf, z podpisem cyfrowym potwierdzającym autentyczność pochodzenia.

Pytanie	Odpowiedź
Czy system umożliwia przygotowanie sprawozdania rocznego dla Rzecznika Praw Obywatelskich?	Tak. System umożliwia przygotowanie sprawozdania rocznego dla Rzecznika Praw Obywatelskich zgodnie z wymaganiami zawartymi w przepisach krajowych, z możliwością pobrania w formacie pdf.
W jaki sposób system jest aktualizowany ( <i>update/upgrade/patche</i> )?	Platforma jest aktualizowana podczas wyznaczonych przerw technicznych, o których użytkownicy systemu informowani są z wyprzedzeniem.
Czy stosowane jest szyfrowanie/pseudonimizacja? Jakie metody szyfrowania (komunikacji / przechowywanych danych)? Kto i jak zabezpiecza klucze deszyfrujące?	Platforma zgłoszeniowa każdą wiadomość wraz z ewentualną tożsamością szyfruje metodą hybrydową. Więcej na dedykowanej stronie internetowej serwisu SYGNALISTA24.info.  Klucze deszyfrujące są szyfrowane algorytmem symetrycznym AES 256.
Gdzie dane są przechowywane? Czy dochodzi do powierzenia przetwarzania danych? Jeżeli tak, to według jakich zasad? Do jakich danych ma dostęp procesor? Czy zawarto umowę powierzenia? Jakie zabezpieczenia wdrożył procesor? Czy dochodzi do transferu danych?	Dane są przechowywane w odpowiednio zabezpieczonej serwerowni w Toruniu, EXEA Data Center sp. z o.o. Miejsce przechowywania danych potwierdzone jest stosownymi certyfikatami. Dostępne są one na stronie <a href="https://sygnalista24.info/">https://sygnalista24.info/</a> .  Nie dochodzi do powierzenia przetwarzania danych i transferu danych do państw spoza EOG. Dane są dostępne wyłącznie dla podmiotu, którego sygnalista wybrał jako adresata zgłoszenia. Właściciel platformy SYGNALISTA24.info nie ma dostępu do korespondencji pomiędzy sygnalistą a odbiorcą.

## V. Postanowienia końcowe

1. Dostęp do obsługi zgłoszeń mają tylko osoby upoważnione do przyjmowania zgłoszeń i wykonywania działań następczych, w tym do komunikacji z sygnalistą.
2. Osoby zajmujące się obsługą zgłoszeń zobowiązane są do wykonywania wszelkich działań związanych ze zgłoszeniem z należytą starannością, zachowaniem w tajemnicy przetwarzanych informacji oraz bezstronnością, a także z zachowaniem poszanowania godności i dobrego imienia sygnalisty i osób, których dotyczy zgłoszenie.