Procedura Zgłoszeń Wewnętrznych i Podejmowania Działań Następczych w proaxia consulting group ag | Oddział w Polsce

Spis treści:

English version below (for reference purposes only)

I – Cel i definicje

§ 1

1. Podstawę prawną dla wprowadzenia Procedury Zgłoszeń Wewnętrznych i Podejmowania Działań Następczych stanowi Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów.
2. Procedura Zgłoszeń Wewnętrznych i Podejmowania Działań Następczych ma na celu zapewnienie bezpiecznego i poufnego sposobu zgłaszania nieprawidłowości, ochrony sygnalistów przed działaniami odwetowymi oraz umożliwienie organizacji skutecznego identyfikowania i eliminowania naruszeń prawa.

§ 2

Użyte w Procedurze określenia oznaczają:

1. **Procedura** – Procedura Zgłoszeń Wewnętrznych i Podejmowania Działań Następczych – zbiór obowiązujących w firmie proaxia consulting group ag Oddział w Polsce zasad, regulacji i działań organizacyjnych, określających sposób przyjmowania, rejestrowania, weryfikacji, rozpatrywania i dokumentowania zgłoszeń dotyczących naruszeń prawa, a także tryb udzielania informacji zwrotnej sygnaliście oraz zasady ochrony osób dokonujących zgłoszenia przed działaniami odwetowymi.
2. **Pracodawca lub Firma** – firma proaxia consulting group ag Oddział w Polsce reprezentowana przez Pełnomocnika oddziału w Polsce.
3. **Pracownik** – osoba pozostająca z Pracodawcą w stosunku pracy.
4. **Sygnalista** – osoba fizyczna dokonująca zgłoszenia nieprawidłowości, działająca w dobrej wierze oraz posiadająca uzasadnione podstawy, by uznać, że informacje o naruszeniu prawa są prawdziwe w chwili dokonania zgłoszenia. Sygnalistą jest każda osoba związana z Firmą, w której zidentyfikowała naruszenia norm prawnych, o których dowiedziała się w związku z wykonywaniem obowiązków zawodowych.
5. **Zespół ds. obsługi zgłoszeń sygnalistów** – osoby wyznaczone przez podmiot prawny i upoważnione do przyjmowania zgłoszeń naruszeń prawa, prowadzenia rejestru zgłoszeń, proponowania, podejmowania działań następczych oraz przekazywania informacji zwrotnej sygnalistom, działające z zachowaniem poufności, bezstronności i zgodnie z przepisami ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów oraz niniejszą procedurą.
6. **Zgłoszenie** – przekazanie, za pośrednictwem ustanowionego kanału zgłoszeń wewnętrznych, informacji dotyczących rzeczywistego lub potencjalnego naruszenia prawa.
7. **Naruszenie** – każde działanie lub zaniechanie sprzeczne z powszechnie obowiązującymi przepisami prawa lub mające na celu obejście prawa, mogące wywołać szkodę dla organizacji, jej pracowników, kontrahentów, klientów lub interesu publicznego.
8. **Działania odwetowe** – wszelkie bezprawne lub nieuzasadnione działania lub zaniechania w kontekście związanym z pracą, podejmowane wobec sygnalisty w związku z dokonanym zgłoszeniem, które wyrządza lub może wyrządzić nieuzasadnioną szkodę sygnaliście.
9. **Kanał zgłoszeń wewnętrznych** – zorganizowane przez Firmę i zapewniające poufność narzędzie lub procedura służąca przekazaniu podmiotowi prawnemu informacji o naruszeniu prawa, obejmująca dedykowany adres poczty elektronicznej.
10. **Działania następcze** – wszelkie czynności podjęte przez Firmę po otrzymaniu zgłoszenia, obejmujące analizę zgłoszenia, prowadzenie postępowania wyjaśniającego, podejmowanie działań korygujących, naprawczych lub dyscyplinarnych, a także przekazywanie sygnaliście informacji zwrotnej zgodnie

z obowiązującymi przepisami. Działania następcze prowadzone są w celu oceny prawdziwości informacji zawartych w zgłoszeniu oraz w celu przeciwdziałania naruszeniu prawa będącemu przedmiotem zgłoszenia.

11. **Poufność** – zasada zapewniająca, że tożsamość sygnalisty, osób wskazanych w zgłoszeniu oraz wszelkie informacje zawarte w zgłoszeniu podlegają ochronie i mogą być ujawnione wyłącznie osobom upoważnionym i podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa lub regulacji wewnętrznych.
12. **Ustawa o ochronie sygnalistów** – Ustawa z dnia 14 czerwca 2024 r. (Dz. U. z 2024 r. poz. 928), która reguluje zasady zgłaszania naruszeń prawa oraz zapewniania ochrony osobom zgłaszającym takie naruszenia (sygnalistom).

II – Zakres naruszeń i osoby objęte procedurą

§ 3

1. Zgłaszane naruszenia – zgłoszeniu w ramach niniejszej Procedury podlegają informacje dotyczące naruszeń prawa lub podejrzeń ich popełnienia, które mieszczą się w zakresie przedmiotowym określonym w Ustawie o ochronie sygnalistów. Zgłoszenia mogą dotyczyć naruszeń prawa dotyczących:

    a) zamówień publicznych,
    b) usług, produktów i rynków finansowych, a także zapobiegania praniu pieniędzy oraz finansowaniu terroryzmu,
    c) bezpieczeństwa produktów,
    d) bezpieczeństwa transportu,
    e) ochrony środowiska,
    f) ochrony radiologicznej i bezpieczeństwa jądrowego,
    g) bezpieczeństwa żywności i pasz, zdrowia i dobrostanu zwierząt,
    h) zdrowia publicznego,
    i) ochrony konsumentów,
    j) ochrony prywatności i danych osobowych,
    k) bezpieczeństwa sieci i systemów teleinformatycznych,
    l) naruszeń dotyczących interesów finansowych Unii Europejskiej,
    m) naruszeń dotyczących rynku wewnętrznego, w tym reguł konkurencji, pomocy państwa oraz zasad opodatkowania przedsiębiorstw.

§ 4

2. Procedura ma zastosowanie do wszystkich osób, które mogą dokonywać zgłoszeń zgodnie z Ustawą o ochronie sygnalistów, zgłaszających informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, w tym:

    a) pracowników,
    b) osób świadczących pracę na innej podstawie niż stosunek pracy, w tym na podstawie umów cywilnoprawnych,
    c) osób wykonujących pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy,
    d) przedsiębiorców, kontrahentów oraz partnerów biznesowych,
    e) akcjonariuszy i wspólników,
    f) członków organów osoby prawnej,

g) stażystów i praktykantów (płatnych i bezpłatnych),
h) wolontariuszy,
i) byłych pracowników oraz osób, których stosunek pracy lub współpracy uległ rozwiązaniu,
j) kandydatów ubiegających się o zatrudnienie lub nawiązanie współpracy, którzy uzyskali informacje o naruszeniach na etapie rekrutacji, rozmów lub negocjacji.

3. Kontekst związany z pracą – należy przez to rozumieć przeszłe, obecne lub przyszłe działania związane z wykonywaniem pracy na podstawie 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, w ramach którego uzyskano informację o naruszeniu prawa oraz istnieje możliwość doświadczenia działań odwetowych.

III – Zgłaszanie nieprawidłowości

§ 5

1. Kanały zgłoszeń:

a) Zgłoszenia wewnętrzne – sygnaliści mogą zgłaszać nieprawidłowości za pośrednictwem adresu e-mail: naruszenia@proaxia-consulting.com. Szczegółowy tryb postępowania w ramach procedury zgłoszeń wewnętrznych został określony w rozdziale IV niniejszej procedury.
b) Ponadto, sygnaliści mogą zgłaszać nieprawidłowości poprzez zgłoszenie kanałem zewnętrznym – należy przez to rozumieć ustne lub pisemne przekazanie Rzecznikowi Praw Obywatelskich albo organowi publicznemu informacji o naruszeniu prawa. Zasady ochrony sygnalisty dokonującego zgłoszenia kanałem zewnętrznym określa Ustawa o Ochronie Sygnalistów.
c) Ponadto, w szczególnych przypadkach sygnaliści mogą zgłaszać nieprawidłowości poprzez ujawnienie publiczne. Zasady ochrony sygnalisty dokonującego ujawnienia publicznego określa Ustawa o Ochronie Sygnalistów.

2. Zgodnie z przepisami Ustawy o ochronie sygnalistów, podmiot zapewnia możliwość dokonywania zgłoszeń wewnętrznych oraz zachęca do korzystania z tej procedury w pierwszej kolejności, z zastrzeżeniem prawa sygnalisty do skorzystania z innych kanałów zgłoszeń przewidzianych przepisami prawa.

IV – Procedura i zasady dokonywania zgłoszeń wewnętrznych

§ 6

1. Zgłoszenie naruszenia – zgłoszenia wewnętrznego należy dokonać za pośrednictwem dedykowanego adresu e-mail: naruszenia@proaxia-consulting.com. Zgłoszenie powinno zostać dokonane przy użyciu Formularza Zgłoszenia Sygnalisty, stanowiącego Załącznik nr 1 do niniejszej Procedury. Formularz należy pobrać, wypełnić offline, a następnie podpisany przesłać drogą elektroniczną na wskazany adres.
    a) Wszystkie zgłoszenia kierowane na wskazany adres będą przyjmowane i obsługiwane wyłącznie przez upoważniony zespół ds. obsługi zgłoszeń.
    b) Firma nie przyjmuje zgłoszeń anonimowych.
2. Przyjęcie zgłoszenia i jego rejestracja

a) Po otrzymaniu zgłoszenia zespół ds. obsługi zgłoszeń dokonuje jego rejestracji w rejestrze zgłoszeń wewnętrznych, prowadzonym w sposób zapewniający dostęp do danych osobowych sygnalisty oraz osób wskazanych w zgłoszeniu wyłącznie członkom tego zespołu, z zachowaniem zasad poufności i ochrony tych danych. Każdemu zgłoszeniu nadawany jest indywidualny numer referencyjny.
b) Rejestr zgłoszeń wewnętrznych zawiera w szczególności:
    i. datę i godzinę otrzymania zgłoszenia,
    ii. przedmiot zgłoszenia oraz wskazanie naruszenia prawa,
    iii. dane sygnalisty umożliwiające kontakt.
c) Do rozpatrzenia zgłoszenia oraz przeprowadzenia postępowania wyjaśniającego wymagany jest udział co najmniej dwóch członków zespołu ds. obsługi zgłoszeń, przy czym żadna z tych osób nie może pozostawać w konflikcie interesów w związku ze zgłoszeniem.
    i. W przypadku, gdy zgłoszenie dotyczyłoby członków zespołu ds. obsługi zgłoszeń, sygnalista dokonuje zgłoszenia poprzez dedykowany kanał (naruszenia@proaxia-consulting.com) jednak może dołączyć do adresatów wyznaczonego pełnomocnika oddziału w Polsce, który nie jest członkiem zespołu ds. obsługi zgłoszeń z jednoczesnym oznaczeniem wiadomości w tytule: „*Zgłoszenie wymagające procedury zastępczej*". W takim wypadku:
        A. Członkowie zespołu ds. obsługi zgłoszeń są zobowiązani do powstrzymania się od podejmowania jakichkolwiek działań w sprawie (w tym otwierania otrzymanej wiadomości) do czasu wyznaczenia osób odpowiedzialnych za jej prowadzenie.
        B. Pełnomocnik oddziału dokonuje wstępnej oceny zgłoszenia i podejmuje decyzję co do dalszego trybu postępowania, w szczególności:
            a. przeprowadzenia postępowania wyjaśniającego wraz z wyznaczonym przez niego członkiem zespołu ds. obsługi zgłoszeń;
            b. przekazania sprawy do niezależnego podmiotu zewnętrznego, w szczególności kancelarii prawnej lub innego wyspecjalizowanego podmiotu, zapewniającego bezstronność i poufność.
        C. W przypadku, gdy zgłoszenie dotyczy członków zespołu ds. obsługi zgłoszeń, osoby te nie uczestniczą w żadnym etapie rozpatrywania zgłoszenia ani postępowania wyjaśniającego.
    ii. W każdym przypadku postępowanie prowadzone jest z zachowaniem zasad niezależności, poufności oraz ochrony sygnalisty, zgodnie z przepisami ustawy o ochronie sygnalistów.

3. Informacja dla sygnalisty – zespół ds. obsługi zgłoszeń przekazuje sygnaliście potwierdzenie przyjęcia zgłoszenia za pośrednictwem adresu e-mail, z którego zgłoszenie zostało przesłane, w terminie 7 dni od dnia jego otrzymania.
4. Wstępna weryfikacja zgłoszenia – po zarejestrowaniu zgłoszenia zespół ds. obsługi zgłoszeń przeprowadza wstępną ocenę zgłoszenia, obejmującą przede wszystkim sprawdzenie czy zgłoszenie dotyczy naruszenia prawa w rozumieniu ustawy o ochronie sygnalistów. W razie niejasności lub braków informacyjnych zespół może zwrócić się do sygnalisty o uzupełnienie informacji.
5. Decyzja po wstępnej weryfikacji – na podstawie wyników wstępnej weryfikacji zespół podejmuje decyzję:
    a) o rozpoczęciu pełnego postępowania wyjaśniającego,

b) o archiwizacji zgłoszenia w przypadku braku podstaw do dalszego działania, z odnotowaniem uzasadnienia w rejestrze.

6. Rozpoczęcie postępowania wyjaśniającego – w przypadku stwierdzenia, że zgłoszenie spełnia warunki do jego rozpatrzenia zespół ds. obsługi zgłoszeń rozpoczyna pełne postępowanie wyjaśniające, mające na celu ustalenie faktów oraz ocenę naruszenia prawa. Postępowanie obejmuje w szczególności:
   a) zebranie i analizę dowodów,
   b) wyjaśnienia osób objętych zgłoszeniem (w granicach przepisów prawa),
   c) kontakt z sygnalistą w celu uzupełnienia informacji.
7. Ocena wyników postępowania wyjaśniającego – po zakończeniu wszystkich spotkań i działań w ramach postępowania wyjaśniającego oraz po przeglądzie zgromadzonych informacji, zespół ds. obsługi zgłoszeń dokonuje oceny ustaleń, aby określić odpowiedni wynik postępowania. Ocena obejmuje w szczególności:
   a) potwierdzenie czy zgłoszenie faktycznie wskazuje na naruszenie prawa,
   b) analizę dowodów i informacji zebranych podczas postępowania,
   c) określenie rekomendacji dotyczących dalszych działań, w tym działań naprawczych i zapobiegawczych,
   d) przygotowanie raportu końcowego, który stanowi podstawę do informacji zwrotnej dla sygnalisty oraz do wdrożenia działań następczych (jeśli w toku postępowania wyjaśniającego ustalono wystąpienie naruszenia prawa).
8. Informacja zwrotna dla sygnalisty
   a) Maksymalny termin na przekazanie sygnaliście informacji zwrotnej o efektach postępowania wyjaśniającego nie może przekroczyć 3 miesięcy od dnia potwierdzenia przyjęcia zgłoszenia wewnętrznego.
   b) Informacja zwrotna jest przekazywana sygnaliście w sposób zapewniający poufność jego tożsamości oraz bezpieczeństwo danych, za pośrednictwem bezpiecznego kanału komunikacji wskazanego w procedurze tj. w formie elektronicznej na wskazany w zgłoszeniu adres e-mail, umożliwiając tym samym dokumentację przekazania.
9. Działania naprawcze – po zakończeniu postępowania wyjaśniającego zespół ds. obsługi zgłoszeń podejmuje niezwłocznie odpowiednie działania naprawcze, w tym w szczególności:
   a) rekomenduje działania korygujące w firmie, mające na celu usunięcie nieprawidłowości,
   b) rekomenduje działania zapobiegawcze w celu ograniczenia ryzyka powtórzenia naruszenia,
   c) zawiadamia właściwe organy publiczne, jeśli przepisy prawa nakładają taki obowiązek.
10. Oficjalne zakończenie obsługi zgłoszenia – po zakończeniu postępowania wyjaśniającego, przekazaniu informacji zwrotnej sygnaliście oraz wdrożeniu lub zaplanowaniu działań naprawczych, zespół ds. obsługi zgłoszeń dokonuje formalnego zamknięcia sprawy.
11. Dokumentacja i archiwizacja – informacje w rejestrze zgłoszeń wewnętrznych (w tym dokumentacja związana ze zgłoszeniem, raport końcowy, działania następcze oraz informacje przekazane sygnaliście) są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze lub postępowania zainicjowane tymi działaniami.

V – Ochrona sygnalisty

§ 7

1. Zakres ochrony – sygnalista podlega ochronie przed działaniami odwetowymi od momentu dokonania zgłoszenia, pod warunkiem, że miał uzasadnione podstawy sądzić, iż przekazywane informacje o naruszeniu prawa są prawdziwe w chwili dokonania zgłoszenia oraz że informacja ta stanowiła informację o naruszeniu prawa w rozumieniu ustawy. Sygnalista, zgłaszając

nieprawidłowość, będącą w sprzeczności z prawem musi wykonać to w dobrej wierze. Aby być chronionym, sygnalista musi mieć uzasadnione przypuszczenia, że zgłaszane informacje są prawdziwe.

a) Zgodnie z obowiązującymi przepisami, w tym art. 57 ustawy o ochronie sygnalistów, dokonanie zgłoszenia lub ujawnienia publicznego, ze świadomością, że do naruszenia prawa nie doszło, może skutkować odpowiedzialnością karną.

2. Zakaz działań odwetowych – zabrania się podejmowania wobec sygnalisty jakichkolwiek działań odwetowych, w tym prób lub gróźb ich zastosowania, w związku z dokonaniem zgłoszenia lub ujawnieniem publicznym o naruszeniu prawa.
    a) Zakaz ten obejmuje w szczególności działania skutkujące niekorzystnym traktowaniem, takie jak nieuzasadnione rozwiązanie lub zmiana warunków stosunku pracy, nieuzasadnione obniżenie wynagrodzenia, nieuzasadnione pominięcie przy awansowaniu, nieuzasadniona negatywna ocena pracy, mobbing lub dyskryminacja.
    b) W przypadku podjęcia wobec sygnalisty działań mogących stanowić działania odwetowe przyjmuje się, że są one związane ze zgłoszeniem, chyba że podmiot (firma) wykaże, iż zostały podjęte z przyczyn niezwiązanych ze zgłoszeniem.
3. Ochrona poufności tożsamości – podmiot zapewnia, że procedura zgłoszeń wewnętrznych oraz przetwarzanie danych związanych ze zgłoszeniami uniemożliwiają dostęp do informacji osobom nieupoważnionym oraz gwarantują ochronę poufności tożsamości sygnalisty, osoby, której dotyczy zgłoszenie, oraz osób trzecich wskazanych w zgłoszeniu, z wyjątkiem przypadków, w których ujawnienie tych danych jest niezbędne właściwym organom publicznym lub podmiotom świadczącym usługi prawne lub doradcze, zgodnie z obowiązującymi przepisami prawa.
    a) Czynności związane z przyjmowaniem i rozpatrywaniem zgłoszeń, podejmowaniem działań następczych oraz przetwarzaniem danych mogą być wykonywane wyłącznie przez osoby pisemnie upoważnione, zobowiązane do zachowania poufności także po ustaniu stosunku pracy lub innego stosunku prawnego.
4. Zgłaszanie działań odwetowych – sygnalista, który uzna, że wobec niego podjęto działania odwetowe, próby ich zastosowania lub groźby takich działań w związku z dokonanym zgłoszeniem, ma prawo zgłosić ten fakt za pośrednictwem kanału przewidzianego w rozdziale IV niniejszej procedury. W takim wypadku w tytule wiadomości należy wskazać: „*Zgłoszenie działań odwetowych*”.
    a) Zgłoszenia dotyczące działań odwetowych są przyjmowane i rozpatrywane niezwłocznie, z zachowaniem poufności tożsamości sygnalisty oraz zasad ochrony wynikających z ustawy o ochronie sygnalistów. Każde zgłoszenie otrzymuje odrębny numer w rejestrze zgłoszeń wewnętrznych wraz ze wskazaniem, którego zgłoszenia sygnalistycznego dotyczy.
    b) W przypadku potwierdzenia wystąpienia działań odwetowych podejmowane są odpowiednie działania naprawcze i dyscyplinujące, zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami podmiotu.

VI – Odpowiedzialność za naruszenie procedury

§ 8

1. Naruszenie procedury, w tym działania utrudniające zgłoszenie, naruszenie terminów, brak bezstronności, ujawnienie poufnych danych lub niewłaściwe przetwarzanie informacji, może skutkować odpowiedzialnością dyscyplinarną, naprawczą lub prawną wobec osoby odpowiedzialnej. Rodzaj i zakres działań zależą od wagi naruszenia oraz skutków dla sygnalisty i organizacji.

2. Odpowiedzialność za naruszenie ochrony sygnalisty – naruszenie zasad ochrony sygnalisty, w tym zakazu działań odwetowych lub poufności tożsamości, stanowi naruszenie procedury i może skutkować odpowiedzialnością służbową, dyscyplinarną lub karną.
    a) Każde podejrzenie naruszenia jest niezwłocznie badane, a wyniki postępowania stanowią podstawę do podjęcia odpowiednich działań, w tym:
        i. działań dyscyplinujących np. upomnienie, nagana;
        ii. działań naprawczych np. przywrócenie praw sygnalisty, korekta decyzji lub procedur;
        iii. działań prawnych np. dochodzenie odszkodowania lub zgłoszenie naruszenia do organów państwowych.
    b) Wszystkie przypadki są dokumentowane, a wnioski wykorzystywane do zapobiegania podobnym naruszeniom w przyszłości.

VII – Dane osobowe

§ 9

1. Zakres przetwarzania danych
    a) Firma po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia oraz 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.
    b) 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 zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami lub przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następczych.
    c) Dostęp do danych mają wyłącznie osoby upoważnione, posiadające pisemne pełnomocnictwo, w zakresie niezbędnym do realizacji procedury. Wszystkie osoby przetwarzające dane są zobowiązane do zachowania poufności również po zakończeniu stosunku pracy lub innego stosunku prawnego.

VIII – Postanowienia końcowe

§ 10

1. Wejście w życie procedury – procedura wchodzi w życie z dniem 12.06.2026.
2. Obowiązek przestrzegania procedury - pracownicy firmy oraz inne osoby wykonujące pracę na jej rzecz, (w zakresie wynikającym z zawartych umów) są zobowiązani do przestrzegania zasad niniejszej procedury oraz do współpracy w toku postępowań wyjaśniających. Naruszenie procedury może skutkować odpowiedzialnością zgodnie z jej zapisami.
3. Aktualizacja procedury – procedura podlega okresowej weryfikacji i aktualizacji w celu zapewnienia zgodności z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami organizacji.
4. Poufność i przechowywanie dokumentacji – wszystkie dokumenty związane ze zgłoszeniami sygnalistów są przechowywane zgodnie z zasadami poufności i bezpieczeństwa danych obowiązującymi w organizacji.
5. Kontakt – wszelkie pytania dotyczące procedury można kierować do zespołu HR i administracji (oddział Polska) poprzez adres e-mail: officepl@proaxia-consulting.com.

IX – Wykaz załączników

- Załącznik nr 1 – Formularz Zgłoszenia Sygnalisty
- Załącznik nr 2 – komunikat RODO dla osoby, która zgłasza naruszenie.

Wrocław, dn. 12.06.2026
proaxia consulting group ag Oddział w Polsce

Załącznik 1 - Formularz Zgłoszenia Sygnalisty

1. Imię i nazwisko osoby dokonującej zgłoszenia:
……

2. Dane kontaktowe:
……
……
……

3. Data oraz miejsce zaistnienia nieprawidłowości lub data i miejsce pozyskania informacji o nieprawidłowościach:
……
……
……

4. Opis sytuacji lub okoliczności, które doprowadziły lub mogą doprowadzić do wystąpienia nieprawidłowości:
……
……
……

5. Wskazanie osoby, której dotyczy zgłoszenie:
……
……
……

6. Wskazanie ewentualnych świadków:
……
……
……

7. Wskazanie ewentualnych dowodów i informacji, jakimi dysponuje zgłaszający, które mogą okazać się pomocne w procesie rozpatrywania nieprawidłowości:

……
……
……

Data i czytelny podpis osoby dokonującej zgłoszenia

……

Załącznik nr 2 – komunikat RODO dla osoby, która zgłasza naruszenie.

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), informujemy, że:

1. Administrator danych – administratorem danych osobowych przetwarzanych w związku ze zgłoszeniem naruszenia prawa jest proaxia consulting group ag Oddział w Polsce z siedzibą we Wrocławiu, przy ul. Strzegomskiej 138.
2. Cele i podstawa prawna przetwarzania – w związku z przepisami ustawy z dnia 14 czerwca 2024 o ochronie sygnalistów, dane osobowe są przetwarzane w celu prowadzenia wewnętrznego postępowania wyjaśniającego w tym: podjęcia działań związanych z ustaleniem, czy będące przedmiotem zgłoszenia działanie lub zaniechanie stanowi rzeczywiste lub potencjalne naruszenie przepisów prawa, zapobiegania występowaniu nieprawidłowości, ustalenia okoliczności, w jakich do naruszenia doszło lub mogłoby dojść, dokonania czynności zmierzających do rozstrzygnięcia sprawy, w szczególności:

   a) przyjęcia zgłoszenia naruszenia prawa,
   b) weryfikacji zgłoszenia oraz prowadzenia działań następczych,
   c) prowadzenia postępowań wyjaśniających,
   d) prowadzenia działań naprawczych, korygujących oraz zapobiegawczych.

3. Odbiorcy danych – dane mogą być udostępniane:

   a) upoważnionym pracownikom i współpracownikom administratora
   b) podmiotom i osobom obsługującym kanał zgłoszeń,
   c) podmiotom świadczącym usługi prawne lub doradcze,
   d) organom publicznym uprawnionym do ich otrzymania na podstawie przepisów prawa, którym firma proaxia consulting group ag Oddział w Polsce przekazała sprawę.

4. Okres przechowywania danych – dane osobowe są przechowywane przez okres niezbędny do realizacji działań następczych, a następnie przez okres wynikający z przepisów prawa, nie dłużej niż 3 lata po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami lub przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następczych.

5. Prawa osoby, której dane dotyczą – Osobie, której dane dotyczą, przysługuje prawo do:

   a) dostępu do danych,
   b) sprostowania danych,
   c) ograniczenia przetwarzania danych,
   d) usunięcia danych w przypadkach przewidzianych prawem,
   e) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

6. Poufność i ochrona tożsamości – Administrator zapewnia poufność danych sygnalisty oraz osób wskazanych w zgłoszeniu. Dane mogą być ujawnione wyłącznie w zakresie niezbędnym do realizacji działań określonych w niniejszej procedurze, w tym działań następczych, wyjaśniających i naprawczych, oraz właściwym organom publicznym lub podmiotom świadczącym usługi prawne lub doradcze. Tożsamość sygnalisty podlega ochronie zgodnie z ustawą o ochronie sygnalistów,

chyba że sygnalista wyrazi zgodę na jej ujawnienie lub ujawnienie jest wymagane przepisami prawa.

7. Dobrowolność podania danych – Podanie danych osobowych jest dobrowolne, jednak niezbędne do rozpatrzenia zgłoszenia i prowadzenia działań następczych.

Whistleblowing Procedure for Internal Reporting and Follow-Up Actions at proaxia consulting group ag | Oddział w Polsce

Table of contents:

In the event of any discrepancies or ambiguities, the Polish language version shall prevail and be legally binding.

I – Purpose and definitions

§ 1

1. The legal basis for the implementation of the Internal Reporting and Follow-Up Procedure is Polish Act of 14 June 2024 on the Protection of Whistleblowers *(Ustawa o ochronie sygnalistów,* 14 June 2024).
2. The purpose of the Internal Reporting and Follow-Up Procedure is to ensure a safe and confidential mechanism for reporting irregularities, to protect whistleblowers against retaliatory actions, and to enable the organization to effectively identify and eliminate violations of law.

§ 2

The terms used in this Procedure shall have the following meanings:

1. **Procedure** – the Internal Reporting and Follow-Up Procedure – a set of rules, regulations, and organizational measures applicable within proaxia consulting group ag Branch in Poland, defining the method for receiving, registering, verifying, examining, and documenting reports concerning violations of law, as well as the procedure for providing feedback to the whistleblower and the principles for protecting reporting persons against retaliatory actions.
2. **Employer or Company** – proaxia consulting group ag Branch in Poland, represented by the Branch Representative in Poland.
3. **Employee** – a person employed by the Employer under an employment relationship.
4. **Whistleblower** – a person making a report of irregularities, acting in good faith, and having reasonable grounds to believe that the information about a violation of law is true at the time of reporting. A whistleblower is any person associated with the Company who identifies breaches of legal norms while performing their professional duties
5. **Whistleblower Reporting Team** – persons authorized to receive reports of violations, maintain a register of reports, propose and take follow-up actions, and provide feedback to whistleblowers, acting with confidentiality, impartiality, and in accordance with the Act of 14 June 2024 on the Protection of Whistleblowers and this Procedure.
6. **Report** – the submission, through the established internal reporting channel, of information regarding an actual or potential violation of law.
7. **Violation** – any act or omission that is contrary to generally applicable laws or intended to circumvent the law, which may cause harm to the organization, its employees, contractors, clients, or the public interest.
8. **Retaliatory Actions** – any unlawful or unjustified act or omission in a work-related context, taken against the Whistleblower in connection with a report made by them, which causes or may cause unjustified harm to the Whistleblower.
9. **Internal Reporting Channel** – an organized tool or procedure established by the Company that ensures confidentiality and is used to report information about a breach of law to a Company, including a dedicated email address.
10. **Follow-Up Actions** – all activities undertaken by the Company after receiving a report, including analysing the report, conducting an inquiry, taking corrective, remedial, or disciplinary measures, and providing feedback to the whistleblower in accordance with applicable regulations. Follow-up actions

are carried out in order to assess the veracity of the information contained in the report and to prevent the legal violation that is the subject of the report.

11. **Confidentiality** – the principle ensuring that the identity of the whistleblower, the persons identified in the report, and all information contained in the report are protected and may be disclosed only to persons and entities authorized to process them under applicable law or internal regulations.
12. **Polish Whistleblower Protection Act** – the Act of 14 June 2024 (Journal of Laws 2024, item 928), which regulates the rules for reporting legal violations and provides protection to persons reporting such violations (whistleblowers).

II – Scope of violations and persons covered by the procedure

§ 3

4. Reported Violations – the Procedure covers reports of actual or suspected violations of law within the scope defined by the Whistleblower Protection Act. Reports may concern violations of law related to:

    a) public procurement,
    b) financial services, products, and markets, as well as prevention of money laundering and terrorist financing,
    c) product safety,
    d) transport safety,
    e) environmental protection,
    f) radiological protection and nuclear safety
    g) food and feed safety, animal health and welfare
    h) public health,
    i) consumer protection
    j) privacy and personal data protection,
    k) the security of network and information systems,
    l) violations affecting the financial interests of the European Union
    m) violations related to the internal market, including competition rules, state aid, and corporate taxation rules.

§ 4

5. Scope of Application – the procedure applies to all persons entitled to make reports under the Whistleblower Protection Act, reporting information about a legal violation obtained in a work-related context, including:
    a) employees,
    b) persons performing work under a basis other than employment, including civil law contracts,
    c) persons working under the supervision and management of a contractor, subcontractor, or supplier,
    d) entrepreneurs, contractors and business partners,
    e) shareholders and partners,
    f) members of the governing bodies,
    g) interns and trainees,
    h) volunteers,
    i) former employees and persons whose employment or cooperation has ended,

j) candidates applying for employment or cooperation who obtained information about violations during recruitment, interviews, or negotiations.

6. Work-Related Context – refers to past, present or future actions related to the performance of work under an employment relationship or any other legal relationship constituting the basis for the provision of work or services, or the performance of functions within or for the legal entity, or the performance of service within the legal entity, in the course of which information about a breach of law was obtained and there is a possibility of experiencing retaliatory actions.

III – Incident reporting

§ 5

3. Reporting Channels:
    a. Internal Reports – Whistleblowers may report irregularities via the email address: naruszenia@proaxia-consulting.com.
        i. The detailed procedure for handling reports under the internal reporting process is set out in Chapter IV of this Procedure.
    b. External Reports – Whistleblowers may also report irregularities through an external channel, meaning the oral or written submission of information about a legal violation to the Ombudsman or a public authority. The rules for protecting whistleblowers making reports via an external channel are defined by the Polish Whistleblower Protection Act.
    c. Public Disclosures – In exceptional cases Whistleblowers may additionally report irregularities through public disclosure. The rules for protecting whistleblowers making public disclosures are defined by the Polish Whistleblower Protection Act.
4. In accordance with the provisions of the Whistleblower Protection Act, the Company provides the possibility to make internal reports and encourages their use as the first option, without prejudice to the whistleblower's right to use other reporting channels provided by law.

IV – Internal reporting procedure and principles

§ 6

1. Reporting a Violation – Internal reports should be submitted via the dedicated email address: naruszenia@proaxia-consulting.com. Reports should be made using the Whistleblower Report Form, attached as Annex 1 to this Procedure. The form must be downloaded, completed offline, signed and then sent electronically to the designated email address.
    a. All reports sent to the designated address will be received and handled exclusively by the authorized Whistleblower Reporting Team.
    b. The Company does not accept anonymous reports.
2. Receipt and Registration of a Report
    a. Upon receipt of a report, the whistleblowing handling team registers it in the internal reporting register, maintained in a manner that ensures access to the personal data of the whistleblower and persons indicated in the report is restricted exclusively to members of this team, while maintaining confidentiality and protecting such data. Each report is assigned a unique reference number.
    b. The internal reports register shall include:
        i. the date and time the report was received,
        ii. the subject of the report and the identification of the violation,
        iii. the contact details of the whistleblower.

c. The examination of a report and the conduct of an inquiry require the participation of at least two members of the Whistleblower Reporting Team, none of whom may have a conflict of interest related to the report.
    i. In the event that the report concerns members of the Whistleblower Reporting Team, the whistleblower shall submit the report via the dedicated channel (naruszenia@proaxia-consulting.com). The whistleblower may additionally include in the recipients a designated proxy of the Polish branch who is not a member of the reporting handling team, while simultaneously marking the subject line of the message as: *'Report requiring an alternative procedure'*. In such case:
        A. Members of the reporting handling team are obliged to refrain from taking any actions in the matter (including opening the received email) until the persons responsible for handling the case have been designated.
        B. The proxy of the branch conducts an initial assessment of the report and decides on the further course of action, in particular:
            a. initiating an investigative procedure together with a member of the reporting handling team designated by them;
            b. referring the case to an independent external entity, in particular a law firm or another specialised entity, ensuring impartiality and confidentiality to conduct the inquiry independently;
        C. Where the report concerns members of the reporting handling team, such persons shall not participate in any stage of the review of the report or the investigative procedure.
    ii. In all cases, the inquiry shall be conducted in accordance with the principles of independence, confidentiality, and whistleblower protection, in line with the provisions of the Polish Whistleblower Protection Act.

3. Information for the Whistleblower – The Whistleblower Reporting Team provides the whistleblower with confirmation of receipt of the report via the email address from which the report was submitted, within 7 days of its receipt.
4. Preliminary Verification of the Report – After the report is registered, the Whistleblower Reporting Team conducts a preliminary assessment of the report, primarily to verify whether the report concerns a violation of law within the meaning of the Polish Whistleblower Protection Act. In case of ambiguities or missing information, the team may contact the whistleblower to request additional details.
5. Decision After Preliminary Verification – Based on the results of the preliminary verification, the team decides:
    a. to initiate a full investigation;
    b. to archive the report if there are no grounds for further action, with the justification recorded in the register.
6. Initiation of the Investigation – if it is determined that the report meets the criteria for consideration, the Whistleblower Reporting Team shall initiate a full investigation aimed at establishing the facts and assessing any legal violations. The investigation shall include:
    a. collection and analysis of evidence;
    b. obtaining explanations from the individuals involved in the report (within the limits of applicable law);
    c. contacting the whistleblower to obtain additional information.
7. Assessment of Investigation Results – after the completion of all meetings and actions within the investigation, and following a review of the collected information, the Whistleblower Reporting Team shall assess the findings to determine the appropriate outcome of the investigation. The assessment shall include:
    a. confirmation of whether the report indeed indicates a legal violation;

   b. analysis of the evidence and information collected during the investigation;
   c. recommendations for further actions, including corrective and preventive measures;
   d. preparation of a final report, which serves as the basis for providing feedback to the whistleblower and for implementing follow-up actions (if a violation was identified).
8. Feedback to the Whistleblower
   a. The maximum timeframe for providing the whistleblower with feedback on the outcome of the investigation shall not exceed three months from the date of confirmation of receipt of the internal report.
   b. Feedback shall be provided to the whistleblower in a manner that ensures the confidentiality of their identity and the security of the data, through a secure communication channel specified in this procedure, i.e., electronically to the email address provided in the report, thereby allowing documentation of the feedback delivery.
9. Follow-up Actions – upon the conclusion of the investigation, the Whistleblower Reporting Team shall promptly undertake appropriate follow-up actions, including:
   a. recommendation of corrective or remedial actions within the company aimed at eliminating irregularities;
   b. recommendation of preventive actions to mitigate the risk of recurrence of the violation;
   c. notification of the relevant public authorities, if required by law.
10. Official closure of the report – after the conclusion of the investigation, the provision of feedback to the whistleblower, and the implementation or planning of follow-up actions, the Whistleblower Reporting Team shall formally close the case.
11. Documentation and archiving – information in the internal reports register (including documentation related to the report, the final report, follow-up actions, and information provided to the whistleblower) shall be retained for a period of three years following the end of the calendar year in which the follow-up actions or the proceedings initiated by such actions were completed.

V – Whistleblower protection

§ 7

1. Scope of Protection – A whistleblower shall be protected against retaliatory actions from the moment the report is made, provided that they had reasonable grounds to believe that the information disclosed regarding a violation was true at the time of reporting and that such information constituted a reportable violation under the Polish Whistleblower Protection Act. When reporting a violation that conflicts with legal provisions, the whistleblower must act in good faith. To be protected, the whistleblower must have a reasonable belief that the information reported is accurate.
   a. In accordance with applicable laws, including Article 57 of the Whistleblower Protection Act, making a report or public disclosure while being aware that no breach of law has occurred may result in criminal liability
2. Prohibition of retaliatory actions – any form of retaliatory action against a whistleblower, including attempts or threats to carry out such actions, in connection with making a report or disclosing information about a violation, is strictly prohibited.
   a. This prohibition specifically includes actions resulting in adverse treatment, such as unjustified termination or unjustified modification of employment conditions, unjustified reduction of remuneration, unjustified denial of promotion, unjustified negative performance evaluation, harassment, or discrimination.
   b. If actions are taken against the whistleblower that could constitute retaliation, they shall be presumed to be related to the report unless the company demonstrates that such actions were taken for reasons unrelated to the report.

3. Protection of identity confidentiality – The company shall ensure that the internal reporting procedure and the processing of report-related data prevent access by unauthorized persons and guarantee the confidentiality of the identity of the whistleblower, the individual concerned by the report, and any third parties mentioned in the report, except where disclosure is necessary to competent public authorities or external legal or advisory service providers, in accordance with applicable law.
    a. Activities related to receiving and handling reports, undertaking follow-up actions, and processing data may only be performed by individuals who are authorized and obligated to maintain confidentiality, including after the termination of employment or any other legal relationship.
4. Reporting Retaliatory Actions – A whistleblower who believes that retaliatory actions, attempts to retaliate, or threats of such actions have been taken against them in connection with a report has the right to report this through the channel specified in Chapter IV of this procedure.
    a. Reports concerning retaliatory actions shall be received and handled promptly, ensuring the confidentiality of the whistleblower's identity and the protection principles established under the Whistleblower Protection Act. Each report is assigned a separate number in the internal reports register, together with an indication of the whistleblowing report to which it relates.
    b. If retaliatory actions are confirmed, appropriate corrective and disciplinary measures shall be taken in accordance with applicable law and the entity's internal regulations.

VI – Consequences of breaching the procedure

§ 8

1. Violation of the Procedure – Any breach of this procedure, including actions that hinder reporting, failure to meet deadlines, lack of impartiality, disclosure of confidential information, or improper processing of information, may result in disciplinary, corrective, or legal action against the responsible individual. The type and scope of such measures shall depend on the severity of the violation and its impact on the whistleblower and the organization.
2. Responsibility for Violating Whistleblower Protection – Any breach of the principles of whistleblower protection, including the prohibition of retaliatory actions or the confidentiality of the whistleblower's identity, shall constitute a violation of the procedure and may result in administrative, disciplinary, civil, or criminal liability.
    a. Any suspected violation shall be promptly investigated, and the results of the investigation shall form the basis for taking appropriate actions, including:
        i. disciplinary actions, e.g., warning, reprimand;
        ii. corrective actions, e.g., restoration of the whistleblower's rights, correction of decisions or procedures;
        iii. legal actions, e.g., claiming damages or reporting the violation to public authorities.
    b. All cases shall be documented, and the findings shall be used to prevent similar violations in the future.

VII – Processing of personal data

§ 9

1. Scope of data processing
    a. Upon receipt of a report, the Company processes personal data only to the extent necessary to receive the report or to undertake any follow-up actions. Personal data that is irrelevant to the handling of the report shall not be collected, and if collected inadvertently, shall be deleted without undue delay. Such personal data shall be deleted within 14 days from the moment it is determined that it is not relevant to the case.

b. Personal data processed in connection with the receipt of a report or the undertaking of follow-up actions, as well as documents related to such report, shall be retained by the legal entity and the public authority for a period of three years following the end of the calendar year in which follow-up actions were completed, or proceedings initiated by such actions were concluded, or the external report was transmitted to the competent public authority for follow-up actions.
c. Access to personal data shall be granted exclusively to authorized individuals holding written authorization, to the extent necessary for the implementation of the procedure. All individuals processing personal data are obligated to maintain confidentiality, including after the termination of employment or any other legal relationship.

VIII –Final provisions

§ 10

1. Entry into Force of the Procedure – This procedure shall enter into force on 12.06.2026.
2. Obligation to Comply with the Procedure – Employees of the Company and, to the extent resulting from concluded agreements, other persons performing work for its benefit, are obliged to comply with the rules of this procedure and to cooperate in the course of investigative proceedings. A breach of the procedure may result in liability in accordance with its provisions.
3. Procedure Updates – This procedure shall be subject to periodic review and updates to ensure compliance with applicable laws and the organization's internal regulations.
4. Confidentiality and Record Retention – All documents related to whistleblower reports shall be stored in accordance with the confidentiality and data security principles applicable within the organization.
5. Contact – Any questions regarding the procedure may be directed to the HR and Administration team (Polish branch) via the following email address: officepl@proaxia-consulting.com

IX – List of appendices

- Appendix No. 1 – Whistleblower Report Form
- Appendix No. 2 – GDPR Information Notice for the Reporting Person

Appendix No. 1 – Whistleblower Report Form

1. Full name of the person making the report:
   ……
   ……
   ……
2. Contact data:
   ……
   ……
   ……
3. Date and place of the occurrence of the irregularities, or the date and place where the information about the irregularities was obtained:
   ……
   ……
   ……
4. Description of the situation or circumstances that led or may lead to the occurrence of irregularities:
   ……
   ……
   ……
5. Name of the person concerned by the report:
   ……
   ……
   ……
6. Names of any potential witnesses:
   ……
   ……
   ……
7. Any evidence or information the reporting person has that may be helpful in reviewing the irregularities:
   ……
   ……
   ……

Date and signature of the person making the report:

……..

Appendix No. 2 – GDPR information notice for the reporting person

In accordance with Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), we inform you that:

1. Data Controller

The controller of personal data processed in connection with the report of a breach of law is proaxia consulting group ag oddział w Polsce, with its registered office in Wrocław, ul. Strzegomska 138.

2. Purposes and legal basis of processing

In connection with the provisions of the Act of 14 June 2024 on whistleblower protection, personal data are processed for the purpose of conducting an internal investigative procedure, including: determining whether the action or omission covered by the report constitutes an actual or potential breach of law, preventing irregularities, establishing the circumstances in which the breach occurred or could have occurred, and taking actions aimed at resolving the matter, in particular:

a) receiving the report of a breach of law,
b) verifying the report and conducting follow-up actions,
c) conducting investigative proceedings,
d) carrying out remedial, corrective and preventive actions.

3. Recipients of data

Data may be disclosed to:
a) authorised employees and collaborators of the controller,
b) entities and persons operating the reporting channel,
c) legal or advisory service providers,
d) public authorities entitled to receive the data under applicable law, to which proaxia consulting group ag Oddział w Polsce has referred the case.

4. Retention period

Personal data are stored for the period necessary to carry out follow-up actions, and thereafter for the period required by law, but not longer than 3 years after the end of the calendar year in which the follow-up actions were completed, or after completion of proceedings initiated by such actions, or after the report has been submitted to the competent public authority responsible for follow-up actions.

5. Rights of the data subject

The data subject has the right to:
a) access their data,
b) rectify their data,
c) restrict processing,
d) erasure of data in cases provided for by law,
e) lodge a complaint with the President of the Personal Data Protection Office.

6. Confidentiality and protection of identity

The Controller ensures the confidentiality of the whistleblower's data and the persons indicated in the report. Data may be disclosed only to the extent necessary for the performance of actions specified in this procedure, including follow-up, investigative and remedial actions, and in accordance with applicable law.

The whistleblower's identity is protected under the Whistleblower Protection Act, unless the whistleblower consents to its disclosure or disclosure is required by law.

7. Voluntary provision of data

Providing personal data is voluntary; however, it is necessary for the handling of the report and the conduct of follow-up actions.