PROCEDURA ZGŁOSZEŃ WEWNĘTRZNYCH W ETHOSENERGY POLAND S.A.

z dnia 18 września 2024 r.

1. WSTĘP

Ustawa o ochronie sygnalistów z dnia 14 czerwca 2024 r. implementuje do polskiego prawa Dyrektywę UE 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii i wprowadza obowiązek utworzenia procedur dokonywania zgłoszeń wewnętrznych o naruszeniach, które wystąpiły w kontekście związanym z pracą.

Ustawa o ochornie sygnalistów zapewnia istotne środki ochrony w zakresie poufności, ochrony przed wszelkimi formami odwetu, środki wsparcia i zapewnienia prywatności osobom, które pracując na rzecz spółki, chcą złożyć pisemne lub ustne zgłoszenie na temat określonych naruszeń prawa, o których dowiedziały się w swoim środowisku pracy.

Dodatkowo Ustawa o ochronie syganlistów jasno określa wymagania techniczne i organizacyjne dotyczące wewnętrznych i zewnętrznych procedur dokonywania zgłoszeń.

CEL I ZAKRES STOSOWANIA

EthosEnergy Poland S.A. (dalej "Spółka") stosując niniejszą procedurę (Procedurę zgłoszeń wewnętrznych) spełnia obowiązki Ustawy o ochronie sygnalistów.

Spółka pragnie wewnętrznie promować kulturę skutecznej komunikacji i dba o to, aby sygnaliści zgłaszając naruszenia, o których się dowiedzieli, w postaci działań, zaniechań czy zachowań niezgodnych z prawem, w znaczący sposób przyczynili się do doskonalenia własnej organizacji.

3. PRZEDMIOT ZGŁOSZENIA

3.1 Naruszenie przepisów Unii Europejskiej lub przepisów krajowych

Sygnalista może zgłosić zachowania, działania lub zaniechania niegodne z prawem lub mające na celu obejście prawa oraz godzące w uczciwość Spółki dotyczące:

- korupcji;
- zamówień publicznych;
- usług, produktów i rynków finansowych;
- przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;
- bezpieczeństwa produtków i ich zgodności z wymogami;
- bezpieczeństwa transportu;
- ochrony środowiska;
- ochrony radiologicznej i bezpieczeństwa jądrowego;
- bezpieczeństwa żywności i pasz;
- zdrowia i dobrostanu zwierząt,
- zdrowia publicznego;
- ochrony konsumentów;
- ochrony prywatności i danych osobowych;
- bezpieczeństwa sieci i systemów teleinformatycznych;
- interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, jednostki samorządu terytorlianego oraz Unii Europejskiej;
- rynku wewnętrznego Unii Europejskiej, w tym publicznoprawnych zasad konkurencji i pomocy państwa oraz opodatkowania osób prawnych;
- konstytucyjnych wolności praw człowieka i obywatela – występujące w stosunkach jednostki z organami władzy publicznej i niezwiązane z dziedzinami wskazanymi w w/w punktach.

3.2 Co nie może być przedmiotem zgłoszenia

Zgłoszeniu podlegają zachowania, działania lub zaniechania, które sygnalista zauważył w swoim środowisku pracy.

Nie można zgłaszać sporów, roszczeń lub żądań związanych z interesem osobistym sygnalisty, które dotyczą wyłącznie jego indywidualnych stosunków pracy lub są nieodłącznie związane z jego stosunkiem pracy z osobami podległymi organizacyjnie. Na przykład nie są objęte niniejszą procedurą zgłoszeń wewnętrznych, zgłoszenia dotyczące sporów pracowniczych i etapów przedsądowych, dyskryminacji wśród współpracowników, konfliktów interpersonalnych pomiędzy sygnalistą a innym pracownikiem lub z przełożonym.

W ramach niniejszej procedury zgłoszeń wewnętrznych, Spółka nie przewidziała również możliwości dodatkowego, zgłaszania informacji o naruszeniach dotyczących obowiązujących w Spółce regulacji wewnętrznych lub standardów etycznych, które zostały ustanowione przez Spółkę na podstawie przepisów prawa powszechnie obowiązującego i pozostają z nimi zgodne, tj. zgłoszeń o których mowa w art. 3 ust. 2 Ustawy o ochronie sygnalistów.

Niemnej jednak, sygnalista może zgłosić zachowania, działania lub zaniechania, które szkodzą integralności Spółki, mimo tego, że nie mieszczą się one w zakresie niniejszej procedury zgłoszeń wewnętrznych (jak wskazano w punkcie 3.1. powyżej), jeśli naruszają one wewnętrzne polityki lub procedury. Zgłoszenia takie, zostaną przekazane do Komisji Etyki Grupy w celu ich rozpatrzenia zgodnie z postanowieniami Kodeksu Etyki Grupy.

3.3 Elementy i cechy zgłoszenia

Zgłoszenia muszą być jak najbardziej precyzyjne i szczegółowe, aby umożliwić ocenę faktów osobom odpowiedzialnym za ich otrzymanie i rozpatrzenie.

Zgłoszenie powinno w szczególności zawierać:

- Datę i miejsce wystąpienia zdarzenia będącego przedmiotem zgłoszenia.
- Opis zdarzenia.
- Dane osobowe lub inne elementy umożliwiające identyfikację osoby, której można przypisać czyny zawarte w zgłoszeniu.
- Dane osobowe umożliwiające identyfikację innych osób potencjalnie świadomych naruszenia.

Przydatne jest także załączenie dostępnych dokumentów na poparcie zgłoszenia.

3.4 Kto może dokonać zgłoszenia

Do składania zgłoszeń, także anonimowych, uprawnione są wszystkie osoby, które pozyskały informacje w kontekście związanym z pracą, w tym:

- Pracownicy;
- Pracownicy tymczasowi;
- Osoby świadczace pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej;
- Przedsiębiorcy;
- Prokurenci;
- Akcjonariusze lub wspólnicy;
- Członkowie organu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej;

- Osoby świadczące pracę pod nadzorem i kierownictwem wykonawcy, podwykonwacy lub dostawcy;
- Stażyści;
- Wolontariusze;
- Praktykanci.

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

4. ZGŁOSZENIA WEWNĘTRZNE

4.1 Procedura zgłoszeń wewnętrznych

Spółka zgodnie z Ustawą o ochronie sygnalistów i po konsultacji z przedstawicielami organizacji związkowych uruchomiła swoją procedurę zgłoszeń wewnętrznych, zapewniając poufność w zakresie tożsamości sygnalisty oraz każdej innej osoby wymienionej w zgłoszeniu, a także w zakresie treści zgłoszenia i związanej z nim dokumentacji.

Spółka powołała **zespół odpowiedzialny za przyjmowanie zgłoszeń**, złożony ze:

1) Specjalisty ds. organizacji/Inspektora Ochrony Danych.
2) Radcy Prawnego (Senior Legal Counsel).

posiadających niezbędną wiedzę ekspercką (Zespół ds. zgłaszania nieprawidłowości).

Spółka do **podejmowania działań następczych** powołała:

Specjalistę ds. Organizacji/Inspektora Ochrony Danych,

który niezwłocznie informuje Przewodniczącego Komisji Etyki Grupy, który ewentualnie powołuje dodatkowych ekspertów.

Sposoby dokonywania zgłoszeń

Zgłoszenia można dokonywać we wszystkich językach przy użyciu następujących kanałów:

- W formie pisemnej za pośrednictwem platformy cyfrowej Navex, dostępnej pod następującym linkiem: https://secure.ethicspoint.eu/domain/media/en/gui/106568/index.html.
- Ustnie, 24/h na dobę, dzwoniąc pod numer Infolinii: 00 800 491 19 83
- Ustnie, składając wniosek o spotkanie osobiste lub wideokonferencję (np. Microsoft Teams), według uznania sygnalisty, zaplanowane w rozsądnym terminie, nie dłuższym niż 14 dni od dnia otrzymania takiego wniosku.

Prośbę o spotkanie można złożyć za pośrednictwem ww. kanałów.

Zgłoszenia dokonywane w ramach wewnętrznego kanału Spółki mogą być również dokonywane anonimowo.

Wszystkie zgłoszenia są traktowane i procedowane jednakowo, niezależnie od tego, czy sygnaliści zdecydują się ujawnić swoją tożsamość, czy też zgłoszenie zostanie złożone anonimowo.

Jeśli zgłoszenie dotyczy zdarzeń bezpośrednio związanych z członkiem Zespołu ds. zgłaszania nieprawidłowości, osoby powołanej do podejmowania działań następczych w Spółce lub kierownictwa wyższego szczebla np. Zarządu lub Rady Nadzorczej Spółki, zgłoszenie może zostać wysłane bezpośrednio do Group General Counsel Chief Compliance Officer and Chief Counsel EH na następujący adres e-mail: alessandra.ferrari@ethosenergy.com

4.2 Procedura zajmowania się zgłoszeniami wewnętrznymi

Po otrzymaniu zgłoszenia Zespół ds. zgłaszania nieprawidłowości podejmuje następujące działania:

- Potwierdza sygnaliście przyjęcie zgłoszenia w terminie 7 dni od dnia jego otrzymania, chyba że sygnalista nie podał adresu do kontaktu.
- Niezwłocznie informuje osobę wyznaczoną do podejmowania działań następczych w Spółce tj. Specjalistę ds. Organizacji/Inspektora Ochrony Danych, która następnie przekazuje informacje do Przewodniczącego Komisji Etyki Grupy (Group Ethics Committee). Jeśli jest to konieczne, osoba wyznaczona do podejmownia działań następczych w Spółce powołuje osobę (bądź osoby) lub zespół, który dokona weryfikacji zgłoszenia, przeprowadzi stosowne przesłuchania i zdobędzie niezbędną dokumentację.
- Skrupulatnie śledzi otrzymane zgłoszenia.
- Na żądanie wyznacza bezpośrednie spotkanie z sygnalistą w rozsądnym terminie, nieprzekraczającym 14 dni.
- Utrzymuje kontakt z sygnalistą i w razie potrzeby zwraca się o dodatkowe informacje
- Organizuje przesłuchanie osoby zaangażowanej w sprawę na jej wniosek lub, jeśli uzna to za stosowne, pozyskuje pisemne uwagi i dokumenty.
- Ocenia, czy spełnione zostały zasadnicze wymagania dotyczace zgłoszenia, aby ocenić jego dopuszczalność/ważność, także w celu zapewnienia ochrony sygnaliście.
- Udziela informacji zwrotnej do zgłoszenia w terminie 3 miesięcy od dnia potwierdzenia jego otrzymania, a w przypadku braku takiego potwierdzenia w terminie 3 miesięcy od upływu terminu 7 dni od dnia złożenia zgłoszenia, chyba że sygnalista nie podał adresu do kontaktu, na który należy przekazać informację zwrotną.

Zespół ds. zgłaszania nieprawidłowści prowadzi również rejestr zgłoszeń wewnętrznych.

Zgłoszenie przekazane podmiotowi innemu niż Zespół ds. zgłaszania nieprawidłowości należy przekazać samemu zespołowi, w jeden ze sposobów określonych w punkcie 4 niniejszej procedury, w terminie 7 dni od dnia jego otrzymania, powiadamiając jednocześnie sygnalistę o przekazaniu.

5. ZGŁOSZENIA ZEWNĘTRZNE[1]

Sygnalista powinien w pierwszej kolejności skorzystać z wewnętrznego kanału zgłaszania Spółki , jak opisano w punkcie 4 niniejszej Procedury. Będzie to najszybszym i najskuteczniejszym środkiem zaradczym w przypadku wszelkich naruszeń. Nie mniej jednak, sygnalista może dokonać zgłoszenia zewnętrznego bez uprzedniego dokonania zgłoszenia wewnętrznego.

Zgłoszenie zewnętrzne jest przyjmowane przez Rzecznika Praw Obywatelskich albo organ publiczny tj. 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

Dotyczy to w szczególności sytuacji, gdy w momencie zgłoszenia zachodzi jeden z poniższych warunków:

- Wewnętrzny kanał zgłaszania jest nieaktywny lub nie spełnia wymogów prawnych.
- Sygnalista dokonał już wcześniej zgłoszenia wewnętrznego, które nie przyniosło żadnych rezultatów.

[1] Przepisy w zakresie zgłoszeń zewnętrznych wchodzą w życie z dniem 25 grudnia 2024r.

- Sygnalista ma uzasadnione powody, aby sądzić, że zgłoszenie wewnętrzne nie będzie skutecznie rozpatrzone lub że dokonanie takiego zgłoszenia może wiązać się z ryzykiem odwetu.
- Sygnalista ma uzasadniony powód, aby sądzić, że naruszenie może stanowić bezpośrednie lub oczywiste zagrożenie dla interesu publicznego.

Rzecznik Praw Obywatelskich oraz organ publiczny są odrębnymi administratorami w zakresie danych osobowych podanych w zgłoszeniu zewnętrznym, które zostało przyjete przez te organy.

Rzecznik Praw Obywatelskich oraz organ publiczny gwarantują, że procedura przyjmowania zgłoszeń zewnętrznych oraz związane z przyjmowaniem zgłoszeń przetwarzanie danych osobowych:

- uniemożliwiają uzyskanie dostępu do informacji objętych zgłoszeniem nieupoważnionym osobom;
- zapewniają ochronę poufności tożsamości sygnalisty oraz osoby, której dotyczy zgłoszenie.

Zgłoszeń zewnętrznych można dokonywać ustnie lub pisemnie (w postaci papierowej lub elektronicznej).

6. ŚRODKI OCHRONY

W przypadku dokonania zgłoszenia, Ustawa o ochronie sygnalistów zapewnia różne środki ochrony:

(i) zapewnienie poufności;

(ii) ochrona przed działaniami odwetowymi;

(iii) ograniczenie odpowiedzialności za ujawnienie informacji poufnych.

Sygnalista podlega ochronie od chwili dokonania zgłoszenia lub ujawnienia publicznego, pod warunkiem, że miał uzasadnione podstawy sądzić, że zgłoszenie lub ujawnienie publiczne jest niezbędne do ujawnienia naruszenia prawa zgodnie z ustawą.

6.1 Obowiązek zachowania poufności

Poufność dotycząca tożsamości sygnalisty, osoby której dotyczy zgłoszenie, innych zaangażowanych stron oraz osób wymienionych w zgłoszeniu jest zapewniona na wszystkich etapach procesu zgłaszania.

Ujawnienie tożsamości sygnalisty osobom nieupoważnionym może nastąpić jedynie:

- za wyraźną zgodą sygnalisty;
- gdy ujawnienie jest koniecznym i proporocjonalnym obowiązkiem wynikającym z przepisów prawa w związku z postępowaniami wyjaśniającymi prowadzonymi przez organy publiczne lub postępowaniami przygtotowaczymi lub sądowymi prowadzonymi przez sądy, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy zgłoszenie.

Przed dokonaniem ujawnienia, o którym mowa powyżej, właściwy organ publiczny lub właściwy sąd powiadamia o tym sygnalistę, przesyłając w postaci papierowej lub elektronicznej wyjaśnienie powodów ujawnienia jego danych osobowych, chyba że takie powiadomienie zagrozi postępowaniu wyjaśniającemu lub postępowaniu przygotowawczemu, lub sądowemu.

6.2 Ochrona przed działaniami odwetowymi

Wobec sygnalisty nie mogą być podejmowane działania odwetowe ani próby lub groźby zastosowania takich działań.

Jeżeli praca była, jest lub ma być świadczona na podstawie stosunku pracy, wobec sygnalisty nie mogą być podejmowane działania odwetowe, polegające w szczególności na:

- odmowie na wiązania stosunku pracy;
- wypowiedzeniu lub rozwiązaniu bez wypowiedzenia stosunku pracy;

- nie zawarciu umowy o pracę na czas określony lub umowy o pracę na czas nieokreślony po rozwiązaniu umowy o pracę na okres próbny, nie zawarciu kolejnej umowy o pracę na czas określony lub nie zawarciu umowy o pracę na czas nieokreślony po rozwiązaniu umowy o pracę na czas określony - w przypadku gdy sygnalista miał uzasadnione oczekiwanie, że zostanie z nim zawarta taka umowa;
- obniżeniu wysokości wynagrodzenia za pracę;
- wstrzymaniu awansu albo pominięciu przy awansowaniu;
- pominięciu przy przyznawaniu innych niż wynagrodzenie świadczeń związanych z pracą lub obniżeniu wysokości tych świadczeń;
- przeniesieniu na niższe stanowisko pracy;
- zawieszeniu w wykonywaniu obowiązków pracowniczych lub służbowych;
- przekazaniu innemu pracownikowi dotychczasowych obowiązków sygnalisty;
- niekorzystnej zmianie miejsca wykonywania pracy lub rozkładu czasu pracy;
- negatywnej ocenie wyników pracy lub negatywnej opinii o pracy;
- nałożeniu lub zastosowaniu środka dyscyplinarnego, w tym kary finansowej, lub środka o podobnym charakterze;
- przymusie, zastraszaniu lub wykluczeniu;
- mobbingu;
- dyskryminacji;
- niekorzystnym lub niesprawiedliwym traktowaniu;
- wstrzymaniu udziału lub pominięciu przy typowaniu do udziału w szkoleniach podnoszących kwalifikacje zawodowe;
- nieuzasadnionym skierowaniu na badania lekarskie, w tym badania psychiatryczne, chyba że przepisy odrębne przewidują możliwość skierowania pracownika na takie badania;
- działaniu zmierzającym do utrudnienia znalezienia w przyszłości pracy w danym sektorze lub w danej branży na podstawie nieformalnego lub formalnego porozumienia sektorowego lub branżowego;
- spowodowaniu straty finansowej, w tym gospodarczej, lub utraty dochodu;
- wyrządzeniu innej szkody niematerialnej, w tym naruszeniu dóbr osobistych, w szczególności dobrego imienia sygnalisty.

Za działania odwetowe z powodu dokonania zgłoszenia lub ujawnienia publicznego uważa się także próbę lub groźbę zastosowania środka określonego powyżej.

Powyższe stosuje się również do osoby pomagającej w dokonaniu zgłoszenia oraz osoby powiązanej z sygnalistą oraz odpowiednio do osoby prawnej lub innej jednostki organizacyjnej pomagającej sygnaliście lub z nim powiązanej.

6.3 Ograniczenia odpowiedzialności sygnalisty

Dokonanie zgłoszenia lub ujawnienia publicznego nie może stanowić podstawy odpowiedzialności, w tym odpowiedzialności dyscyplinarnej lub odpowiedzialności za szkodę z tytułu naruszenia praw innych osób lub obowiązków określonych w przepisach prawa, w szczególności w przedmiocie zniesławienia, naruszenia dóbr osobistych, praw autorskich, ochrony danych osobowych oraz obowiązku zachowania tajemnicy, w tym tajemnicy przedsiębiorstwa, z uwzględnieniem art. 5 Ustawy o ochronie sygnalistów, pod warunkiem że sygnalista miał uzasadnione podstawy sądzić, że zgłoszenie lub ujawnienie publiczne jest niezbędne do ujawnienia naruszenia prawa zgodnie z ustawą.

W przypadku wszczęcia postępowania prawnego dotyczącego odpowiedzialności, o której mowa powyżej, sygnalista może wystąpić o umorzenie takiego postępowania.

Uzyskanie informacji będących przedmiotem zgłoszenia lub ujawnienia publicznego lub dostęp do takich informacji nie mogą stanowić podstawy odpowiedzialności, pod warunkiem, że takie uzyskanie lub taki dostęp nie stanowią czynu zabronionego.

7. OCHRONA DANYCH

Pozyskiwanie i zarządzanie zgłoszeniami odbywa się z zachowaniem pełnej zgodności z przepisami RODO dotyczącymi ochrony danych osobowych. Na przykład Spółka wyznacza Inspektorów ds. ochrony danych osobowych, upoważnione osoby odpowiedzialne za zajmowanie się danymi osobowymi i przekazuje informację o przetwarzaniu danych osobowych sygnalistom i innym stronom zaangażowanym w zgłoszenie. Ochronę danych osobowych zapewniamy sygnaliście, osobom których dotyczy zgłoszenie oraz innym osobom zaangażowanym w zgłoszenie, w tym osobom wymienionym w zgłoszeniu jako osoby, których dane dotyczą. Wszystkie osoby, które są zaangażowane w proces obsługi zgłoszenia są upoważnione do przetwarzania danych osobowych i zobowiązują się do zachowania tajemnicy w zakresie pozyskanych informacji i danych osobowych. Ocena skutków dla ochrony danych osobowych (A Data Protection Impact Assessment - DPIA) została przeprowadzona.

Raporty wewnętrzne i związana z nimi dokumentacja są przechowywane przez okres niezbędny do rozpatrzenia zgłoszenia i nie dłużej niż 3 lata po zakończeniu roku kalnedarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.

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.

8. SANKCJE

Ustawa o ochronie sygnalisty przewiduje następujące sankcje karne:

- Kto, chcąc, aby inna osoba nie dokonała zgłoszenia, uniemożliwia jej to lub istotnie utrudnia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Jeżeli sprawca czynu określonego powyżej stosuje wobec innej osoby przemoc, groźbę bezprawną lub podstęp, podlega karze pozbawienia wolności do lat 3.
- Kto podejmuje działania odwetowe wobec sygnalisty, osoby pomagającej w dokonaniu zgłoszenia lub osoby powiązanej z sygnalistą, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- Jeżeli sprawca czynu określonego w ust. 1 działa w sposób uporczywy, podlega karze pozbawienia wolności do lat 3.
- Kto wbrew przepisom ustawy ujawnia tożsamość sygnalisty, osoby pomagającej w dokonaniu zgłoszenia lub osoby powiązanej z sygnalistą, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- Kto dokonuje zgłoszenia lub ujawnienia publicznego, wiedząc, że do naruszenia prawa nie doszło, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- Kto, będąc odpowiedzialnym za ustanowienie procedury zgłoszeń wewnętrznych, wbrew przepisom ustawy procedury tej nie ustanawia lub ustanawia ją z istotnym naruszeniem wynikających z ustawy wymogów, podlega karze grzywny.

Ponadto:

- Sygnalista, wobec którego dopuszczono się działań odwetowych, ma prawo do odszkodowania w wysokości nie niższej niż przeciętne miesięczne wynagrodzenie w gospodarce narodowej w poprzednim roku, ogłaszane do celów emerytalnych w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" przez Prezesa Głównego Urzędu Statystycznego, lub prawo do zadośćuczynienia.
- Osoba, która poniosła szkodę z powodu świadomego zgłoszenia lub ujawnienia publicznego nieprawdziwych informacji przez sygnalistę, ma prawo do odszkodowania lub zadośćuczynienia za naruszenie dóbr osobistych od sygnalisty, który dokonał takiego zgłoszenia lub ujawnienia publicznego.

9. INFORMACJA

Procedura zgłaszania nieprawidłowosci jest dostępna dla każdego i jest opublikowana zarówno w wewnętrznej sieci komputerowej Spółki, na stronie internetowej Spółki www.ethosenergy.com/pl oraz w intranecie Spółki dla wszystkich pracowników, pod poniższym linkiem https://ethosenergygroup.share-point.com/sites/Home.

Spółka zapewnia okresowe szkolenia dla członków Zespołu ds. zgłaszania nieprawidłowości oraz całego personelu, który może brać udział w weryfikacji danego zgłoszenia. Ma to na celu zagwarantowanie właściwego rozumienia celów i zabezpieczeń przewidywanych przez prawo, a także kultywowanie kultury uczciwości i odpowiedzialności w Spółce.

EthosEnergy Poland S.A.
PREZES ZARZĄDU
Dyrektor Naczelny
Janusz Osadnik

EthosEnergy

INTERNAL REPORTING PROCEDURE

at EthosEnergy Poland S.A.

dated 18 September, 2024

1. INTRODUCTION

The Whistleblower Protection Act of 14 June 2024 implements EU Directive 2019/1937 on the protection of individuals reporting information on breaches of Union law into Polish law and it introduces the obligation to establish internal procedures for reporting information on breaches acquired in a work-related context.

The Whistleblower Protection Act provides important protection measures in terms of confidentiality, protection against any forms of retaliation, support measures, and privacy for individuals who, while working on behalf of the company, wish to make a written or oral report on specific breaches of law of which they have become aware in their work environment.

Additionally, The Whistleblower Protection Act clearly defines the technical and organizational requirements for internal and external reporting procedures.

2. PURPOSE AND SCOPE OF APPLICATION

EthosEnergy Poland S.A. (hereinafter referred to as the "Company"), by adopting this Procedure (Internal Reporting Procedure), intends to comply with the Whistleblower Protection Act.

The Company wishes to foster a culture of effective communication internally and to ensure that whistleblowers, by reporting breaches of law that they have become aware of in the form of actions, omissions or misconduct, make a significant contribution to the improvement of their own organization.

3. SUBJECT OF THE REPORT

3.1 Violation of European Union or national regulations

A whistleblower may report conduct, actions, or omissions that are unlawful or intended to circumvent the law and harm the Company's integrity, concerning:

- Corruption
- Public procurement
- Financial services, products, and markets
- Anti-money laundering and counter-terrorism financing
- Product safety and compliance
- Transport safety
- Environmental protection
- Radiation protection and nuclear safety
- Food and feed safety
- Animal health and welfare
- Public health
- Consumer protection
- Privacy and data protection
- Network and information system security
- The financial interests of the Polish State Treasury, local government units, and the European Union

- The internal market of the European Union, including public law principles of competition and state aid and corporate taxation
- Constitutional freedoms of human rights and civil liberties - occurring in relations between individuals and public authorities and not related to the areas indicated in the above points.

3.2 What cannot be the subject of reporting

The Procedure covers behaviors, actions, or omissions that the whistleblower has observed in their work environment.

However, personal disputes, claims, or demands that are solely related to the whistleblower's individual employment relationship or are inextricably linked to their employment relationship with organizational subordinates cannot be reported. For example, reports concerning labour disputes and pre-trial stages, discrimination among coworkers, or interpersonal conflicts between the whistleblower and another employee or supervisor are not eligible for reporting under this Procedure.

Within the scope of this internal reporting procedure, the Company has also not provided for the possibility of additional, reporting of information on violations of internal regulations or ethical standards applicable to the Company, which have been established by the Company pursuant to and remain in compliance with generally applicable laws, i.e. reports referred to in Article 3.2 of the Law on the Protection of Whistleblowers.

Nonetheless, a whistleblower may report behaviors, actions or omissions that damage the integrity of the Company, even though they do not fall within the scope of this internal reporting procedure (as indicated in Section 3.1 above), if they violate internal policies or procedures. Such reports, will be forwarded to the Group Ethics Committee for consideration in accordance with the provisions of the Group Code of Ethics.

3.3 The elements and the characteristics of the report

Reports must be as precise and detailed as possible to enable those responsible for receiving and processing them to assess the facts. A report should in particular include:

- The date and place of the event that is the subject of the report.
- A description of the event.
- Personal data or other elements that allow for the identification of the person to whom the acts described in the report can be attributed.
- Personal data allowing for the identification of other persons who may be aware of the violation.

It is also helpful to attach any available documents in support of the report.

3.4 Who Can Make a Report

All persons who have obtained information in a work-related context are entitled to make reports, including anonymous ones, namely:

- Employees;
- Temporary workers;
- Persons performing work on a basis other than an employment relationship, including under a civil law contract;

- Entrepreneurs;
- Procurators;
- Shareholders or partners;
- Members of the body of a legal person or organizational unit without legal personality;
- Persons performing work under the supervision and management of a contractor, subcontractor or supplier;
- Trainees;
- Volunteers;
- Interns.

This Procedure also applies to a natural person referred to above in the case of a report or public disclosure of information about a violation of the law obtained in a work-related context before entering into an employment relationship or other legal relationship constituting the basis for providing work or services or performing a function in a legal entity or on behalf of such an entity, or after their termination.

4. INTERNAL REPORTING

4.1 Internal Reporting Procedure

The Company - in accordance with the Law on the Protection of Whistleblowers and after consultation with representatives of the Company Trade Unions - has implemented its Internal Reporting Procedure, ensuring confidentiality regarding the identity of the whistleblower and any other person mentioned in the report, as well as the content of the report and related documentation.

The Company has established a team responsible for receiving reports, composed of:

1. An Organization Specialist/Data Protection Officer
2. Senior Legal Counsel

possessing the necessary expertise (the "Whistleblowing Team").

For follow-up actions, the Company has appointed:

an Organization Specialist/Data Protection Officer

which immediately informs the Chair of the Group Ethics Committee, which, if necessary, appoints additional experts.

Methods of Reporting

Reports can be made in all languages using the following channels:

- In writing via the Navex digital platform, available at the following link: https://secure.ethicspoint.eu/domain/media/en/gui/106568/index.html.
- Orally, 24/7, by calling the Hotline Contact Number 00 800 491 19 83
- Orally, by requesting an in-person meeting or videoconference (for example via MicrosoftTeams), at the whistleblower's discretion, scheduled within a reasonable timeframe, no longer than 14 days from the date of receipt of such a request.

A request for a meeting can be submitted through the aforementioned channels. Reports made within the internal channel of company can also be made anonymously.

All reports are treated and processed equally, regardless of whether whistleblowers decide to disclose their identity or whether the report is made anonymously.

If the report concerns events directly related to a member of the Whistleblowing Team, a person appointed to take follow-up actions in the Company, or senior management such as the Management Board or Supervisory Board of the Company, the report may be sent directly to the Group General Counsel, Chief Compliance Officer and Chief Counsel EH at the following email address: alessandra.ferrari@ethosenergy.com

4.2 Procedure for handling internal reports

Upon receipt of a report, the Whistleblowing Team shall take the following actions:

- Acknowledge receipt of the report to the whistleblower within 7 days of its receipt, unless the whistleblower has not provided a contact address.
- Immediately inform the person designated to take follow-up actions in the Company, who shall then forward the information to the Chair of the Group Ethics Committee. If necessary, the person designated to take follow-up actions in the Company shall appoint a person (or persons) or a team to verify the report, conduct appropriate interviews, and obtain the necessary documentation.
- Meticulously track all received reports.
- Schedule a direct meeting with the whistleblower at their request, within a reasonable timeframe, not exceeding 14 days.
- Maintain contact with the whistleblower and request additional information if necessary.
- Arrange for an interview with the person involved in the matter at their request or, if deemed appropriate, through written proceedings, obtaining written statements and documents.
- Assess whether the essential requirements for the report have been met in order to assess its admissibility/validity, also to ensure the protection of the whistleblower.
- Provide feedback on the report within 3 months of acknowledging its receipt, and in the absence of such acknowledgment within 3 months of the expiry of the 7-day period from the date of filing the report, unless the whistleblower has not provided a contact address to which the feedback should be sent.

  The Whistleblowing Team shall also maintain a register of internal reports.

  Any report submitted to an entity other than the Whistleblowing Team shall be forwarded to the Team itself, in one of the ways specified in section 4 of this Procedure, within 7 days of its receipt, and the whistleblower shall be simultaneously notified of the forwarding.

5. EXTERNAL REPORTING[1]

The whistleblower should first use the Company's internal reporting channel as described in section 4 of this Procedure. This will be the quickest and most effective remedy for any violations. However, the whistleblower may make an external report without first making an internal report.

An external report is received by the Ombudsman or a public authority, such as central and central government administration bodies, regional government administration bodies, local government units, other state bodies, and other entities performing public administration tasks by law, which are competent to take follow-up actions.

This applies in particular if, at the time of the report, one of the following conditions is met:

- The internal reporting channel is inactive or does not meet legal requirements.

[1] The provisions regarding external reporting shall enter into force on 25 December 2024.

- The whistleblower has previously made an internal report that has not yielded any results.
- The whistleblower has reasonable grounds to believe that the internal report will not be effectively investigated or that making such a report may carry a risk of retaliation.
- The whistleblower has reasonable grounds to believe that the violation may pose a direct or obvious threat to the public interest.

The Ombudsman and the public authority are separate data controllers for personal data provided in an external report which has been received by these bodies. The Ombudsman and the public authority guarantee that the procedure for receiving external reports and the processing of personal data related to receiving reports:

- prevent unauthorized persons from gaining access to information contained in the report;
- ensure the confidentiality of the identity of the whistleblower and the person to whom the report relates.

External reports can be made orally or in writing (in paper or electronic form).

6. PROTECTION MEASURES

In the event of a report, the Whistleblower Protection Act provides various safeguards:

(i) ensuring confidentiality;
(ii) protection against retaliation;
(iii) limiting liability for disclosing confidential information.

A whistleblower is entitled to protection from the moment a report is made or information is publicly disclosed, provided that they had reasonable grounds for believing that the report or public disclosure was necessary to disclose a violation of the law in accordance with the Act.

6.1 Duty of confidentiality

Confidentiality regarding the identity of the whistleblower, the person to whom the report relates, other involved parties, and persons mentioned in the report is ensured at all stages of the reporting process.

Disclosure of the whistleblower's identity to unauthorized persons may only occur:

- with the whistleblower's express consent;
- when disclosure is a necessary and proportionate obligation arising from the law in connection with investigative proceedings conducted by public authorities or preparatory or judicial proceedings conducted by courts, including to guarantee the right to defense of the person to whom the report relates.

Before disclosure as referred to above, the competent public authority or the competent court shall notify the whistleblower thereof, sending a written or electronic explanation of the reasons for disclosing their personal data, unless such notification would jeopardize the investigative or preparatory proceedings, or judicial proceedings.

6.2 Protection against retaliation

No retaliatory actions or attempts or threats to take such actions may be taken against a whistleblower. If the work was, is or is to be performed on the basis of an employment relationship, no retaliatory actions may be taken against the whistleblower, in particular consisting of:

- refusal to enter into an employment relationship;
- termination of an employment contract or dismissal without notice;

- failure to conclude a fixed-term employment contract or an open-ended employment contract after the termination of a probationary employment contract, failure to conclude another fixed-term employment contract or failure to conclude an open-ended employment contract after the termination of a fixed-term employment contract - where the whistleblower had a reasonable expectation that such a contract would be concluded with him;
- reduction of remuneration;
- withholding of promotion or omission in promotion;
- omission in granting benefits other than remuneration related to work or reduction of the amount of such benefits;
- transfer to a lower position;
- suspension from performing employee or official duties;
- transferring the whistleblower's previous duties to another employee;
- an unfavorable change in the place of work or working hours;
- negative performance appraisal or negative work opinion;
- imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature;
- coercion, intimidation or exclusion;
- mobbing;
- discrimination;
- unfavourable or unfair treatment;
- withholding participation or omission in nominating for participation in training to improve professional qualifications;
- unjustified referral for medical examinations, including psychiatric examinations, unless separate regulations provide for the possibility of referring an employee for such examinations;
- actions aimed at making it difficult to find work in the future in a given sector or industry on the basis of an informal or formal sectoral or industry agreement;
- causing financial or economic loss or loss of income;
- causing other non-pecuniary damage, including infringement of personal rights, in particular the whistleblower's good name.

An attempt or threat to take a measure specified above shall also be considered a retaliatory action for making a report or public disclosure.

The above shall also apply to a person assisting in making a report and a person related to the whistleblower and, accordingly, to a legal person or other organizational unit assisting the whistleblower or related to him.

6.3 Limitations on the whistleblower's liability

Making a report or public disclosure cannot constitute grounds for liability, including disciplinary liability or liability for damages resulting from the infringement of the rights of other persons or obligations under the law, in particular in the matter of defamation, infringement of personal rights, copyrights, protection of personal data and the obligation to maintain confidentiality, including trade secrets, taking into account Article 5 of the Whistleblower Protection Act, provided that the whistleblower had reasonable grounds for believing that the report or public disclosure was necessary to disclose a violation of the law in accordance with the Act. In the event of legal proceedings concerning the liability referred to above, the whistleblower may request the dismissal of such proceedings. Obtaining information that is the subject of a report or public disclosure or access to such

information cannot constitute grounds for liability, provided that such obtaining or such access does not constitute an unlawful act.

7. Data Protection

The collection and management of reports are carried out in full compliance with the GDPR regulations on the protection of personal data. For example, the Company appoints Data Protection Officers, authorized persons responsible for handling personal data, and provides information about the processing of personal data to whistleblowers and other parties involved in the report. We ensure the protection of personal data for the whistleblower, the person to whom the report relates, and other persons involved in the report, including those mentioned in the report as data subjects. All persons involved in the process of handling reports are authorized to process personal data and are obliged to maintain confidentiality regarding the obtained information and personal data. A Data Protection Impact Assessment (DPIA) has been carried out.

Internal reports and related documentation are stored for the period necessary to process the report and no longer than 3 years after the end of the calendar year in which the follow-up actions were completed, or after the completion of the proceedings initiated by these actions. Personal data that is not relevant to the processing of the report is not collected and, if collected by mistake, is immediately deleted. The deletion of such personal data shall take place within 14 days from the moment it is established that they are not relevant to the case.

8. Sanctions

The Whistleblower Protection Act provides for the following criminal penalties:

- Anyone who, intending to prevent another person from making a report, prevents or significantly hinders them from doing so, shall be subject to a fine, restriction of liberty or imprisonment of up to one year.
- If the perpetrator of the act specified above uses violence, unlawful threat or deceit against another person, they shall be subject to imprisonment of up to 3 years.
- Anyone who takes retaliatory actions against a whistleblower, a person assisting in making a report or a person associated with the whistleblower, shall be subject to a fine, restriction of liberty or imprisonment of up to 2 years.
- If the perpetrator of the act specified in paragraph 1 acts persistently, they shall be subject to imprisonment of up to 3 years.
- Anyone who, in violation of the Act, discloses the identity of a whistleblower, a person assisting in making a report or a person associated with the whistleblower, shall be subject to a fine, restriction of liberty or imprisonment of up to one year.
- Anyone who makes a report or public disclosure, knowing that no violation of the law has occurred, shall be subject to a fine, restriction of liberty or imprisonment of up to 2 years.
- Anyone who, being responsible for establishing an Internal Reporting Procedure fails to establish such a procedure in violation of the Act or establishes it in significant violation of the requirements arising from the Act, shall be subject to a fine.

Furthermore:

- A whistleblower against whom retaliatory actions have been taken has the right to compensation of at least the average monthly wage in the national economy in the previous year, announced for pension purposes in the Journal of Laws of the Republic of Poland by the President of the Central Statistical Office, or the right to compensation.
- A person who has suffered damage due to a deliberate report or public disclosure of false information by a whistleblower has the right to damages or satisfaction for the infringement of personal rights from the whistleblower who made such a report or public disclosure.

9. Information

The Internal Reporting Procedure is available to everyone and is published both on the Company's internal computer network, on the Company's website www.ethosenergy.com/pl and on the Company's intranet for all employees, under the following link https://ethosenergygroup.share-point.com/sites/Home.

The Company provides regular training for members of the Whistleblowing Team and all personnel who may be involved in verifying a given report. This is to ensure a proper understanding of the objectives and safeguards provided by law, as well as to cultivate a culture of honesty and responsibility in the Company.

EthosEnergy Poland S.A.
PREZES ZARZĄDU
Dyrektor Naczelny
Janusz Osadnik