

Ochrona sygnalistów w sektorze publicznym + wzory do pobrania

Przejdź do produktu na ksiegarnia.beck.pl

Urszula Góral

Rozdział I. System ochrony sygnalistów w sektorze publicznym z perspektywy europejskiej

1. Uwagi wstępne

Unijna dyrektywa 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii wprowadza zasady, zgodnie z którymi państwa członkowskie mają zapewnić funkcjonowanie skutecznych kanałów poufnego zgłaszania naruszeń prawa przez sygnalistów. System zgłaszania naruszeń ma zastosowanie do sektora publicznego i prywatnego, poprzez kanały zarówno wewnętrzne (w organizacji), jak i zewnętrzne (zgłaszanie właściwemu organowi publicznemu).

Unijny prawodawca stworzył jednocześnie podstawy prawne do utworzenia solidnego systemu ochrony sygnalistów przed działaniami odwetowymi. W poniższym rozdziale skupimy się na **budowaniu unijnych reguł ochrony sygnalistów i systemów zgłaszania nieprawidłowości – opisując je w kontekście osiągnięć Rady Europy** w tym obszarze. Analiza działań instytucji pozwoli na sformułowanie wyjaśnień, dlaczego nie udało się osiągnąć skutecznych form walki z naruszeniami i nieprawidłowościami na poziomie krajowym i niezbędna była interwencja unijnego prawodawcy w tym zakresie.

Debata na temat utworzenia narzędzia, które w sposób najbardziej efektywny będzie działało w obronie interesu publicznego, toczyła się przez wiele lat. Liczne raporty i analizy podkreślały skuteczność wprowadzanych systemów zgłaszania naruszeń przez sygnalistów, wskazując jednocześnie na potrzebę udoskonalenia i uszczelnienia tego rozwiązania z uwagi na brak systemowych gwarancji. Powszechnemu przekonaniu o pozytywnym wpływie sygnalistów na zwalczanie naruszeń i przeciwdziałanie w tym zakresie

towarzyszyło jednak wiele wątpliwości związanych z ograniczeniami w optymalizowaniu korzyści płynących z whistleblowingu¹.

W raporcie opracowanym przez Komisję Prawną Parlamentu Europejskiego podkreślano, że powody odnotowywanej powściągliwości w zgłaszaniu naruszeń przez sygnalistów są wielorakie i **obejmują zarówno brak wiedzy na temat dostępnych opcji zgłaszania, jak i obawy przed represjami w przypadku ujawnienia nieprawidłowości**. Szkodliwe konsekwencje takich ograniczeń w korzystaniu z tego instrumentu mogły mieć bezpośredni wpływ na całe społeczeństwo, z uwagi na występujące liczne zagrożenia dla interesu publicznego, niezależnie od tego, czy dotyczą one środowiska, walki z uchylaniem się od opodatkowania lub z korupcją, czy też zdrowia publicznego, podważając w ten sposób prawo społeczeństwa do informacji².

Dodatkowym wyzwaniem, na które miały odpowiedzieć przepisy dyrektywy 2019/1937, było przeciwdziałanie ryzyku negatywnego wpływu braku skutecznej ochrony sygnalistów na wolność wypowiedzi i wolność mediów, zagwarantowane w art. 11 Karty praw podstawowych Unii Europejskiej. Jak podkreślała KE, przedstawiając projekt dyrektywy 2019/1937 w kwietniu 2018 r., **ochrona sygnalistów jako źródeł informacji dla dziennikarzy ma kluczowe znaczenie dla zagwarantowania dziennikarstwu śledczemu możliwości należytego wypełniania powierzonej mu strażniczej roli**³.

Przedstawiony przez Komisję w 2018 r. projekt dyrektywy stanowił odpowiedź na dotychczasową sytuację prawną sygnalistów w krajach UE, gdzie poziom ochrony był zapewniony w sposób niejednorodny i fragmentaryczny. Państwa członkowskie często zmieniały przepisy chroniące sygnalistów dopiero po poważnych skandalach lub katastrofach.

Istotną rolę w ugruntowaniu poziomu ochrony sygnalistów odegrały zalecenia przyjęte przez Radę Europy w 2014 r.⁴. Wytyczne przyjęte przez Radę Europy stanowiły znaczący krok naprzód w ustanowieniu zestawu standardów, które w późniejszych latach wielokrotnie były przedmiotem prac na tym forum. Problemem, na który wskazywano, było właśnie wyzwanie zapewnienia skuteczności obowiązujących zasad zgłaszania naruszeń, gdyż, jak podkreślano, w wielu państwach członkowskich, mimo obowiązujących przepisów dotyczących ochrony sygnalistów, skuteczność zgłaszania nieprawidłowości nie dość, że nie była satysfakcjonująca, to wręcz prowadziła do pogarszania sytuacji sygnalisty⁵. Dlatego też system wprowadzony przepisami dyrektywy 2019/1937 miał stanowić kompleksową odpowiedź na powyższe wyzwania, a jej skuteczność warunkowało prawidłowe wdrożenie dyrektywy przez państwa członkowskie, które miały przetrans-

¹ Draft report on the proposal for a directive of the European Parliament and of the Council on protection of persons reporting on breaches of Union law [COM(2018)0218-C8-0159/2018-2018/0106(COD)], 2.7.2018 r., s. 42, https://www.europarl.europa.eu/doceo/document/JURI-PR-623965_EN.html (dostęp: 11.9.2024 r.).

² Tamże.

³ Wniosek – Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii, Bruksela, 23.4.2018 r., COM(2018) 218 final, 2018/0106(COD), <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018PC0218> (dostęp: 11.9.2024 r.).

⁴ Zalecenia Komitetu Ministrów Rady Europy CM/Rec(2014)7 z 30.4.2014 r. w sprawie ochrony sygnalistów, <https://rm.coe.int/09000016805c5ea5> (dostęp: 11.9.2024 r.).

⁵ Speech by *Josan Meijers* (Netherlands, SOC), Congress rapporteur, Debate on „The Protection of whistleblowers. Challenges and opportunities for local and regional Government”, 36th Session of the Congress of Local and Regional Authorities (2–4 April 2019), <https://rm.coe.int/090000168093bdf0> (dostęp: 11.9.2024 r.).

ponować środki niezbędne do wykonania dyrektywy do 17.12.2021 r., jednak nie wszystkie zdołały spełnić ten obowiązek w terminie⁶.

Dyrektywa 2019/1937 odgrywa kluczową rolę w egzekwowaniu prawa Unii w wielu ważnych obszarach polityki, **w których naruszenia prawa Unii mogą szkodzić interesowi publicznemu** – od ochrony środowiska, przez obszary zamówień publicznych, usług finansowych, bezpieczeństwa jądrowego i bezpieczeństwa produktów, po ochronę interesów finansowych Unii. W tym artykule szczególną uwagę poświęcono zagadnieniom usprawnienia systemu zarządzania zgłoszeniami naruszeń w sektorze publicznym.

2. Standardy dotyczące ochrony sygnalistów w pracach Rady Europy

Rada Europy, organizacja utworzona w celu ochrony gwarancji praw człowieka, jako pierwsza organizacja o zasięgu międzynarodowym przyjęła dokument wytyczający standardy ochrony sygnalistów w Europie. W Rekomendacji CM/Rec(2014)7 Komitetu Ministrów Rady Europy z 30.4.2014 r. znalazły się zalecenia wprowadzenia przez rządy państw Rady Europy systemu gwarancji normatywnych, instytucjonalnych i judykacyjnych chroniących jednostki ujawniające informacje o zachowaniach stanowiących zagrożenie lub naruszenie interesu publicznego⁷.

W ramach wyznaczonych przez Radę Europy zaleceń warto podkreślić **wymóg ukonstytuowania odpowiednich rozwiązań instytucjonalnych odpowiedzialnych za monitorowanie wdrożenia** postanowień Rekomendacji. Rada Europy zwracała uwagę, że odpowiednie traktowanie przez pracodawców i organy publiczne ujawnień informacji będących w interesie publicznym ułatwi podejmowanie działań mających na celu zaradzenie ujawnionym zagrożeniom lub szkodom. Podkreślano, że **zgłoszenia w interesie publicznym i ujawnienia dokonane przez sygnalistów powinny być niezwłocznie badane**, a w razie potrzeby pracodawca i właściwy organ regulacyjny, organ ścigania lub organ nadzorujący powinni podejmować odpowiednie działania w sposób efektywny i skuteczny.

Budowanie efektywnego systemu instytucjonalnego w praktyce mogło jednak napotykać różnego rodzaju przeszkody, czego przykładem może być działanie RPO, który w ramach swoich kompetencji odwoływał się do Rekomendacji Rady Europy, podkreślając, że działalność sygnalistów może stanowić wczesne ostrzeżenie i pomoc w ujawnianiu nieprawidłowości, które w przeciwnym razie mogłyby pozostać ukryte, oraz w identyfikacji osób odpowiedzialnych za naruszenia. Wskazywał też, że **przepisy chroniące sygnalistów wzmacniają wartość kanałów ułatwiających zgłaszanie ryzyka lub wykroczeń**.

⁶ Komisja Europejska skierowała do Trybunału Sprawiedliwości wnioski przeciwko Czechom, Niemcom, Estonii, Hiszpanii, Włochom, Luksemburgowi, Węgrom i Polsce w związku z brakiem transpozycji i brakiem zawiadomienia o krajowych środkach transponujących do prawa krajowego. Komunikat prasowy KE z 15.2.2023 r. „Komisja Europejska podejmuje decyzję o skierowaniu do Trybunału Sprawiedliwości UE spraw przeciwko 8 państwom członkowskim w związku z ochroną sygnalistów”, https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_703 (dostęp: 11.9.2024 r.).

⁷ A.M. Świątkowski, Sygnalizacja (whistleblowing) a prawo pracy, PS 2015, Nr 5, s. 6–25.

Służą też samej organizacji, gdyż pomagają jej zrozumieć, że uczynienie procesu informowania o nieprawidłowościach łatwiejszym i bezpieczniejszym leży w jej interesie. Powołując się na Rekomendację Rady Europy, Rzecznik wskazywał, że ma to szczególne znaczenie w przypadku służb egzekwujących prawo, albowiem niewłaściwe zachowanie funkcjonariusza może rzutować na wizerunek całej formacji oraz szacunek dla prawa i instytucji państwa. Wdrażanie wewnętrznych mechanizmów raportowania o nieprawidłowościach sprzyja zaś kreowaniu wysokich standardów obsługi i zarządzania ryzykiem. Ochrona sygnalistów stanowi też narzędzie do usprawnienia mechanizmów kontrolnych⁸.

Ważne

Ochrona sygnalistów stanowi jeden z elementów działań podejmowanych na forum Rady Europy w związku ze zwalczaniem korupcji.

Podkreślano zwłaszcza aspekt związany z faktem, iż większość zmian w przepisach dotyczących ochrony sygnalistów ogranicza się do szczebla krajowego, jednocześnie marginalizując rolę organów lokalnych i regionalnych, które posiadają ograniczone narzędzia i mechanizmy zgłaszania podejrzeń o działaniach niezgodnych z prawem. Dlatego też w dokumencie „Challenges and opportunities for local and regional government” zwrócono uwagę, że: „sygnaliści odgrywają wyjątkową rolę w zarządzaniu lokalnym i regionalnym. Na szczeblu lokalnym (regionalnym), a więc najbliższym obywatelom, łatwiej jest wykryć domniemane naruszenia prawa niż na szczeblu krajowym. Oznacza to również, że **władze lokalne i regionalne są szczególnie narażone na różne rodzaje korupcji, biorąc pod uwagę ich odpowiedzialność za świadczenie usług publicznych**, która w coraz większym stopniu opiera się na partnerstwach publiczno-prywatnych, którym towarzyszy transfer zasobów publicznych do sektora prywatnego”⁹.

Należy zauważyć, że większość krajowych przepisów regulujących kwestie ochrony sygnalistów było wprowadzanych w ramach zwalczania korupcji, przy czym rola Rady Europy, a zwłaszcza komitetu GRECO, ma szczególne znaczenie, jeśli chodzi o wprowadzanie odpowiednich standardów. W konsekwencji walka z korupcją, będąca uzasadnieniem ustanowienia chronionego ujawniania informacji, często powoduje, że system koncentruje się wyłącznie na korupcji.

Ważne

Często nie uwzględnia się złożonego charakteru whistleblowingu, w szczególności tego, że jest on praktycznym przejawem wolności wypowiedzi, co zostało również uznane w orzecznictwie ETPC.

W przeciwieństwie do większości instrumentów prawnych w tej dziedzinie orzecznictwo nie podchodzi do kwestii whistleblowingu z punktu widzenia rodzaju ujawnianych infor-

⁸ List RPO Adama Bodnara do Prezesa RM Mateusza Morawieckiego, pismo z 16.4.2018 r., KMP.570.1.2018.RK, <https://bip.brpo.gov.pl/sites/default/files/Wyst%C4%85piecie%20RPO%20do%20premiera%20ws.%20ochrony%20sygnalist%C3%B3w%20jako%20mechanizmu%20ochronnego%20przed%20torturami.pdf> (dostęp: 23.9.2024 r.).

⁹ Raport „The Protection of whistleblowers. Challenges and opportunities for local and regional government” CG/GOV08(2018)07, 16.5.2018 r., <https://rm.coe.int/09000016808a4547> (dostęp: 23.9.2024 r.).

macji, ale raczej kluczowe znaczenie ma fakt, że whistleblowing jest praktycznym przejawem wolności wypowiedzi określonej w EKPC. Ponadto **w przeciwieństwie do raportów i rezolucji orzecznictwo jest źródłem prawa, które ma charakter bezwzględnie obowiązujący i jest wiążące**. W związku z tym wszelkie zmiany dokonane przez ETPC są bardzo istotne dla ochrony sygnalistów¹⁰.

W sposób jednoznaczny Rada Europy wskazywała, że w poszczególnych krajach brakuje niezbędnych przepisów na poziomie lokalnym i regionalnym, tj. samorządowym, a skupiają się one na wdrożeniu systemu w sektorze administracji na poziomie krajowym. Większość przepisów krajowych ograniczała się początkowo do pracowników sektora publicznego. Kanały zgłaszania nie były wystarczająco jasno określone w przepisach prawnych, a jednocześnie niektóre z nich kładły nacisk na regulację zgłoszeń wewnętrznych, które miały charakter obowiązkowy, w przeciwieństwie do powiadomień zewnętrznych. Ponadto brakowało jasności w kwestii tego, czy poufność jest gwarantowana. W regulacjach krajowych anonimowe zgłaszanie nieprawidłowości nie było rozwiązaniem preferowanym, a w niektórych państwach wręcz ustawowo zastrzegano możliwość odrzucania bądź odmowy podejmowania dochodzenia w sprawie anonimowych zgłoszeń. **Rada Europy podejmowała zatem liczne działania na rzecz usprawnienia i wdrożenia jednolitych standardów w ustawodawstwie przyjmowanym w Europie**. Z tego też względu działania podjęte w UE wychodziły naprzeciw zaleceniom i rekomendacjom Rady Europy.

3. Ochrona sygnalistów w instytucjach Unii Europejskiej

Kontekst, w którym KE przedstawiła projekt dyrektywy regulującej ochronę osób zgłaszających naruszenia – skandale takie jak Dieselgate, LuxLeaks, Panama Papers, Cambridge Analytica – podkreślał istotną rolę tzw. sygnalistów w wykrywaniu nielegalnych działań, które narażają na szwank interes publiczny oraz dobrobyt obywateli i społeczeństwa¹¹. Komisja podejmowała zatem działania, które miały uregulować na poziomie krajowym problem zwalczania nadużyć poprzez utworzenie mechanizmu zgłaszania bądź ujawniania informacji o nieprawidłowościach, gdyż rozwiązania wcześniej przyjęte na krajowym poziomie nie zapewniały w sposób kompleksowy i jednolity skutecznego systemu.

Ważne

Z prawnego punktu widzenia problem ze skutecznością systemu zgłaszania nieprawidłowości polegał w istocie na fragmentarycznej i niewystarczającej ochronie sygnalistów.

¹⁰ Report „The protection of whistleblowers. Challenges and opportunities for local and regional government”, CG36(2019)14 final, 3.4.2019 r., <https://rm.coe.int/the-protection-of-whistleblowers-challenges-and-opportunities-for-loc/16809312bd> (dostęp: 11.9.2024 r.).

¹¹ Komunikat prasowy KE „Ochrona osób sygnalizujących naruszenia – Komisja określa nowe ogólno-unijne zasady”, 23.4.2018 r., https://ec.europa.eu/commission/presscorner/detail/pl/ip_18_3441 (dostęp: 11.9.2024 r.).

W niektórych państwach członkowskich przepisy regulowały mechanizm w sposób kompleksowy, jednak w większości europejskich państw oferowano jedynie ochronę sektorową, np. w zakresie walki z korupcją, lub tylko dla sektora publicznego. **Elementy ochrony sygnalistów wprowadzone zostały też w konkretnych instrumentach UE** w obszarach takich jak usługi finansowe, bezpieczeństwo transportu i ochrona środowiska, gdzie istniała pilna potrzeba zapewnienia prawidłowego wdrożenia prawa UE.

W odpowiedzi na te wyzwania Komisja podjęła działania zmierzające do wprowadzenia ogólnounijnej „ochrony osób ujawniających przypadki naruszenia prawa Unii w dziedzinach takich jak: zamówienia publiczne, usługi finansowe, pranie pieniędzy i finansowanie terroryzmu, bezpieczeństwo produktów, bezpieczeństwo transportu, ochrona środowiska, bezpieczeństwo jądrowe, bezpieczeństwo żywności i pasz, zdrowie i dobrostan zwierząt, zdrowie publiczne, ochrona konsumentów, prywatność, ochrona danych i bezpieczeństwo sieci i systemów informatycznych. Ma on również zastosowanie do naruszeń unijnych reguł konkurencji, naruszeń i nadużyć przepisów dotyczących podatku od osób prawnych i szkody dla interesów finansowych UE¹². Przepisy dyrektywy stanowią niejako „docenienie” roli sygnalistów, zmierzając jednocześnie do usystematyzowania ich ochrony, również w obszarze związanym z przetwarzaniem danych osobowych¹³.

Jednym z elementów skuteczności mechanizmu jest z pewnością zapewnienie poufności i ochrona tożsamości osoby dokonującej zgłoszenia. Motyw 82 dyrektywy 2019/1937 określa, że ochrona poufności tożsamości osoby dokonującej zgłoszenia jest jednym z zasadniczych elementów zapobiegających działaniom odwetowym. Natomiast zgodnie z motywem 83 dyrektywy 2019/1937 należy zapewnić zgodność z RODO i OchrOsFizD, a także z rozporządzeniem UE 2018/1725 – w przypadku instytucji unijnych.

Prawodawca unijny, podejmując działania zmierzające do ograniczania przypadków naruszeń przepisów prawa unijnego, określił obszary, które szczególnie są ukierunkowane na osiągnięcie efektów – zamówienia publiczne, rynek finansowy, bezpieczeństwo produktów. Wskazuje się, że również w obszarze ochrony danych osobowych dyrektywa 2019/1937 zmierza do osiągnięcia poprawy poprzez umożliwienie dokonywania zgłoszeń bez zagrożenia negatywnymi skutkami, co może wpłynąć na ograniczenie incydentów w zakresie naruszeń prywatności oraz wycieku danych osobowych¹⁴.

¹² Tamże.

¹³ M. Możdżeń-Marcinkowski, Sygnalizowanie naruszeń prawa w administracji publicznej. Studium prawne, Warszawa 2024, s. 394.

¹⁴ Motyw 83 dyrektywy 2019/1937; B. Rodak (red.), Ochrona sygnalistów i postępowanie w sprawach zgłaszania naruszenia prawa, Warszawa 2023, s. 13.

4. Wytyczne Europejskiego Inspektora Ochrony Danych dotyczące przetwarzania danych osobowych w ramach procedury zgłaszania nieprawidłowości

Zgodnie z motywem 83 dyrektywy 2019/1937 wymiana lub przekazywanie informacji przez instytucje, organy lub jednostki organizacyjne Unii powinno odbywać się zgodnie z rozporządzeniem 2018/1725. Z tego też względu EDPS, który jest organem odpowiedzialnym za monitorowanie i egzekwowanie przestrzegania zasad ochrony danych osobowych w instytucjach i organach UE, posiada odpowiednie kompetencje w ramach systemów zgłaszania nieprawidłowości w unijnych instytucjach. Dyrektywa 2019/1937 odnosi się do wymiany i przekazywania informacji przez instytucje, organy lub jednostki organizacyjne Unii. Przypadki takie będą występowały zwłaszcza wtedy, **kiedy w ocenie właściwego organu wymagana byłaby interwencja podmiotu dysponującego ponadnarodowymi możliwościami wyjaśniania naruszeń**, np. OLAF¹⁵.

Europejski Inspektor Ochrony Danych ma prawo wydawać wytyczne i zalecenia dotyczące najlepszych praktyk w zakresie ochrony danych osobowych. W kontekście procedur zgłaszania nieprawidłowości EDPS wydał szczegółowe Wytyczne¹⁶, które mają na celu zapewnienie, że przetwarzanie danych osobowych w tych procedurach jest zgodne z prawem i chroni prywatność zarówno sygnalistów, jak i innych osób, których te zgłoszenia dotyczą. Dokument ten jest istotny dla wszelkich organizacji, które wprowadzają lub stosują procedury zgłaszania nieprawidłowości, aby mogły upewnić się, że przetwarzanie danych osobowych w tych procesach jest zgodne z unijnymi przepisami o ochronie danych.

Wytyczne stanowią więc praktyczny zestaw wskazówek, jak należy przetwarzać dane osobowe w ramach procedur zgłaszania nieprawidłowości, aby zapewnić ochronę zarówno osób zgłaszających nieprawidłowości, jak i osób, których te zgłoszenia dotyczą; EDPS odgrywa zatem kluczową rolę w zapewnianiu, że procedury zgłaszania nieprawidłowości chronią tożsamość sygnalistów, co jest istotnym elementem zgodności z przepisami o ochronie danych. Instytucje UE muszą stosować odpowiednie zabezpieczenia, aby zapobiec ujawnieniu tożsamości sygnalistów, chyba że wymaga tego prawo lub sygnalista wyraża na to zgodę; EDPS podkreśla znaczenie ochrony tożsamości osób zgłaszających nieprawidłowości. Instytucje muszą zapewnić, że tożsamość sygnalistów pozostanie poufna, aby chronić ich przed ewentualnymi represjami lub negatywnymi konsekwencjami. Obejmuje to wdrażanie odpowiednich zabezpieczeń technicznych i organizacyjnych, które minimalizują ryzyko nieautoryzowanego ujawnienia tożsamości sygnalisty.

¹⁵ T. Łodziana, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 27 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii. Komentarz, Ridero 2020, s. 118.

¹⁶ Wytyczne EDPS „Guidelines on processing personal information within a whistleblowing procedure”, grudzień 2019 r., https://www.edps.europa.eu/sites/default/files/publication/19-12-17_whistleblowing_guidelines_en.pdf (dostęp: 11.9.2024 r.).

Ważne

W Wytocznych EDPS zwraca uwagę na zasadę minimalizacji danych, co oznacza, że instytucje powinny przetwarzać tylko te dane osobowe, które są niezbędne do realizacji celu zgłoszenia. Oznacza to unikanie zbierania nadmiarowych danych, które nie są ściśle związane z konkretnym przypadkiem zgłoszenia nieprawidłowości.

Osoby, których dane są przetwarzane w ramach procedur zgłaszania nieprawidłowości, muszą być informowane o tym, w jaki sposób ich dane są przetwarzane. Europejski Inspektor Ochrony Danych zwraca uwagę, że instytucje powinny dostarczać jasne i zrozumiałe informacje na temat tego, jakie dane są zbierane, w jakim celu, kto będzie miał do nich dostęp oraz jak długo będą przechowywane.

Duży nacisk kładzie się też na konieczność przestrzegania praw osób, których dane dotyczą, takich jak prawo dostępu do danych, prawo do ich sprostowania, usunięcia czy ograniczenia przetwarzania. Instytucje muszą zapewnić, że te prawa mogą być skutecznie realizowane, nawet w kontekście poufności i ochrony tożsamości sygnalistów.

W Wytocznych EDPS **wyjaśnia również kwestie zabezpieczeń technicznych i organizacyjnych, wymagając, aby instytucje stosowały odpowiednie i adekwatne środki** w celu ochrony danych osobowych przetwarzanych w ramach procedur zgłaszania nieprawidłowości. Obejmuje to m.in. szyfrowanie danych, kontrolę dostępu oraz regularne przeglądy procedur bezpieczeństwa.

Europejski Inspektor Ochrony Danych podkreśla, że dane osobowe zebrane w ramach procedur zgłaszania nieprawidłowości powinny być wykorzystywane wyłącznie w celach, dla których zostały zgromadzone. Przetwarzanie tych danych w innych celach powinno być ściśle ograniczone i uzasadnione, a w niektórych przypadkach wymagać zgody osób, których dane dotyczą. Jak podkreślają Wytoczne, **zakres procedury musi być ograniczony, aby uniknąć jej nadużywania**. Cel procedury zgłaszania nieprawidłowości musi być jasno określony w regulaminie wewnętrznym/polityce unijnej instytucji. Przepisy wewnętrzne lub polityka powinny wyraźnie określać, w jakich okolicznościach należy korzystać z kanałów informowania o nieprawidłowościach, a w jakich nie.

Generalnie kanały zgłaszania nieprawidłowości nie powinny być wykorzystywane, gdy pracownicy mogą skorzystać ze swoich praw pracowniczych na ogólnych zasadach, np. poprzez złożenie wniosku lub skargi (np. zgodnie z art. 90 regulaminu pracowniczego¹⁷), lub w przypadku innych roszczeń mogą zwrócić się do działu kadr, służby mediacyjnej, poufnego doradcy na podstawie innych procedur (np. postępowanie przeciwko osobie dopuszczającej się gróźb, obraźliwych lub zniesławiających czynów lub wypowiedzi, lub jakiegokolwiek napaści).

¹⁷ Ogólne ramy prawne dla pracowników UE działających jako sygnaliści są określone w regulaminie pracowniczym, REGULATION No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community OJ 45, 14.6.1962, p. 1385, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20140101:en:PDF> (dostęp: 2.10.2024 r.).

Przepisy wewnętrzne lub polityka powinny ponadto określać, że informacje szczególnie chronione, takie jak pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych oraz dane dotyczące zdrowia lub życia seksualnego, które nie są istotne dla sprawy, nie powinny być gromadzone. Pomoże to uniknąć gromadzenia nadmiernych danych osobowych.

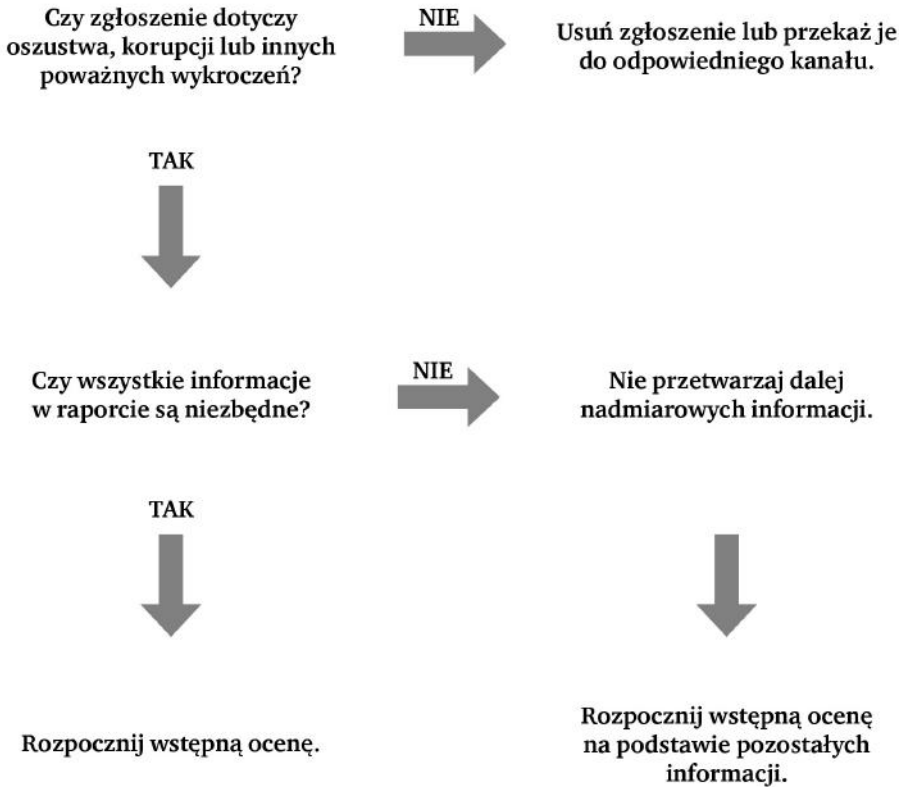
Zasadniczo zgłaszanie nieprawidłowości nie powinno być anonimowe. Osoby zgłaszające nieprawidłowości powinny być prośzone o ujawnienie swojej tożsamości nie tylko w celu uniknięcia nadużyć procedury, ale także w celu umożliwienia im skutecznej ochrony przed wszelkimi działaniami odwetowymi. Pozwoli to również na lepsze zarządzanie dokumentacją, jeśli konieczne będzie zebranie dalszych informacji.

Europejski Inspektor Ochrony Danych zwraca też uwagę na konieczność ograniczenia okresu przechowywania danych osobowych do minimum niezbędnego do realizacji celu, dla którego zostały zebrane. Po zakończeniu postępowania wyjaśniającego dane powinny być usunięte, chyba że istnieją uzasadnione powody prawne do ich dalszego przechowywania.

Nie bez znaczenia jest też rola szkoleń i podnoszenia świadomości wśród pracowników instytucji UE na temat ochrony danych osobowych w kontekście procedur zgłaszania nieprawidłowości. Pracownicy muszą być świadomi swoich obowiązków i znać procedury, które mają na celu ochronę danych osobowych. Te aspekty mają kluczowe znaczenie dla zapewnienia, że procedury zgłaszania nieprawidłowości są zgodne z przepisami ochrony danych i chronią zarówno sygnalistów, jak i osoby, których dane dotyczą.

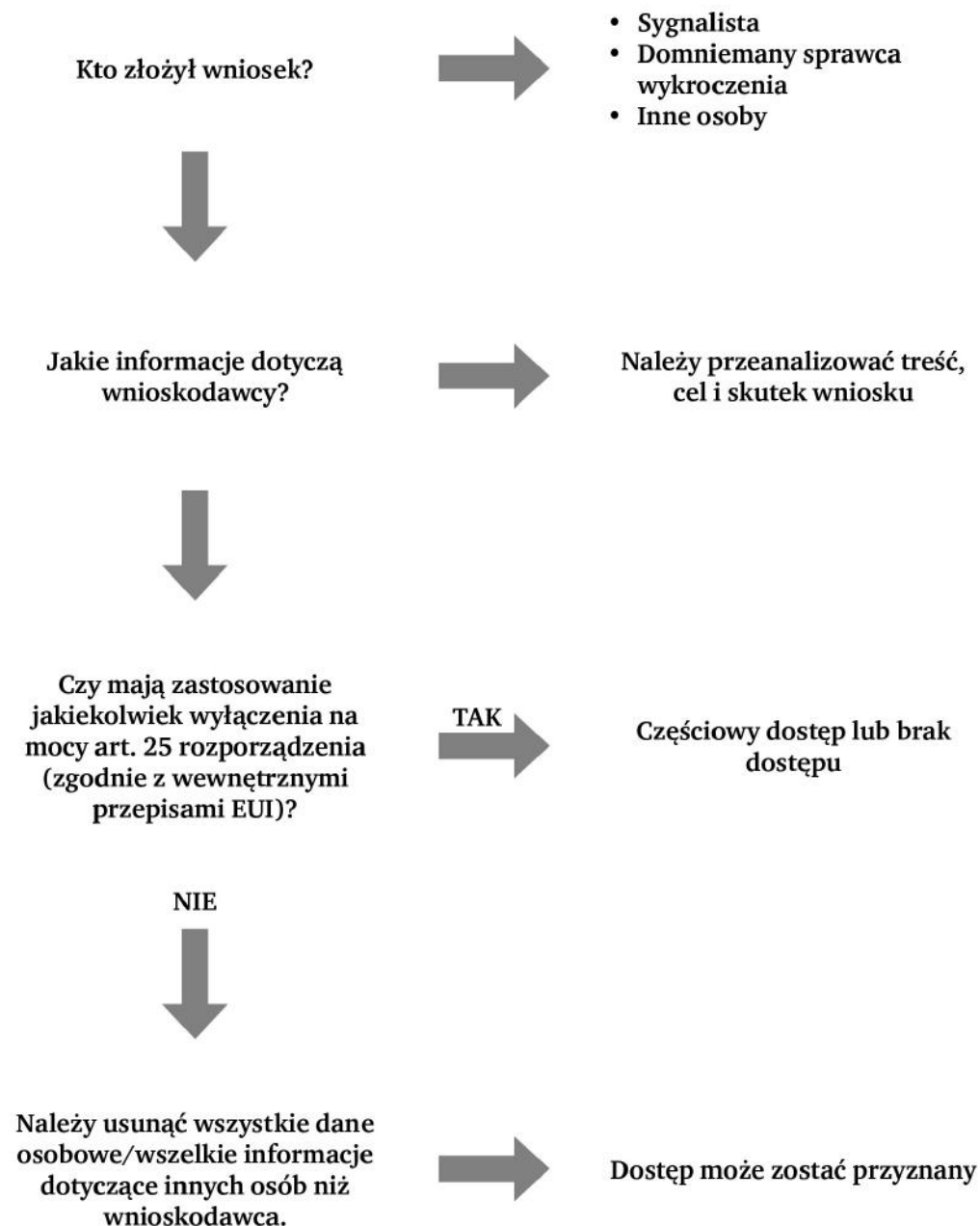
W dokumencie zawarte zostały również przykładowe schematy procedur zgłaszania nieprawidłowości oraz realizacji praw osób, których dane dotyczą.

Rysunek 1. Obsługa zgłoszeń o nieprawidłowościach



Źródło: Schemat opracowany na podstawie Wytycznych EDPS „Guidelines on processing personal information within a whistleblowing procedure” (tłumaczenie własne), s. 13.

Rysunek 2. Obsługa wniosków o dostęp do danych



Źródło: Schemat opracowany na podstawie Wytycznych EDPS „Guidelines on processing personal information within a whistleblowing procedure” (tłumaczenie własne), s. 13.

5. Podsumowanie

Utworzenie skutecznego mechanizmu zgłaszania naruszeń prawa UE wymagało podjęcia przez unijnego prawodawcę działań legislacyjnych, które doprowadziły do przyjęcia dyrektywy 2019/1937. Jak się podkreśla, dopiero obowiązek implementacji jej przepisów wpłynął na podjęcie istotnych działań przez krajowych prawodawców, zmierzających do stworzenia racjonalnego i kompleksowego systemu ochrony interesu publicznego w celu wyeliminowania wielu zagrożeń, których to rozwiązań dostarczyły uregulowania unijnej dyrektywy o sygnalistach¹⁸. Warto jednak zauważyć, że proces wdrożenia dyrektywy 2019/1937, który napotkał wiele wyzwań, ma szansę przyczynić się do ugruntowania nowych, dobrze przemyślanych rozwiązań, odpowiadających europejskim standardom.

Podstawa prawna:

- motywy: 82, 83 dyrektywy 2019/1937.

¹⁸M. Jabłoński, T. Radziszewski, D. Wasiak, K. Wygoda, Sygnalista, Toruń 2022.

Marlena Sakowska-Baryła

Rozdział II. Podmioty publiczne zobowiązane do wprowadzenia systemu ochrony sygnalistów

1. Uwagi wstępne

Charakterystyka „publicznych podmiotów” zobowiązanych do wprowadzenia systemu ochrony sygnalistów wymaga na wstępie sprecyzowania, o jakie podmioty i w jakim kontekście tu chodzi, a więc podejścia nieco szerszego niż w przypadku zdefiniowania pojęcia „podmiot publiczny” w słowniczku ustawowym. **Podmioty należące do kategorii „publicznych” zasadniczo nie tworzą bowiem jednorodnej grupy.** Sposób ich określania w przepisach dotyczących ochrony sygnalistów ma ścisły związek z wyodrębnieniem i specyfiką zapewniania obsługi wewnętrznych i zewnętrznych zgłoszeń naruszeń prawa, a także z wyłączeniami lub ograniczeniami, jakie w odniesieniu do pewnych podmiotów lub szczególnych obszarów ich działalności przewidziano w przepisach regulujących problematykę ochrony sygnalistów. Niniejszy rozdział poświęcony jest zasadniczo podmiotom, które mieszczą się w zakresie ustawowego pojęcia „podmiot publiczny” i są zobowiązane do zorganizowania systemu ochrony sygnalistów w tym sensie, że mają zapewnić:

- 1) możliwość dokonywania zgłoszeń wewnętrznych z zachowaniem rygorów przewidzianych w przepisach prawa;
- 2) przeprowadzenie działań następczych;
- 3) ochronę sygnalisty przed działaniami odwetowymi;
- 4) wdrożenie odpowiednich środków organizacyjnych i technicznych na wszystkich etapach działań podejmowanych w związku z przyjmowanymi zgłoszeniami naruszeń prawa.

W praktyce jednak o podmiotach publicznych, podmiotach sektora publicznego, sektorze publicznym, sferze publicznej mówi się w znacznie szerszym kontekście. Istotne jest zatem, by te wątki podmiotów o wyraźnie publicznym charakterze, do których w różnej mierze adresowana jest regulacja z zakresu ochrony sygnalistów, odpowiednio uchwycić i uporządkować, ponieważ – jak się okazuje – określenia te w analizowanym obszarze nie powinny być używane zamiennie. **Takie pojęcia jak „organ publiczny” i „podmiot publiczny” mają bowiem skonkretyzowane znaczenie.**

Dla dokonania kategoryzacji niezbędne jest sięgnięcie przede wszystkim do przepisów dyrektywy 2019/1937 oraz OchrSygnalU. Zaznaczyć przy tym należy, że analiza prowadzona w tym rozdziale dotyczy regulacji zawartych w tych właśnie aktach prawnych z pominięciem innych regulacji przewidujących osobne procedury zgłaszania naruszeń prawa i ochrony sygnalistów. Z oczywistych względów szczególna uwaga skupiona jest na rozwiązaniach wynikających z treści OchrSygnalU, ponieważ tę – w przeciwieństwie do przepisów dyrektywy 2019/1937 – stosuje się bezpośrednio i ta ustawa właśnie narzuca pewien rygor terminologiczny, którego należy przestrzegać, kształtując system ochrony sygnalistów zgodnie z jej wymaganiami.

Ustawa o ochronie sygnalistów definiuje podmioty publiczne w art. 2 pkt 12 poprzez odesłanie do przepisów OtwDanU i podmiotom publicznym w tym rozumieniu poświęcone zostanie najwięcej uwagi. Oparcie klasyfikacji publicznych podmiotów w kontekście ochrony sygnalistów wyłącznie na tym, co wynika z powyższego odesłania, nie wyczerpuje jednak problematyki podmiotów o wyraźnie publicznym charakterze, którym przepisy OchrSygnalU przypisują określoną rolę oraz do których w jakimś kontekście się odnoszą.

Publiczne podmioty, do których odnosi się OchrSygnalU, sklasyfikować można w następujący sposób:

- 1) podmioty publiczne w rozumieniu art. 2 pkt 12 OchrSygnalU – zobowiązane do obsługi wewnętrznych zgłoszeń naruszeń prawa;
- 2) organy publiczne w rozumieniu art. 2 pkt 6 OchrSygnalU – zobowiązane do obsługi zewnętrznych zgłoszeń naruszeń prawa, z uwzględnieniem szczególnego przypadku określonego w art. 5 ust. 4 OchrSygnalU;
- 3) podmioty i organy publiczne, które na podstawie art. 5 ust. 1–3 OchrSygnalU podlegają ograniczeniom w zakresie stosowania jej przepisów, a także takie, do których zastosowanie ma art. 10 OchrSygnalU.

Dla przybliżenia powyższą klasyfikację można przedstawić w ujęciu tabelarycznym, obejmującym również treść właściwych przepisów OchrSygnalU.

Tabela 1. Podmioty publiczne, których dotyczy OchrSygnalU

Kategoria podmiotowa	Przepis OchrSygnalU	Zakres przedmiotowy
Podmioty publiczne	art. 2 pkt 12 Ilekcroć w niniejszej ustawie jest mowa o podmiocie publicznym – należy przez to rozumieć podmiot wskazany w art. 3 OtwDanU.	Obsługa zgłoszeń wewnętrznych

Kategoria podmiotowa	Przepis OchrSygnalU	Zakres przedmiotowy
Organy publiczne	<p>art. 2 pkt 6 Ilekcroć w niniejszej ustawie jest mowa o organie publicznym – należy przez to rozumieć naczelne i centralne organy administracji rządowej, terenowe organy administracji rządowej, organy jednostek samorządu terytorialnego, inne organy państwowe oraz inne podmioty wykonujące z mocy prawa zadania z zakresu administracji publicznej, właściwe do podejmowania działań następczych w dziedzinach wskazanych w art. 3 ust. 1.</p> <p>art. 5 ust. 4 Organem publicznym właściwym do przyjęcia zgłoszenia zewnętrznego dotyczącego naruszenia prawa przez służby specjalne, o których mowa w art. 11 BezpWewnU, oraz realizacji zadań, o których mowa w rozdziale 4, jest Prezes Rady Ministrów albo Minister – Koordynator Służb Specjalnych, w przypadku jego powołania.</p>	Obsługa zgłoszeń zewnętrznych
Podmioty i organy publiczne podlegające wyłączeniom	<p>art. 5 ust. 1 Ustawy nie stosuje się do informacji objętych: 1) przepisami o ochronie informacji niejawnych oraz innych informacji, które nie podlegają ujawnieniu z mocy przepisów prawa powszechnie obowiązującego ze względów bezpieczeństwa publicznego; 2) tajemnicą zawodową zawodów medycznych oraz prawniczych; 3) tajemnicą narady sędziowskiej; 4) postępowaniem karnym – w zakresie tajemnicy postępowania przygotowawczego oraz tajemnicy rozprawy sądowej prowadzonej z wyłączeniem jawności.</p> <p>art. 5 ust. 2 Ustawy nie stosuje się do naruszeń prawa w zakresie zamówień w dziedzinach obronności i bezpieczeństwa w rozumieniu art. 7 pkt 36 PrZamPubl, do których nie stosuje się tej ustawy, umów offsetowych zawieranych na podstawie OffsetU oraz innych środków podejmowanych w celu ochrony podstawowych lub istotnych interesów bezpieczeństwa państwa na podstawie art. 346 TFUE.</p> <p>art. 5 ust. 3 Przepisów rozdziału 5 nie stosuje się do naruszeń prawa bezpośrednio związanych z realizacją przez służby specjalne, o których mowa w art. 11 BezpWewnU, ustawowych zadań mających na celu zapewnienie bezpieczeństwa narodowego.</p>	Obszary wyłączone spod stosowania OchrSygnalU lub określonych jej przepisów, do których ustawa ma zastosowanie w zakresie nieuregulowanym w przepisach aktów normatywnych ustanowionych przez instytucje UE, a także obszary objęte regulacją innych przepisów prawa

[Przejdź do księgarni →](#)

ksiegarnia.beck.pl