

Załącznik nr 5 Do Procedury Zgłoszeń Wewnętrznych

Zasady ochrony danych sygnalisty oraz innych osób których dane są przetwarzane w związku z rozpatrywaniem zgłoszenia i podejmowaniem działań następczych

Procedura stanowi integralną część wewnętrznego regulaminu przyjmowania i rozpatrywania zgłoszeń naruszeń prawa, na podstawie ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. poz. 928).

I. Zasady ogólne

1. Procedura zostaje ustanowiona w celu zapewnienia należytej ochrony sygnalistów, czyli osób zgłaszających lub publicznie ujawniających informacje o naruszeniach prawa, a także osób, które pomagają im dokonać zgłoszenia.
2. Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego realizuje zadania związane z ochroną sygnalistów, zgodnie z przepisami ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. poz. 928).
3. Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.U. UE. L. Nr 119, s. 1 ze zm.) – dalej RODO, przetwarzanych w celu realizacji zadań związanych z obsługą zgłoszeń wewnętrznych.
4. Administrator, po uzyskaniu zgłoszenia, przetwarza je zgodnie z zasadami ochrony danych osobowych, o których mowa w art. 5 RODO, w szczególności zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a) RODO) oraz zasady minimalizacji (art. 5 ust. 1 lit. c) RODO), w zakresie niezbędnym do weryfikacji zgłoszenia i podjęcia ewentualnych działań następczych.
5. Dane sygnalisty powinny pozostać poufne i nie mogą być ujawniane w toku postępowania stronom i uczestnikom tego postępowania, bez wyraźnego i jednoznacznego przyzwolenia ze strony sygnalisty.
6. Dostęp do danych sygnalisty może mieć tylko i wyłącznie osoba, która otrzymała pisemne upoważnienie do przetwarzania danych osobowych w tym zakresie i została zobligowana do zachowania poufności danych oraz ochrony tożsamości sygnalisty.
7. Jeżeli zgłoszenie dotyczy innych osób (np. świadków, osób trzecich), należy zapewnić ochronę poufności ich tożsamości, na takich samych zasadach jak ochrona danych sygnalisty.
8. Wobec danych sygnalisty stosuje się pseudonimizację.
9. Nie są przyjmowane zgłoszenia anonimowe. W przypadku wpłynięcia takiego zgłoszenia nie jest ono rozpatrywane.

10. Pracownicy i osoby zatrudnione są zobligowane do stosowania Procedury.
11. Na stronie internetowej jednostki zamieszcza się klauzulę informacyjną dla sygnalistów oraz innych osób których dane są przetwarzane przy rozpatrywaniu zgłoszenia naruszenia. Ponadto Klauzula informacyjna jest także przekazywana przy pierwszym kontakcie z sygnalistą.
12. Osobom wyznaczonym do rozpatrywania zgłoszeń gwarantuje się niezależność w wykonywaniu swoich działań. Osoby te winny zachować bezstronność podczas rozpatrywania zgłoszenia i stosowania działań następczych.
13. Administrator stosuje odpowiednie środki organizacyjne i techniczne, o których mowa w art. 32 RODO, zapewniające ochronę danych sygnalisty, osoby, której dotyczy zgłoszenie, osoby trzeciej wskazanej w zgłoszeniu. Administrator zapewnia ochronę poufności danych osobowych sygnalisty, osoby, której dotyczy zgłoszenie, osób wskazanych w zgłoszeniu.
14. Administrator zapewnia, że dostęp do danych osobowych zawartych w zgłoszeniu następuje wyłącznie w odniesieniu do osób upoważnionych przez niego, w formie pisemnej, do przetwarzania danych osobowych, a osoby upoważnione zobowiązały się do zachowania w tajemnicy informacji i danych osobowych uzyskanych w ramach powierzonych zadań związanych z obsługą sygnalistów, tj. przyjmowania, weryfikacji zgłoszeń, podejmowania działań następczych.
15. Administrator informuje wskazanego sygnalistę, osoby, których dotyczy zgłoszenie, osoby wskazane w zgłoszeniu, o zasadach ochrony ich danych osobowych

II. Zasady ochrony danych podczas rozpatrywania zgłoszeń

1. Dostęp do kanałów zgłaszania nieprawidłowości mają tylko i wyłącznie osoby uprawnione do rozpatrywania zgłoszeń naruszenia prawa na podstawie pisemnego upoważnienia udzielonego przez Administratora
2. W przypadku zgłoszeń ustnych lub przyjmowania ustnych wyjaśnień, należy zapewnić środki umożliwiające ochronę poufności tożsamości sygnalisty poprzez brak obecności osób postronnych podczas wizyty, wybór pomieszczenia, które nie jest objęte monitoringiem wizyjnym.
3. Tworzy się rejestr zgłoszeń wewnętrznych.
4. Dostęp do danych w rejestrze ma tylko i wyłącznie osoba upoważniona do przetwarzania danych sygnalistów.
5. Osoba wyznaczona do przyjmowania zgłoszeń, niezwłocznie po otrzymaniu dokonuje pseudonimizacji danych sygnalisty i nadaje mu identyfikator (np. numeryczny), który będzie wykorzystywany podczas postępowania wyjaśniającego.
6. Pseudonimizacja obejmuje wszelkiego rodzaju informacje umożliwiające bezpośrednią lub pośrednią identyfikację sygnalisty, ze szczególnym uwzględnieniem tego, czy sama treść zgłoszenia nie wskazuje na tożsamość sygnalisty.
7. Nie dokonuje się pseudonimizacji danych sygnalisty, jeżeli wyraźnie wyraził zgodę na upublicznienie jego danych.
8. Zakazane jest stosowanie jakichkolwiek działań odwetowych wobec sygnalisty.
9. Udział w procesie rozpatrywania mogą brać tylko bezstronne osoby, które zostały zobligowane do zachowania poufności, także po ustaniu stosunku pracy lub zakończeniu współpracy.
10. Zapewnia się ochronę dokumentacji dotyczącej zgłoszeń oraz postępowania następczych:
 1. dane papierowe są przechowywane w szafie zamykanej na klucz, do której dostęp mają tylko osoby upoważnione do przetwarzania danych związanych z postępowaniami;
 2. dostęp do systemów, w których są przetwarzane dane, jest ograniczony do uprawnionych użytkowników, a każde działanie na danych (dostęp, edycja, usuwanie, itp.) jest rejestrowane;
 3. dane przekazywane drogą elektroniczną są wcześniej zaszyfrowane i/lub pseudonimizowane;

4. dane po ustaniu przydatności są usuwane bezpowrotnie z systemów, a dane papierowe niszczone w niszczarce.
11. Na wszystkich etapach postępowania wyjaśniającego zamiast danych sygnalisty jest stosowany przypisany identyfikator.
12. W postępowaniu należy odwołać się do numeru sprawy, pod którą zostało zarejestrowane zgłoszenie od sygnalisty, a nie sprawy, której dotyczy zgłoszenie naruszenia.
13. Dane sygnalisty nie ujawnia się na wniosek stron lub uczestników postępowania wyjaśniającego.
14. Sygnalista jest informowany o okolicznościach, w których ujawnienie jego tożsamości stanie się konieczne. Obowiązek uzyskania zgody sygnalisty na ujawnienie jego tożsamości nie dotyczy 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
15. Dane sygnalisty nie zamieszcza się w rozdzielnikach dokumentów związanych z postępowaniem wyjaśniającym, ani w korespondencji mailowej.
16. Jeżeli zgłoszenie wpłynie innym, niż zatwierdzony do przyjmowania zgłoszeń kanałem, osoba która je otrzyma jest zobligowana niezwłocznie przekazać je do osoby upoważnionej do rozpatrywania zgłoszeń i usunąć wszelkie jej kopie (np. z poczty e-mail).
17. Dane sygnalisty mogą być ujawnione tylko we wskazanych okolicznościach:
 1. uprawnionym organom, w związku z prowadzonym postępowaniem;
 2. na wniosek i za zgodą sygnalisty
 3. jeśli sygnalista nie spełnił wymogów określonych w art. 6 ustawy o ochronie sygnalistów
18. Dane osobowe mogą być udostępnione podmiotom zewnętrznym wspierającym administratora w zakresie przyjmowania zgłoszeń wewnętrznych, na podstawie umowy powierzenia przetwarzania danych osobowych, określającej w szczególności przedmiot, czas trwania powierzenia, charakter i cel przetwarzania, rodzaj danych osobowych, prawa i obowiązki administratora, zgodnie z art. 28 RODO. Administrator zapewnia, że taki podmiot zostanie zweryfikowany w celu ustalenia, czy zapewnia odpowiedni poziom ochrony danych osobowych w odniesieniu do powierzonych zadań (przyjmowanie zgłoszeń sygnalistów).
19. Dane osobowe będą udostępniane odrębnym administratorom, tj. właściwym organom, w przypadku podejmowania działań następczych i prowadzenia postępowań.
20. Administrator zapewnia realizację praw osób, których dane są przetwarzane w ramach obsługi zgłoszeń sygnalistów, wskazanych w treści klauzuli informacyjnej kierowanej do sygnalisty, osoby, której dotyczy zgłoszenie oraz osoby wskazanej w zgłoszeniu.
21. Realizacja niektórych praw osób, których dane dotyczą, następuje z ograniczeniami, o których mowa w art. 8 ust. 5 i 6 ustawy o ochronie sygnalistów:
 - 1) administrator nie informuje osób, których dane są przetwarzane na podstawie art. 14 RODO (osoby, której dotyczy zgłoszenie oraz osoby wskazanej w zgłoszeniu) o źródle danych osobowych, chyba, że sygnalista nie spełnia warunków wskazanych w art. 6 ustawy o ochronie sygnalistów albo wyraził wyraźną zgodę na takie przekazanie,
 - 2) w ramach realizacji prawa dostępu do danych osobowych administrator nie przekazuje informacji o źródle danych, chyba że sygnalista nie spełnia warunków wskazanych w art. 6 ustawy o ochronie sygnalistów albo wyraził wyraźną zgodę na takie przekazanie.
22. Dane osobowe, przetwarzane w ramach systemu zgłoszeń wewnętrznych, będą przechowywane przez okres 3 lat od zakończenia roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.
23. 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.