

Ochrona sygnalistów

23 lipca 2024



JURKIEWICZ
KAN C E L A R I A P R A W N A

Kancelaria Prawna Monika Jurkiewicz

Autor: radca prawny Monika Jurkiewicz

Sygnalista, czyli kto?

W definicji „sygnalisty” zawarto katalog zgłaszających.

Sygnalistą jest więc osoba fizyczna, która zgłasza lub ujawnia publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, w tym:

- 1) pracownik;
- 2) pracownik tymczasowy;
- 3) osoba świadcząca pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej;
- 4) przedsiębiorca;
- 5) prokurent;
- 6) akcjonariusz lub wspólnik;
- 7) członek organu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej;
- 8) osoba świadcząca pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy;
- 9) stażysta;
- 10) wolontariusz;
- 11) praktykant;
- 12) funkcjonariusz w rozumieniu art. 1 ust. 1 ustawy z dnia 18 lutego 1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin (Dz. U. z 2023 r. poz. 1280, 1429 i 1834);
- 13) żołnierz w rozumieniu art. 2 pkt 39 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2024 r. poz. 248 i 834).

Ustawę stosuje się także do osoby fizycznej, o której mowa wyżej w przypadku zgłoszenia lub ujawnienia publicznego informacji o naruszeniu prawa uzyskanej w kontekście związanym z pracą przed nawiązaniem stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji w podmiocie prawnym lub na rzecz tego podmiotu, lub pełnienia służby w podmiocie prawnym lub już po ich ustaniu.

Status sygnalisty będzie pochodną dokonania zgłoszenia wewnętrznego lub zgłoszenia zewnętrznego bądź ujawnienia publicznego na zasadach określonych w ustawie. Konieczne będzie zachowanie wymaganego trybu, tj. w szczególności dokonanie zgłoszenia z wykorzystaniem przewidzianych w tym zakresie kanałów zgłoszeń bądź zachowanie zasad ujawnienia publicznego. W każdym przypadku wymagane będzie dopełnienie przesłanek związanych z rzetelnością postępowania sygnalisty oraz wiarygodnością zgłaszanych lub ujawnianych przez niego informacji, w szczególności wymogu, że zgłaszający powinien mieć uzasadnione podstawy, aby sądzić, że będąca przedmiotem zgłoszenia informacja o naruszeniu jest prawdziwa w momencie dokonywania zgłoszenia. W przypadku zgłoszenia zewnętrznego lub wewnętrznego bezpośrednim uprawnieniem sygnalisty, wynikającym z samego dokonania zgłoszenia, będzie możliwość monitorowania toku sprawy, tj. uzyskania informacji zwrotnych dotyczących działań następczych, umożliwiających ocenę czy zgłoszenie spotkało się z właściwą reakcją. W przypadku zarówno zgłoszenia zewnętrznego lub wewnętrznego, jak i ujawnienia publicznego będą przysługiwać ponadto wynikające z ustawy środki ochrony.

„(2) Na poziomie Unii, dokonywane przez sygnalistów zgłoszenia i ujawnianie publiczne dotyczące naruszeń stanowią jeden z elementów oddolnego egzekwowania prawa i polityk Unii. Dostarczają one informacji na potrzeby krajowych i unijnych systemów egzekwowania prawa, umożliwiając skuteczne wykrywanie przypadków naruszenia prawa Unii, prowadzenie postępowań wyjaśniających w sprawie tych naruszeń oraz ich ścigania, tym samym zwiększając przejrzystość i rozliczalność.”

Od czego zacząć?

Wdrożenie mechanizmów związanych z procesem zgłaszania nieprawidłowości to działania wielopłaszczyznowe, wymagające dostosowania wewnętrznego organizacji je wprowadzającej.

1. Pierwszy obszar, który stanowi podwaliny whistleblowingu, to odpowiednio skonstruowana **polityka zgłaszania nieprawidłowości oraz procedura prowadzenia wewnętrznych postępowań wyjaśniających**.
2. Sposoby przekazywania zgłoszeń powinny zapewniać **ochronę poufności tożsamości osoby zgłaszającej oraz osób wymienionych w treści zgłoszenia**, a także uniemożliwiać dostęp do tych danych przez podmioty do tego nieupoważnione.
3. Kanały przekazywania zgłoszeń mogą stanowić, o ile spełniają wskazane powyżej przesłanki, dedykowany zgłoszeniom adres mailowy lub infolinia, dedykowana aplikacja przewidziana do przyjmowania zgłoszeń i kontaktu z sygnalistom, ewentualnie inne narzędzia jak np. fax lub skrzynka umieszczona w ogólnodostępnym dla pracowników miejscu nieobjętym monitoringiem.
4. Zgodnie z postanowieniami dyrektywy 2019/1937 podmiot wdrażający **system whistleblowingowy** zobowiązany jest do wyznaczenia bezstronnej osoby lub struktury, która będzie odpowiedzialna za przyjmowanie raportów od sygnalistów, prowadzenie wewnętrznych postępowań wyjaśniających oraz podejmowanie działań następczych, natomiast w uzasadnionych przypadkach będzie podejmować kontakt zwrotny do sygnalisty.
5. Kolejnym aspektem jest ten związany z **edukacją wewnętrzną oraz szkoleniami**. Dla skutecznego wdrożenia systemu zgłaszania nieprawidłowości niezbędne jest jasne przedstawienie jego celu w organizacji, zapoznanie pracowników z jego działaniem, przedstawienie mechanizmów ochrony osób zgłaszających, a także osób wskazanych w zgłoszeniu oraz narzędzi pozwalających na poufność całego procesu oraz zachowanie bezstronności osób odpowiedzialnych za obsługę zgłoszeń.
6. Bez przeprowadzonych kampanii komunikacyjnych zaznajamiających pracowników wszystkich szczebli z nowym rozwiązaniem wprowadzanym w organizacji oraz przedstawieniem jego istoty jako instrumentu wewnętrznego zabezpieczenia podmiotu przed nieprawidłowościami, pozwalającego na szybkie podjęcie kroków zaradczych w sytuacji wystąpienia nieprawidłowości, **nie będzie możliwe prawdziwie efektywne implementowanie whistleblowingu**.

Przedmiot zgłoszeń objęty regulacją.

Przechodząc do szczegółowych regulacji trzeba wskazać, iż zarówno dyrektywa 2019/1937, jak i projekt polskiej ustawy o ochronie osób zgłaszających nieprawidłowości dotyczy następujących zakresów:

Art. 3. 1. Naruszeniem prawa jest działanie lub zaniechanie niezgodne z prawem lub mające na celu obejście prawa dotyczące:

- 1) korupcji;
- 2) zamówień publicznych;
- 3) usług, produktów i rynków finansowych;
- 4) przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
- 5) bezpieczeństwa produktów i ich zgodności z wymogami;
- 6) bezpieczeństwa transportu;
- 7) ochrony środowiska;
- 8) ochrony radiologicznej i bezpieczeństwa jądrowego;
- 9) bezpieczeństwa żywności i pasz;
- 10) zdrowia i dobrostanu zwierząt;
- 11) zdrowia publicznego;
- 12) ochrony konsumentów;
- 13) ochrony prywatności i danych osobowych;
- 14) bezpieczeństwa sieci i systemów teleinformatycznych;
- 15) interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, jednostki samorządu terytorialnego oraz Unii Europejskiej;
- 16) rynku wewnętrznego Unii Europejskiej, w tym publicznoprawnych zasad konkurencji i pomocy państwa oraz opodatkowania osób prawnych;
- 17) konstytucyjnych wolności i praw człowieka i obywatela – występujące w stosunkach jednostki z organami władzy publicznej i niezwiązane z dziedzinami wskazanymi w pkt 1–17.

Podmiot prawny może dodatkowo w ramach procedury zgłoszeń wewnętrznych przewidzieć możliwość zgłaszania informacji o naruszeniach dotyczących obowiązujących w tym podmiocie prawnym regulacji wewnętrznych lub

standardów etycznych, które zostały ustanowione przez podmiot prawny na podstawie przepisów prawa powszechnie obowiązującego i pozostają z nimi zgodne.

Obowiązki przewidziane w projekcie ustawy o ochronie sygnalistów – Regulamin zgłoszeń wewnętrznych.

Zasady te stosuje się do podmiotu prawnego, na rzecz którego według stanu na dzień 1 stycznia lub 1 lipca danego roku wykonuje pracę zarobkową co najmniej 50 osób.

Do liczby 50 osób wykonujących pracę zarobkową na rzecz podmiotu prawnego wlicza się pracowników w przeliczeniu na pełne etaty lub osoby świadczące pracę za wynagrodzeniem na innej podstawie niż stosunek pracy, jeżeli nie zatrudniają do tego rodzaju pracy innych osób, niezależnie od podstawy zatrudnienia.

- 1) Pracodawca ustala regulamin zgłoszeń wewnętrznych, określający wewnętrzną procedurę zgłaszania naruszeń prawa i podejmowania działań następczych,
- 2) Regulamin zgłoszeń wewnętrznych pracodawca ustala po konsultacji z przedstawicielami pracowników, wyłonionymi w trybie przyjętym u danego pracodawcy – jeżeli u pracodawcy nie działa zakładowa organizacja związkowa.
- 3) Regulamin(wchodzi w życie w życie po upływie 2 tygodni od dnia podania go do wiadomości pracowników sposób przyjęty u danego pracodawcy).

Procedura zgłoszeń wewnętrznych określa w szczególności:

Procedura zgłoszeń wewnętrznych określa:

- 1) wewnętrzną jednostkę organizacyjną lub osobę w ramach struktury organizacyjnej podmiotu prawnego, lub podmiot zewnętrzny, upoważnione przez podmiot prawny do przyjmowania zgłoszeń wewnętrznych;

-
- 2) sposoby przekazywania zgłoszeń wewnętrznych przez sygnalistę wraz z jego adresem korespondencyjnym lub adresem poczty elektronicznej, zwanymi dalej „adresem do kontaktu”;
 - 3) bezstronną wewnętrzną jednostką organizacyjną lub osobę w ramach struktury organizacyjnej podmiotu prawnego, upoważnione do podejmowania działań następczych, włączając w to weryfikację zgłoszenia wewnętrznego i dalszą komunikację z sygnalistą, w tym występowanie o dodatkowe informacje i przekazywanie sygnaliście informacji zwrotnej; funkcję tę może pełnić wewnętrzna jednostka organizacyjna lub osoba, o których mowa w pkt 1, jeżeli zapewniają bezstronność;
 - 4) tryb postępowania z informacjami o naruszeniach prawa zgłoszonymi anonimowo;
 - 5) obowiązek potwierdzenia sygnaliście przyjęcia zgłoszenia wewnętrznego w terminie 7 dni od dnia jego otrzymania, chyba że sygnalista nie podał adresu do kontaktu, na który należy przekazać potwierdzenie;
 - 6) obowiązek podjęcia, z zachowaniem należytej staranności, działań następczych przez wewnętrzną jednostkę organizacyjną lub osobę, o których mowa w pkt 3;
 - 7) maksymalny termin na przekazanie sygnaliście informacji zwrotnej, nieprzekraczający 3 miesięcy od potwierdzenia przyjęcia zgłoszenia wewnętrznego lub – w przypadku nieprzekazania potwierdzenia, o którym mowa w pkt 5 – 3 miesięcy od upływu 7 dni od dnia dokonania zgłoszenia wewnętrznego, chyba że sygnalista nie podał adresu do kontaktu, na który należy przekazać informację zwrotną;
 - 8) zrozumiałe i łatwo dostępne informacje na temat dokonywania zgłoszeń zewnętrznych do Rzecznika Praw Obywatelskich albo organów publicznych oraz – w stosownych przypadkach – do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej.

Procedura MOŻE zawierać ponadto:

1. wskazanie naruszeń, o których mowa w art. 3 ust. 2 projektu ustawy, jeżeli podmiot prawny ustanowi zgłaszanie takich naruszeń,
2. wskazanie czynników ryzyka odpowiadających profilowi działalności podmiotu prawnego, sprzyjających możliwości wystąpienia określonych naruszeń prawa związanych w szczególności z naruszeniem obowiązków regulacyjnych lub innych obowiązków określonych w przepisach prawa lub z ryzykiem korupcji,
3. wskazanie, że informacja o naruszeniu prawa może być w każdym przypadku zgłoszona również do Rzecznika Praw Obywatelskich albo organu publicznego z pominięciem procedury zgłoszeń wewnętrznych,

-
- określenie systemu zachęt do korzystania z procedury zgłoszeń wewnętrznych, w przypadku, gdy naruszeniu prawa można skutecznie zaradzić w ramach struktury organizacyjnej podmiotu prawnego, a sygnalista uważa, że nie zachodzi ryzyko działań odwetowych.

Osobie ubiegającej się o wykonywanie pracy na podstawie stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji, lub pełnienia służby podmiot prawny przekazuje informację o procedurze zgłoszeń wewnętrznych wraz z rozpoczęciem rekrutacji lub negocjacji poprzedzających zawarcie umowy.

Pracodawca ponadto prowadzi rejestr zgłoszeń wewnętrznych i....

- Jest administratorem danych zgromadzonych w tym rejestrze.
- wpisu do rejestru zgłoszeń wewnętrznych dokonuje na podstawie zgłoszenia wewnętrznego.

W rejestrze zgłoszeń wewnętrznych gromadzi się następujące dane:

- Numer sprawy;
- Przedmiot naruszenia;
- Datę dokonania zgłoszenia wewnętrznego;
- Informację o podjętych działaniach następczych;
- Datę zakończenia sprawy.
- Dane w rejestrze zgłoszeń wewnętrznych są przechowane przez okres 5 lat od dnia przyjęcia zgłoszenia.

Podsumowując obowiązki pracodawców/podmiotów prawnych będą następujące:

- 1) obowiązek przyjmowania i rozpoznawania zgłoszeń naruszenia prawa w zakresach wymienionych w ustawie,
- 2) obowiązek ustanowienia procedury zgłoszeń wewnętrznych,
- 3) obowiązek przeprowadzenia konsultacji ze związkami zawodowymi lub przedstawicielami pracowników projektów procedury zgłoszeń wewnętrznych,
- 4) ustalenie wewnętrznej jednostki organizacyjnej lub osoby w ramach struktury organizacyjnej podmiotu prawnego, lub podmiot zewnętrzny, upoważnione przez podmiot prawny do przyjmowania zgłoszeń wewnętrznych (podmiotem zewnętrznym może być na przykład kancelaria prawna),
- 5) ustalenie bezstronnej wewnętrznej jednostki organizacyjnej lub osoby w ramach struktury organizacyjnej podmiotu prawnego, upoważnione do podejmowania działań następczych, włączając w to weryfikację zgłoszenia wewnętrznego i dalszą komunikację z sygnalistą, w tym występowanie o dodatkowe informacje i przekazywanie sygnaliście informacji zwrotnej,
- 6) udzielenie upoważnień dla osób, które mają przyjmować i weryfikować zgłoszenia oraz podejmować działania następcze,
- 7) obowiązek potwierdzania sygnaliście przyjęcia zgłoszenia wewnętrznego w terminie 7 dni od dnia jego otrzymania, chyba że sygnalista nie poda adresu do kontaktu, na który należy przekazać potwierdzenie,
- 8) obowiązek ustanowienia kanałów zgłoszeń,
- 9) obowiązek podejmowania, z zachowaniem należytej staranności, działań następczych przez wewnętrzną jednostkę organizacyjną lub osobę, o których mowa wyżej,
- 10) obowiązek przygotowania zrozumiałych i łatwo dostępnych informacji na temat dokonywania zgłoszeń zewnętrznych do Rzecznika Praw Obywatelskich albo organów publicznych oraz – w stosownych przypadkach – do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej,
- 11) obowiązek zagwarantowania, że procedura zgłoszeń wewnętrznych oraz związane z przyjmowaniem zgłoszeń przetwarzanie danych osobowych uniemożliwiają nieupoważnionym osobom uzyskanie dostępu do informacji objętych zgłoszeniem oraz zapewniają ochronę poufności tożsamości sygnalisty, osoby, której dotyczy zgłoszenie, oraz osoby trzeciej wskazanej w zgłoszeniu,
- 12) obowiązek prowadzenia rejestru zgłoszeń (taki rejestr może prowadzić zewnętrzna kancelaria prawna).

Instrumenty ochrony sygnalisty

ŚRODEK OCHRONY	PODSTAWA PRAWNA	DEFINICJA
Zakaz działań odwetowych	Art. 2 pkt 2) oraz 11 - 13. ustawy	bezpośrednie lub pośrednie działanie lub zaniechanie w kontekście związanym z pracą, które jest spowodowane zgłoszeniem lub ujawnieniem publicznym i które narusza lub może naruszyć prawa sygnalisty lub wyrządza lub może wyrządzić nieuzasadnioną szkodę sygnaliście, w tym niezasadne inicjowanie postępowań przeciwko sygnaliście
Roszczenia	Art. 14 - 15 ustawy	<p>Art. 14. Sygnalista, wobec którego dopuszczono się działań odwetowych, ma prawo do odszkodowania w wysokości nie niższej niż przeciętne miesięczne wynagrodzenie w gospodarce narodowej w poprzednim roku, ogłaszane do celów emerytalnych w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” przez Prezesa Głównego Urzędu Statystycznego, lub prawo do zadośćuczynienia.</p> <p>Art. 15. Osoba, która poniosła szkodę z powodu świadomego zgłoszenia lub ujawnienia publicznego nieprawdziwych informacji przez sygnalistę, ma prawo do odszkodowania lub zadośćuczynienia za naruszenie dóbr osobistych od sygnalisty, który dokonał takiego zgłoszenia lub ujawnienia publicznego.</p>
Zakazy postępowań dyscyplinarnych i dochodzenia odszkodowań	Art. 16 ustawy	<i>Art. 16. 1. Dokonanie zgłoszenia lub ujawnienia publicznego nie może stanowić podstawy odpowiedzialności, w tym odpowiedzialności dyscyplinarnej lub odpowiedzialności za szkodę z tytułu naruszenia praw innych osób lub obowiązków określonych w przepisach prawa, w szczególności w przedmiocie zniestawienia, naruszenia dóbr osobistych, praw autorskich, przepisów o ochronie danych osobowych oraz obowiązku zachowania tajemnicy, w tym tajemnicy przedsiębiorstwa, z zastrzeżeniem art. 5, pod warunkiem że sygnalista miał uzasadnione podstawy sądzić, że zgłoszenie lub</i>

		<p><i>ujawnienie publiczne jest niezbędne do ujawnienia naruszenia prawa zgodnie z ustawą.</i></p> <p><i>2. W przypadku wszczęcia postępowania prawnego dotyczącego odpowiedzialności, o której mowa w ust. 1, sygnalista może wystąpić o umorzenie takiego postępowania.</i></p> <p><i>3. Uzyskanie informacji będących przedmiotem zgłoszenia lub ujawnienia publicznego lub dostęp do takich informacji nie mogą stanowić podstawy odpowiedzialności, pod warunkiem że takie uzyskanie lub taki dostęp nie stanowią czynu zabronionego.</i></p>
<p>Inne zakazy (kontrahenci lub odmowa przyznania praw)</p>	<p>Art. 13 ustawy</p>	<p><i>Art. 13. 1. Jeżeli praca lub usługa były, są lub mają być świadczone na podstawie innego niż stosunek pracy stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji, lub pełnienia służby, przepis art. 12 stosuje się odpowiednio, o ile charakter świadczonej pracy lub usługi lub pełnionej funkcji, lub pełnionej służby nie wyklucza zastosowania wobec sygnalisty takiego działania.</i></p> <p><i>2. Jeżeli praca lub usługa były, są lub mają być świadczone na podstawie innego niż stosunek pracy stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji, lub pełnienia służby, dokonanie zgłoszenia lub ujawnienia publicznego nie może stanowić podstawy działań odwetowych ani próby lub groźby zastosowania działań odwetowych, obejmujących w szczególności:</i></p> <ol style="list-style-type: none"> <i>1) wypowiedzenie umowy, której stroną jest sygnalista, w szczególności dotyczącej sprzedaży lub dostawy towarów lub świadczenia usług, odstąpienie od takiej umowy lub rozwiązanie jej bez wypowiedzenia;</i> <i>2) nałożenie obowiązku lub odmowę przyznania, ograniczenie lub odebranie uprawnienia, w szczególności koncesji, zezwolenia lub ulgi.</i>

Kwestie RODO

Pamiętaj o regulacjach w ustawie dotyczące:



Ochrony tożsamości osób dokonujących zgłoszenia



Realizacji obowiązku informacyjnego z art. 14 RODO oraz prawa dostępu z art. 15 RODO

Art. 8.

- 1. Dane osobowe sygnalisty, pozwalające na ustalenie jego tożsamości, nie podlegają ujawnieniu nieupoważnionym osobom, chyba że za wyraźną zgodą sygnalisty.*
- 2. Przepisu ust. 1 nie stosuje się w przypadku, gdy ujawnienie jest koniecznym i proporcjonalnym obowiązkiem wynikającym z przepisów prawa w związku z postępowaniami wyjaśniającymi prowadzonymi przez organy publiczne lub postępowaniami przygotowawczymi lub sądowymi prowadzonymi przez sądy, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy zgłoszenie.*
- 3. Przed dokonaniem ujawnienia, o którym mowa w ust. 2, właściwy organ publiczny lub właściwy sąd powiadamia o tym sygnalistę, przesyłając w postaci papierowej lub elektronicznej wyjaśnienie powodów ujawnienia jego danych osobowych, chyba że takie powiadomienie zagrozi postępowaniu wyjaśniającemu lub postępowaniu przygotowawczemu, lub sądowemu.*
- 4. Podmiot prawny albo organ publiczny po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.*
- 5. Przepisu art. 14 ust. 2 lit. f rozporządzenia 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, z późn. zm.)), zwanego dalej „rozporządzeniem 2016/679”, nie stosuje się, chyba że sygnalista nie spełnia warunków wskazanych w art. 6 albo wyraził wyraźną zgodę na ujawnienie swojej tożsamości.*

-
6. Przepisu art. 15 ust. 1 lit. g rozporządzenia 2016/679 w zakresie przekazania informacji o źródle pozyskania danych osobowych nie stosuje się, chyba że sygnalista nie spełnia warunków wskazanych w art. 6 albo wyraził wyraźną zgodę na takie przekazanie.
 7. Dane osobowe przetwarzane w związku z przyjęciem zgłoszenia zewnętrznego oraz dokumenty związane z tym zgłoszeniem są przechowywane przez Rzecznika Praw Obywatelskich przez okres 12 miesięcy po zakończeniu roku kalendarzowego, w którym przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następczych.
 8. 8. Dane osobowe przetwarzane w związku z przyjęciem zgłoszenia lub podjęciem działań następczych oraz dokumenty związane z tym zgłoszeniem są przechowywane przez podmiot prawny oraz organ publiczny przez okres 3 lat po zakończeniu roku kalendarzowego, w którym przekazano zgłoszenie wewnętrzne do organu publicznego właściwego do podjęcia działań następczych lub zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.
 9. 9. W przypadku, o którym mowa w ust. 7 i 8, Rzecznik Praw Obywatelskich, podmiot prawny i organ publiczny usuwają dane osobowe oraz niszczą dokumenty związane ze zgłoszeniem po upływie okresu przechowywania. Przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164) nie stosuje się.
 10. 10. Przepisu ust. 9 nie stosuje się w przypadku, gdy dokumenty związane ze zgłoszeniem stanowią część akt postępowań przygotowawczych lub spraw sądowych lub sądo-administracyjnych.

Ponadto w zakresie zgłoszeń wewnętrznych:

Art. 27.

1. Podmiot prawny gwarantuje, że procedura zgłoszeń wewnętrznych oraz związane z przyjmowaniem zgłoszeń przetwarzanie danych osobowych uniemożliwiają nieupoważnionym osobom uzyskanie dostępu do informacji objętych zgłoszeniem oraz zapewniają ochronę poufności tożsamości sygnalisty, osoby, której dotyczy zgłoszenie, oraz osoby trzeciej wskazanej w zgłoszeniu. Ochrona poufności dotyczy informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość takich osób.
2. Do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych oraz przetwarzania danych osobowych osób, o których mowa w ust. 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie podmiotu prawnego. Osoby upoważnione są obowiązane do zachowania tajemnicy w zakresie informacji i danych osobowych, które uzyskały w ramach przyjmowania i weryfikacji zgłoszeń wewnętrznych, oraz podejmowanych działań następczych, także po ustaniu stosunku pracy lub innego stosunku prawnego, w ramach którego wykonywały tę pracę.

Zgłoszenia tylko uzasadnione

Zgłoszenia sygnalistów będą dotyczyć informacji o naruszeniu prawa – należy przez to rozumieć informację, w tym uzasadnione podejrzenie dotyczące zaistniałego lub potencjalnego naruszenia prawa, do którego doszło lub prawdopodobnie dojdzie w podmiocie prawnym, w którym sygnalista uczestniczył w procesie rekrutacji lub innych negocjacji poprzedzających zawarcie umowy, pracuje lub pracował, lub w innym podmiocie prawnym, z którym sygnalista utrzymuje lub utrzymywał kontakt w kontekście związanym z pracą, lub informację dotyczącą próby ukrycia takiego naruszenia prawa.

Ważne !


Sygnalista podlega ochronie określonej w przepisach rozdziału 2 od chwili dokonania zgłoszenia lub ujawnienia publicznego, pod warunkiem, że miał **uzasadnione podstawy** sądzić, że informacja będąca przedmiotem zgłoszenia lub ujawnienia publicznego jest prawdziwa w momencie dokonywania zgłoszenia lub ujawnienia publicznego i że stanowi informację o naruszeniu prawa.

Termin wdrożenia

Ustawa wejdzie w życie 24 września 2024 r. Oznacza to, że wdrożenie powinno się zacząć już teraz, aby na 25 września dokumentacja była gotowa, aby móc rozpocząć konsultacje ze związkami zawodowymi czy innym przedstawicielstwem załogi.

Sugerujemy rozpocząć pracę na wdrożeniem już teraz, ponieważ zmian w procedurach będzie dużo.

Plan wdrożenia



PLAN WDROŻENIA:

1. Audyt stanu dokumentacji koniecznej do wdrożenia procedury ochrony sygnalistów.
2. Przygotowanie dokumentacji - procedur i struktury funkcjonowania systemu ochrony sygnalistów w organizacji.
3. Opracowanie dokumentacji dla kanałów zgłoszeń.
4. Opracowanie „komunikacji” systemu ochrony (informacje dla pracowników, wyciągi z dokumentacji, plakaty).
5. Modyfikacja dokumentacji ochrony danych oraz AML w związku z wdrożeniem.
6. Przeszkolenie personelu.
7. Audyt kończący – wnioski, zalecenia.

2

Jakie dokumenty obowiązujące w organizacji należy poddać analizie w ramach wdrożenia,

są to w szczególności.....



NIEZBĘDNE ZASOBY

Dokumentacja niezbędna do Audytu:

1. Polityka ochrony danych osobowych (o ile stworzona);
2. Regulaminy Organizacyjne / Funkcjonowania Przedsiębiorcy;
3. Polityka Antykorupcyjna (o ile stworzona);
4. Procedura AML;
5. Polityki Antydyskryminacyjne i Antymobbingowe;
6. Regulamin Pracy, Wynagrodzenia, Premiowania;
7. Regulacje dotyczące pracy zdalnej;
8. Regulaminy Zarządu, Rady Nadzorczej;
9. Procedury wynikające z odpowiednio wdrożonych norm ISO;
10. Rejestr czynności przetwarzania (RODO);
11. Zakresy obowiązków personelu administracyjnego;
12. Dokumentacja jakości w zakresie cyberbezpieczeństwa;
13. Wykaz stosowanych oprogramowań.

3

Czy obsługa procesu zgłoszeń oraz tzw. Działań następczych może być powierzona podmiotowi zewnętrznemu?

Ustawodawca wręcz to sugeruje wskazując, że pracodawca ma powołać:

niezależny organizacyjnie podmiot, upoważniony do podejmowania działań następczych, włączając w to weryfikację zgłoszenia i dalszą komunikację ze zgłaszającym, w tym występowanie o dodatkowe informacje i przekazywanie zgłaszającemu informacji zwrotnej.

Rolę tę może też pełnić podmiot wewnętrzny upoważniony przez pracodawcę do przyjmowania zgłoszeń, o ile spełni przesłanki i kryteria bezstronności oraz należytej staranności w prowadzeniu działań następczych w wyniku przyjętego zgłoszenia, co w praktyce będzie trudne do osiągnięcia.

Zmiany muszą między innymi dotyczyć następujących zasobów wewnętrznych:

- Procedury rekrutacji,
- Procedury onboardingu pracownika,
- Procedury dotyczącą awansów i ścieżek kariery pracownika,
- Procedury przeciwdziałania dyskryminacji i Mobbingowi,
- Procedury rozwiązywania umów o pracę lub/i innych stosunków na podstawie, których sygnalista może wykonywać czynności,
- Ocen okresowych.
- Procedury ochrony informacji (szerzej niż RODO),
- Procedury ochrony danych osobowych,
- Procedury jakościowe dla produktów i usług,
- Procedury obiegu dokumentacji oraz informacji,
- Procedury nadzoru nad decyzjami finansowymi.

Jeśli chcesz dowiedzieć się dokładnie jak wdrożyć system ochrony sygnalistów.

SKONTAKTUJ SIĘ Z NAMI !

biuro@kancelaria-Jurkiewicz.pl mob: 607942 031

9

Oferujemy rozliczenia w trzech elastycznych Pakietach, a także istnieje możliwość dopasowania Pakietu indywidualnie.

Oto nasze propozycje:



Pakiet I

Obejmujący:

1. identyfikację wszystkich procedur obowiązujących w przedsiębiorstwie, które wymagają zmiany w związku z wdrożeniem oraz dokonanie niezbędnych zmian,
2. przedstawienie możliwych do wdrożenia kanałów zgłoszeń oraz wsparcie w wyborze odpowiednich dla państwa przedsiębiorstwa, kanałów sygnalizacyjnych,

-
3. lista kontrolna wyboru kanału zgłoszeń,
 4. opracowanie procedury zgłoszeń wewnętrznych,
 5. opracowanie dokumentacji wykonawczej do procedury zgłoszeń wewnętrznych, w tym wzorów formularzy, schematów postępowania, standardowych odpowiedzi w związku ze zgłoszeniem, rejestru zgłoszeń.
 6. asysta prawna w konsultacjach z ZZ lub innym przedstawicielstwem załogi,
 7. opracowanie i wdrożenie w istniejących procedurach ochrony danych osobowych zmian wynikających wdrożenia systemu ochrony sygnalistów,
 8. opracowanie standardów dla działań następczych,
 9. opracowania standardów związanych z identyfikacją oraz prewencją działań odwetowych związanych z ochroną sygnalistów,
 10. stworzenie karty opisu procesów lub/i zmian do takich kart w związku z wdrożeniem,
 11. wsparcie w dostosowaniu procedury oraz dokumentacji do systemów ochrony informacji jak ISO 27001, czy TISAX.
 12. wsparcie w wyborze bezstronnej jednostki, która będzie podejmować działania następcze,
 13. wsparcie we wdrożeniu standardów postępowania wyjaśniających w ramach systemu ochrony sygnalistów,
 14. opracowanie planu komunikacji, w tym infografik związanych z wdrożeniem,
 15. przeprowadzenie szkoleń:
 - 1) dla kadry menedżerskiej,
 - 2) dla osób zaangażowanych w system przyjmowania i obsługi zgłoszeń,
 - 3) szkoleń dla wszystkich osób, które będą mogły dokonywać zgłoszeń i korzystać ze statusu sygnalisty.

Koszt takiego wdrożenia to kwota od 10 000 zł netto.

Termin realizacji: 1 miesiąc (30 dni) od daty podpisania umowy i dostarczenia przez Klienta wszystkich wymaganych dokumentów.

Sposób komunikacji zdalnie.

Ostatnie spotkanie statusowe i podsumowanie projektu - w siedzibie klienta.

Szkolenia - mogą być przeprowadzone bądź zdalnie bądź stacjonarnie. W przypadku szkoleń stacjonarnych do kosztu należy doliczyć koszty przejazdu według tak zwanej kilometrówki oraz koszt noclegu w wysokości 500 zł za osobę.



Pakiet II

Obejmujący:

1. identyfikację wszystkich procedur obowiązujących w przedsiębiorstwie, które wymagają zmiany w związku z wdrożeniem oraz dokonanie niezbędnych zmian,
2. przedstawienie możliwych do wdrożenia kanałów zgłoszeń oraz wsparcie w wyborze odpowiednich dla państwa przedsiębiorstwa, kanałów sygnalizacyjnych,
3. opracowanie procedury zgłoszeń wewnętrznych,
4. opracowanie dokumentacji wykonawczej do procedury zgłoszeń wewnętrznych, w tym wzorów formularzy, schematów postępowania, standardowych odpowiedzi w związku ze zgłoszeniem, rejestru zgłoszeń,
5. asysta prawna w konsultacjach z ZZ lub innym przedstawicielstwem załogi,
6. opracowanie i wdrożenie w istniejących procedurach ochrony danych osobowych zmian wynikających z wdrożenia systemu ochrony sygnalistów,
7. wsparcie w wyborze bezstronnej jednostki, która będzie podejmować działania następcze,
8. wsparcie we wdrożeniu standardów postępowania wyjaśniających w ramach systemu ochrony sygnalistów,
9. przeprowadzenie szkoleń:
 - a. dla kadry menedżerskiej,
 - b. dla osób zaangażowanych w system przyjmowania i obsługi zgłoszeń.

Koszt takiego wdrożenia to kwota: od 5000 zł netto.

Termin realizacji: 1 miesiąc (30 dni) od daty podpisania umowy i dostarczenia przez Klienta wszystkich wymaganych dokumentów.

Sposób komunikacji zdalnie.

Ostatnie spotkanie statusowe i podsumowanie projektu - w siedzibie klienta.

Szkolenia - mogą być przeprowadzone bądź zdalnie bądź stacjonarnie. W przypadku szkoleń stacjonarnych do kosztu należy doliczyć koszty przejazdu według tak zwanej kilometrówki oraz koszt noclegu w wysokości 500 zł za osobę.



Pakiet III

Obejmujący:

1. przedstawienie możliwych do wdrożenia kanałów zgłoszeń oraz wsparcie w wyborze odpowiednich dla państwa przedsiębiorstwa, kanałów sygnalizacyjnych,
2. opracowanie procedury zgłoszeń wewnętrznych,
3. opracowanie dokumentacji wykonawczej do procedury zgłoszeń wewnętrznych, w tym wzorów formularzy, schematów postępowania, standardowych odpowiedzi w związku ze zgłoszeniem, rejestru zgłoszeń,
4. wsparcie w wyborze bezstronnej jednostki, która będzie podejmować działania następcze,
5. przeprowadzenie szkoleń:
 - a. dla osób zaangażowanych w system przyjmowania i obsługi zgłoszeń.

Koszt takiego wdrożenia to kwota: od 3500 zł netto.

Termin realizacji: 1 miesiąc (30 dni) od daty podpisania umowy i dostarczenia przez Klienta wszystkich wymaganych dokumentów.

Sposób komunikacji zdalnie.

Ostatnie spotkanie statusowe i podsumowanie projektu - w siedzibie klienta.

Szkolenia - mogą być przeprowadzone bądź zdalnie bądź stacjonarnie. W przypadku szkoleń stacjonarnych do kosztu należy doliczyć koszty przejazdu według tak zwanej kilometrówki oraz koszt noclegu w wysokości 500 zł za osobę.

Zapraszamy do współpracy



Monika Jurkiewicz

Radca prawny



JURKIEWICZ