SYGNALISTA24.info

Szanowni Państwo,

Poniżej zamieszczamy odpowiedzi na pytania dot. elektronicznych kanałów dokonywania zgłoszeń przez sygnalistów, zaproponowanych przez Wolters Kluwer Polska na stronie LEX, pod adresem: https://www.lex.pl/

Lista kontrolna dotycząca elektronicznych kanałów dokonywania zgłoszeń przez sygnalistów

Pytania ogólne	Odpowiedzi
W jaki sposób będzie następować zgłoszenie? Np. formularz dostępny na www?	Formularz dostępny jest na platformie zgłoszeniowej SYGNALISTA24.info umieszczonej pod adresem https://app.sygnalista24.info/ Formularz zawiera opis naruszenia, termin i lokalizację wystąpienia naruszenia. Formularz umożliwia wysłanie dokumentów/załączników w następujących formatach: .pdf,.xls,.xlsx,.doc,.docx,.ods,.odt,.jpg,.bmp,.png,.txt.
Czy system będzie dawał możliwość wyświetlenia klauzuli informacyjnej (RODO) na formularzu zgłoszenia? W jaki sposób będzie potwierdzane zrealizowanie obowiązku informacyjnego?	Tak. Podmiot umieszcza klauzulę informacyjną w postaci pliku pdf na platformie we wskazanym miejscu, widocznym dla sygnalisty. Treść zamieszczonej klauzuli informacyjnej jest dostępna dla sygnalisty. Sygnalista przed wysłaniem naruszenia obowiązkowo potwierdza znajomość klauzuli informacyjnej podmiotu.
Jakie pola zawierać będzie formularz zgłoszenia? Czy tylko pole "treść zgłoszenia"?	Nie. Obok samej treści zgłoszenia sygnalista może załączyć do zgłoszenia dowody w postaci plików w ww. formacie. W formularzu są również inne pola, np. miejsce i czas zdarzenia/naruszenia.
Czy zgłoszenia będą realizowane wyłącznie anonimowo (Uwaga! Należy uwzględnić treść przepisów krajowych regulujących kwestię anonimowości zgłoszeń.)?	Aplikacja umożliwia obsługę zgłoszeń jawnych i anonimowych. Przy wykorzystaniu aplikacji kontakt z sygnalistą jest możliwy bez potrzeby wykorzystywania jego danych osobowych i kontaktowych. To od sygnalisty będzie zależało, czy będzie chciał ujawnić swoją tożsamość. Zależy to również od wewnętrznych regulaminów, które dopuszczą lub nie przyjmowanie zgłoszeń anonimowych. Ze względu na dopuszczenie w projekcie ustawy o ochronie sygnalistów fakultatywnego przyjmowania zgłoszeń anonimowych aplikacja SYGNALISTA24.info będzie informowała o tym, że dany podmiot będzie przyjmował lub nie zgłoszenia anonimowe (indywidualne ustawienia pierwszego okna podmiotu, z informacją dla sygnalisty).
Czy system zapewni możliwość przesłania/ przekazania/ pobrania potwierdzenia zgłoszenia? Czy i w jaki sposób zabezpieczona będzie treść (plik) z potwierdzeniem zgłoszenia?	Tak. Sygnalista otrzymuje potwierdzenie dokonania zgłoszenia. Może go również pobrać w formacie pdf i zapisać z użyciem własnego hasła (wymóg systemu) lub wydrukować. Również odbiorca zgłoszenia ma możliwość wygenerowania do pliku pdf raportu dotyczącego konkretnego zgłoszenia. Plik zabezpiecza nadanym przez siebie hasłem. Może go również wydrukować.

SYGNALISTA24.info

Czy system służy wyłącznie zgłoszeniu naruszenia czy umożliwia także prowadzenie dalszej korespondencji? Jeżeli tak to: • w jaki sposób sygnalista będzie logował się do systemu? • jak zapewniono bezpieczeństwo danych do logowania? • jak zapewniono anonimowość sygnalisty? • kiedy i na jakich zasadach będzie blokowany dostęp sygnalisty do treści zgłoszenia (np. brak możliwości zalogowania się po X czasu)?	Tak. Korespondencja między sygnalistą a podmiotem może być prowadzona w sposób ciągły. Po przesłaniu informacji przez sygnalistę podmiot otrzymuje powiadomienie za pomocą wskazanego adresu email, informującego o tym, że na platformie znajduje się wiadomość do odszyfrowania i odczytania. Dostęp odbiorcy do platformy możliwy po zalogowaniu indywidualnymi poświadczeniami. Sygnalista nie otrzymuje powiadomień. Każdorazowo będzie logować się na platformie za pomocą dwóch, generowanych automatycznie w momencie zgłoszenia naruszenia, kluczy: nr sprawy i hasło. Bez nich nie będzie miał możliwości odczytania wiadomości od podmiotu. Bezpieczeństwo logowania jest zapewnione przez konieczność wejścia do platformy i użycia wygenerowanych przez system: numeru zgłoszenia i klucza dostępowego. Można go zanotować lub zapisać w formacie pdf na komputerze wyłącznie przy użyciu hasła (wymóg systemu) lub wydrukować. Bezpieczeństwo sygnaliście zapewniamy przez: każdorazowe logowanie się za pomocą wygenerowanych podczas wysłania wiadomości kluczy. Każda wysłana wiadomość generuje inny, własny numer zgłoszenia i indywidualne hasło. Anonimowość sygnalisty zapewniamy również przez usuwanie metadanych i szyfrowanie całej korespondencji (wraz z załącznikami). Sygnalista ma dostęp do swojej wiadomości przez cały okres toczących się wyjaśnień i działań następczych. Zostanie powiadomiony na platformie o każdej czynności związanej z jego zgłoszeniem, a także jego zakończeniem, archiwizacją lub usunięciem. Może pobrać całą korespondencję w formacie pdf i wydrukować/zapisać używając własnego hasła. Dostęp sygnalisty do zgłoszenia blokowany jest po 12 miesiącach od zamknięcia sprawy.
W jaki sposób system zapewni poufność komunikacji i ograniczy dostęp do zgłoszenia do osób uprawnionych? • kto będzie nadawał dostępy? • jaki będzie zakres dostępu osób uprawnionych do dostępu do zgłoszenia? • kto będzie blokował dostęp? • kto i jak będzie definiował zakres uprawnień systemowych (np. przeglądanie spraw, tworzenie notatek)? • kto będzie mógł prowadzić komunikację z sygnalistą? • czy system wprowadza separacje uprawnień ze względu na role osób upoważnionych?	Nadajemy uprawnienia administratora osobie wskazanej i wymienionej w umowie z podmiotem zawartej na świadczone usługi. Administrator otrzyma narzędzie do zarejestrowania pozostałych użytkowników/odbiorców zgłoszeń. Będzie mógł nadawać i odbierać uprawnienia osobom upoważnionym przez podmiot. W przypadku zmiany administratora Usługodawca wygeneruje nowe uprawnienia dla nowego administratora wskazanego przez podmiot na piśmie. Administrator będzie miał możliwość blokować dostęp koordynatorom ze względu na lokalizację zgłoszenia. Usługodawca będzie blokować dostęp Administratorowi na wyraźne, pisemne życzenie podmiotu. Nadanie uprawnień dot. zgłoszenia, np. temat, poziom ważności i notatki dla sygnalisty będą wykonywane przez administratora i koordynatorów.

SYGNALISTA24.info

• czy system będzie logował: kto / kiedy / jakie dane wprowadził / zmodyfikował / usunął / pobrał po stronie rozpatrującej zgłoszenie? • jak i gdzie będą zabezpieczone dane do logowania przez osoby uprawnione po stronie organizacji przyjmującej zgłoszenia?	Każda wykonana ww. czynność będzie zarejestrowana pod kątem terminu jak i osoby dokonywającej zmiany systemowej czy odpowiedzi sygnaliście. Zarówno administrator jak i koordynator będzie mógł odpowiadać sygnaliście. • Tak. System wprowadza separacje uprawnień ze względu na role osób upoważnionych (administrator posiada większe uprawnienia). • Tak. System będzie odnotowywał każdą czynność przekazaną sygnaliście: kto / kiedy / jakie dane wprowadził / zmodyfikował / pobrał i przesłał. • Dane do logowania będą zabezpieczone przez osoby uprawnione po stronie podmiotu przyjmującej zgłoszenia. Do tego będzie służyć hasło firmowe, imienny mail służbowy oraz hasło własne administratora i koordynatora.
W jaki sposób wykluczono możliwość identyfikacji sygnalisty poprzez mechanizmy śledzenia i profilowania? Np. systemy monitorujące stację roboczą? Śledzenie poprzez mechanizm *cookies*?	Nie ma możliwości identyfikacji sygnalisty poprzez mechanizmy śledzenia i profilowania pod warunkiem, że sygnalista nie będzie korzystać z urządzeń firmowych. Nasza platforma 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.
Czy system daje możliwość tworzenia przez osoby uprawnione do przyjmowania / rozpatrywania zgłoszeń notatek / historii zgłoszenia? Jeżeli tak to jak zapewniono wymóg poprawności i minimalizacji a także ograniczenia przechowywania?	Tak. System daje możliwość tworzenia notatek przez osoby uprawnione do przyjmowania / rozpatrywania zgłoszeń oraz wygenerowania historii danego zgłoszenia w formacie pdf. Odbiorca zgłoszenia ma dostęp do historii zgłoszenia: • usuniętego – przez 12 miesięcy po usunięciu, • zakończonego i zarchiwizowanego – przez minimum 5 lat, chyba że przepisy ustanowią inaczej. Wygenerowany dokument będzie podpisany cyfrowo, potwierdzający tym samym autentyczność pochodzenia.
Czy wdrożono dwuskładnikową (wieloskładnikową) autoryzację na poziomie osób uprawnionych do dostępu do treści zgłoszenia?	Tak. Hasło oraz imienny mail. Dodatkowo każda wiadomość jest szyfrowana i dostępna dla odbiorcy/sygnalisty po odkodowaniu indywidualnymi poświadczeniami. Dla bezpieczeństwa jedna sesja ograniczona do 10 minut. Po tym czasie ponownie należy się zalogować. Hasło może być zmieniane przez administratora i koordynatorów. Zmiana hasła jest możliwa przy pomocy administratora, który ponadto może dodać lub usunąć użytkownika.
Czy system da możliwość *uploadu* treści? Np. przesłania skanu dokumentu? • jeżeli tak to jak ten plik będzie zabezpieczony? • jaki będzie format pliku? • czy będzie skanowany pod kątem złośliwego oprogramowania?	Tak. Aplikacja umożliwia wysłanie dokumentów/załączników w następujących formatach: .pdf,.xls,.xlsx,.doc,.docx,.ods,.odt,.jpg,.bmp,.png,.txt. Z załączników usuwane są wszelkie etadane. Cała wiadomość wraz z załącznikami sprawdzana jest pod kątem obecności złośliwego oprogramowania.

SYGNALISTA24.info

W jaki sposób i po jakim czasie usuwane będą dane sygnalisty/ samego zgłoszenia?	Decyzja co do statusu zgłoszenia należy do podmiotu. Osoby upoważnione decydują, czy zgłoszenie jest zamknięte, usunięte itd. Zgłoszenia zamknięte i zarchiwizowane - przechowywane do 5 lat, chyba że przepisy ustanowią inaczej. Zgłoszenia usunięte - przechowywane do 12 miesięcy od momentu usunięcia.
Czy system umożliwia prowadzenie rejestru zgłoszeń?	Tak. Zgodny z wymaganiami zawartymi w przepisach krajowych. Zestawienie naruszeń zawiera wszystkie niezbędne elementy, zarówno dla rejestru zgłoszeń w kanale wewnętrznym i rejestru zbiorczego w kanale zewnętrznym, z możliwością pobrania w formacie pdf., z podpisem cyfrowym potwierdzającym autentyczność pochodzenia.
W jaki sposób system będzie aktualizowany *(update/ upgrade/ patche)*?	Aplikacja będzie aktualizowana podczas wyznaczonych przerw technicznych.
Czy do rozwoju aplikacji używane będą zewnętrzne biblioteki? Np. *open source*?	Tak. Będą.
Czy w ramach rozwoju aplikacji wykorzystywane będą narzędzia telemetryczne/ diagnostyczne?	Tak. Będą.
Czy stosowane będzie szyfrowanie/ pseudonimizacja? Jakie metody szyfrowania (komunikacji / przechowywanych danych)? Kto i jak zabezpiecza klucze deszyfrujące?	Platforma zgłoszeniowa każdą wiadomość/naruszenie wraz z ewentualną tożsamością szyfruje metodą hybrydową. Więcej na dedykowanej stronie internetowej. 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? Czy zawarto umowę powierzenia? Jakie zabezpieczenia wdrożył procesor? Czy dochodzi do transferu danych?	Dane są przechowywane w odpowiednio zabezpieczonej serwerowni na terenie UE (miejsce Toruń). Miejsce przechowywania danych potwierdzone stosownymi certyfikatami. Dostępne na stronie https://sygnalista24.info/ Nie dochodzi do powierzenia przetwarzania danych i transferu danych. Dane są dostępne wyłącznie dla podmiotu (Usługobiorcy), do której sygnalista wysyła naruszenie. Usługodawca nie ma dostępu do korespondencji pomiędzy sygnalistą a odbiorcą.

W naszej ocenie lista pytań nie została wyczerpana.

W naszej ocenie elektroniczne kanały dokonywania zgłoszeń przez sygnalistów powinny m.in.:

- również umożliwić rejestrację innych zgłoszeń (np. podczas osobistych spotkań),
- być umiejscowione, ze względu na RODO, na terenie Europejskiego Obszaru Gospodarczego i nie korzystać z dostawców tego typu rozwiązań spoza UE,
- być przyjazne dla osób niepełnosprawnych i spełniać wymogi oraz kryteria wytycznych dla dostępności treści internetowej WCAG 2.1. AA, związane z ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

Z poważaniem
Marek Doering
Doering&Partnerzy