PROCEDURA ZGŁOSZEŃ WEWNĘTRZNYCH W ETHOSENERGY SPÓŁKA Z O.O.

EthosEnergy

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 ochronie 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 sygnalistów jasno określa wymagania techniczne i organizacyjne dotyczące wewnętrznych i zewnętrznych procedur dokonywania zgłoszeń.

2. CEL I ZAKRES STOSOWANIA

EthosEnergy Sp. z o.o. (dalej "Spółka") stosując niniejszą procedurę (Procedurę zgłoszeń wewnętrznych) zamierza zastosować się do 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.

Dlatego też Spółka zachęca wszystkich odbiorców Procedury zgłoszeń wewnętrznych do dokonywania zgłoszeń opisanych w niej naruszeń, zapewniając jednocześnie poniżej opisane zabezpieczenia.

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 terytorialnego 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

Ponieważ w Spółce nie działa zakładowa organizacja związkowa, Spółka - zgodnie z Ustawą o ochronie sygnalistów i po konsultacji z przedstawicielami osób świadczących pracę na rzecz Spółki, wyłonionymi w trybie przyjętym w Spółce - 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 z:

1) Radcy prawnego Spółki.
2) Specjalisty ds. organizacji/Inspektora Ochrony Danych (Compliance Manager)

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

Spółka do **podejmowania działań następczych** powołała:

1) Radcę prawnego Spółki,

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

4.2. 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

4.3. 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. Radcę Prawnego Spółki, który 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.

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

- Sygnalista dokonał już wcześniej zgłoszenia wewnętrznego, które nie przyniosło żadnych rezultatów.
- 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 przygotowawczymi 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 nawiązania 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:

1) Kto, chcąc, aby inna osoba nie dokonała zgłoszenia, uniemożliwia jej to lub istotnie utrudnia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
2) Jeżeli sprawca czynu określonego powyżej stosuje wobec innej osoby przemoc, groźbę bezprawną lub podstęp, podlega karze pozbawienia wolności do lat 3.
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.
4) Jeżeli sprawca czynu określonego w ust. 1 działa w sposób uporczywy, podlega karze pozbawienia wolności do lat 3.
5) 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.
6) Kto dokonuje zgłoszenia lub ujawnienia publicznego, wiedząc, że do naruszenia prawa nie doszło, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
7) 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:

1) 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.
2) 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 nieprawidłowosci 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.

Signed by / Podpisano przez:
Murat Demirel
Date / Data: 2024-09-14 11:06

Murat Demirel – Prezes Zarządu

Signed by / Podpisano przez:
Ian Charles Stanley
Date / Data: 2024-09-13 16:01

Ian Stanley – Członek Zarządu

INTERNAL REPORTING PROCEDURE IN ETHOSENERGY SPÓŁKA Z O.O.

1. INTRODUCTION

The Whistleblower Protection Act of June 14, 2024, implements EU Directive 2019/1937 on the protection of persons who report breaches of Union law into Polish law and introduces the obligation to establish procedures for making internal reports of breaches that occurred in a work-related context. The Whistleblower Protection Act provides significant protection measures in terms of confidentiality, protection against all forms of retaliation, support measures, and privacy assurances for individuals working for the Company who wish to make written or oral reports about specific breaches of law they have learned about 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 Sp. z o.o. (hereinafter referred to as the "Company"), by applying this procedure (Internal Reporting Procedure), intends to comply with the Whistleblower Protection Act. The Company aims to internally promote a culture of effective communication and ensures that whistleblowers, by reporting breaches they have learned about, in the form of actions, omissions, or behaviors that are against the law, significantly contribute to the improvement of their own organization. Therefore, the Company encourages all recipients of the Internal Reporting Procedure to report the breaches described in it, while providing the safeguards described below.

3. SUBJECT OF THE REPORT

3.1 Breaches of European Union or national laws

A whistleblower may report behaviors, actions, or omissions that are unlawful or aimed at circumventing the law and harming the integrity of the Company concerning:

- Corruption;
- Public procurement;
- Financial services, products, and markets;
- Anti-money laundering and counter-terrorist financing;
- Product safety and compliance;
- Transport safety;
- Environmental protection;
- Radiological protection and nuclear safety;
- Food and feed safety;
- Animal health and welfare;
- Public health;
- Consumer protection;
- Privacy and personal data protection;
- Network and information systems security;
- Financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union;
- The internal market of the European Union, including public competition and state aid rules, and corporate taxation;
- Constitutional freedoms and human and citizen rights – occurring in relations between individuals and public authorities and unrelated to the areas indicated in the above points

3.2 What cannot be reported

Reports should concern behaviors, actions, or omissions that the whistleblower has noticed in their work environment.

Disputes, claims, or demands related to the whistleblower's personal interest, which concern only their individual employment relations or are inherently related to their employment relationship with subordinate persons, cannot be reported. For example, this internal reporting procedure does not cover reports concerning employee disputes and pre-litigation stages, discrimination among colleagues, interpersonal conflicts between the whistleblower and another employee or supervisor.

Under this internal reporting procedure, the Company has also not provided for the possibility of additionally reporting breaches concerning the internal regulations or ethical standards in force at the Company, which have been established by the Company based on generally applicable laws

and remain compliant with them, i.e., reports referred to in Article 3(2) of the Whistleblower Protection Act.

However, the whistleblower may report behaviors, actions, or omissions that harm the integrity of the Company, even if they do not fall within the scope of this internal reporting procedure (as indicated in point 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 Elements and features of the report

Reports must be as precise and detailed as possible to enable the assessment of facts by the persons responsible for receiving and considering them.

The report should particularly include:

- The date and place of the event being reported.
- A description of the event.
- Personal data or other elements enabling the identification of the person to whom the actions contained in the report can be attributed.
- Personal data enabling the identification of other persons potentially aware of the breach.

It is also useful to attach available documents supporting 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, including:

- Employees;
- Temporary workers;
- Persons performing work on a basis other than an employment relationship, including under a civil law contract;
- Entrepreneurs;
- Proxies;
- Shareholders or partners;
- Members of the body of a legal person or an organizational unit without legal personality;
- Persons performing work under the supervision and direction of a contractor, subcontractor, or supplier;
- Interns;
- Volunteers;
- Trainees.

The procedure also applies to the natural person referred to above in the case of reporting or publicly disclosing information about a breach of law obtained in a work-related context, occurring before the establishment of an employment relationship or another legal relationship constituting the basis for performing work or services or holding a function in a legal entity or for the benefit of that entity or after their termination.

4. INTERNAL REPORTING

4.1 Internal Reporting Procedure

Since there is no trade union organization operating in the Company, the Company - in accordance with the Whistleblower Protection Act and after consultation with representatives of persons providing work for the Company, selected in the manner adopted in the Company - has launched 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 appointed a **team responsible for receiving reports**, consisting of:

- The Company's Legal Counsel.

- Organization Specialist/Data Protection Officer (Compliance Manager) with the necessary expertise (Whistleblowing Team).

The Company has appointed the following **for follow-up actions**:

- The Company's Legal Counsel, who immediately informs the Chairman of the Group Ethics Committee, who may appoint additional experts if necessary.

4. 2 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.
- Verbally, 24/7, by calling the Hotline: 00 800 491 19 83.
- Verbally, by requesting a personal meeting or videoconference (e.g., Microsoft Teams), at the discretion of the whistleblower, scheduled within a reasonable time, not exceeding 14 days from the date of receipt of such a request

Requests for meetings can be made through the aforementioned channels.

Reports made through the Company's internal channel can also be made anonymously.

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

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

4.3 Procedure for Handling Internal Reports

Upon receiving a report, the Whistleblowing Team takes the following actions:

- Confirms receipt of the report to the whistleblower within 7 days of its receipt, unless the whistleblower has not provided a contact address.
- Immediately informs the person designated for follow-up actions in the Company, i.e., the Company's Legal Counsel, who then forwards the information to the Chairman of the Group Ethics Committee. If necessary, the person designated for follow-up actions in the Company appoints a person (or persons) or a team to verify the report, conduct appropriate interviews, and obtain necessary documentation.
- Carefully tracks received reports.
- Upon request, schedules a direct meeting with the whistleblower within a reasonable time, not exceeding 14 days.
- Maintains contact with the whistleblower and, if necessary, requests additional information.
- Organizes an interview with the person involved in the matter at their request or, if deemed appropriate, obtains written comments and documents.
- Assesses whether the essential requirements for the report have been met to evaluate its admissibility/validity, also to ensure the whistleblower's protection.
- Provides feedback on the report within 3 months from the date of confirming its receipt, and in the absence of such confirmation, within 3 months from the expiry of the 7-day period from the

date of submitting the report, unless the whistleblower has not provided a contact address for feedback.

The Whistleblowing Team also keeps a register of internal reports.

A report submitted to an entity other than the Whistleblowing Team should be forwarded to the team itself, in one of the ways specified in point 4 of this procedure, within 7 days of its receipt, simultaneously notifying the whistleblower of the forwarding.

5. EXTERNAL REPORTS[1]

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

An external report is accepted by the Ombudsman or a public authority, i.e., supreme and central government administration bodies, local government administration bodies, local government units, other state bodies, and other entities performing public administration tasks by law, competent to take follow-up actions.

This particularly applies to situations where, at the time of reporting, one of the following conditions is met:

- The internal reporting channel is inactive or does not meet legal requirements.
- The whistleblower has already 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 considered or that making such a report may involve the risk of retaliation.
- The whistleblower has reasonable grounds to believe that the breach may pose a direct or obvious threat to the public interest.

The Ombudsman and the public authority are separate data controllers regarding the personal data provided in the external report, which has been accepted by these authorities.

The Ombudsman and the public authority guarantee that the procedure for accepting external reports and the related processing of personal data:

- Prevent unauthorized persons from accessing the information covered by the report;
- Ensure the confidentiality of the whistleblower's identity 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 making a report, the Whistleblower Protection Act provides various protection measures:

i. Ensuring confidentiality;
ii. Protection against retaliatory actions;
iii. Limitation of liability for disclosing confidential information.

The whistleblower is protected from the moment of making the report or public disclosure, provided that they had reasonable grounds to believe that the report or public disclosure was necessary to reveal a breach of law in accordance with the Act.

[1] The regulations for external notifications come into force on 25 December 2024.

6.1. Obligation to Maintain 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 can only occur:

- With the explicit consent of the whistleblower;
- When disclosure is a necessary and proportionate obligation arising from legal provisions 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 making the disclosure mentioned above, the relevant public authority or court notifies the whistleblower by sending an explanation of the reasons for disclosing their personal data in paper or electronic form, unless such notification would jeopardize the investigative or preparatory or judicial proceedings.

6.2. Protection Against Retaliatory Actions

No retaliatory actions or attempts or threats of such actions may be taken against the whistleblower.

If the work was, is, or is to be performed based on an employment relationship, no retaliatory actions may be taken against the whistleblower, particularly involving:

- Refusal to establish an employment relationship;
- Termination or dismissal without notice of the employment relationship;
- Failure to conclude a fixed-term or indefinite-term employment contract after the termination of a probationary period employment contract, failure to conclude another fixed-term employment contract, or failure to conclude an indefinite-term employment contract after the termination of a fixed-term employment contract - if the whistleblower had a reasonable expectation that such a contract would be concluded;
- Reduction of remuneration for work;
- Suspension of promotion or omission in promotion;
- Omission in granting work-related benefits other than remuneration or reduction of such benefits;
- Transfer to a lower position;
- Suspension from performing employee or official duties;
- Transfer of the whistleblower's current duties to another employee;
- Unfavorable change in the place of work or work schedule;
- Negative evaluation of work results or negative opinion about work;
- Imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature;
- Coercion, intimidation, or exclusion;
- Mobbing;
- Discrimination;

- Unfavorable or unfair treatment;
- Suspension of participation or omission in selecting 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 hindering future employment in a given sector or industry based on an informal or formal sectoral or industry agreement;
- Causing financial loss, including economic loss, or loss of income;
- Causing other non-material damage, including violation of personal rights, particularly the good name of the whistleblower.

Retaliatory actions due to making a report or public disclosure also include attempts or threats to apply the measures specified above.

The above also applies to a person assisting in making the report and a person associated with the whistleblower, as well as to a legal entity or other organizational unit assisting the whistleblower or associated with them.

6.3. Limitations of Whistleblower Liability

Making a report or public disclosure cannot be the basis for liability, including disciplinary liability or liability for damage due to the violation of the rights of other persons or obligations specified in legal provisions, particularly concerning defamation, violation of personal rights, copyright, data protection, and the obligation to maintain confidentiality, including trade secrets, considering Article 5 of the Whistleblower Protection Act, provided that the whistleblower had reasonable grounds to believe that the report or public disclosure was necessary to reveal a breach of law in accordance with the Act.

In the event of initiating legal proceedings concerning the liability mentioned above, the whistleblower may request the dismissal of such proceedings.

Obtaining information that is the subject of the report or public disclosure or access to such information cannot be the basis for liability, provided that such obtaining or access does not constitute a prohibited act.

7. DATA PROTECTION

The collection and management of reports are carried out in full compliance with GDPR regulations regarding 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 data protection for the whistleblower, the persons 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 report handling process are authorized to process personal data and are committed to maintaining the confidentiality of the acquired information and personal data. A Data Protection Impact Assessment (DPIA) has been conducted.

Internal reports and related documentation are stored for the period necessary to consider the report and no longer than 3 years after the end of the calendar year in which follow-up actions were completed or after the conclusion of proceedings initiated by these actions.

Personal data that is not relevant to the consideration of the report is not collected, and if accidentally collected, it is promptly deleted. The deletion of such personal data occurs within 14 days from the moment it is determined that it is not relevant to the case.

8. SANCTIONS

The Whistleblower Protection Act provides for the following criminal sanctions:

1. Anyone who, wanting another person not to make a report, prevents or significantly hinders them from doing so, is subject to a fine, restriction of liberty, or imprisonment for up to one year.
2. If the perpetrator of the act specified above uses violence, unlawful threat, or deceit against another person, they are subject to imprisonment for up to 3 years.
3. Anyone who takes retaliatory actions against a whistleblower, a person assisting in making a report, or a person associated with the whistleblower, is subject to a fine, restriction of liberty, or imprisonment for up to 2 years.
4. If the perpetrator of the act specified in point 1 acts persistently, they are subject to imprisonment for up to 3 years.
5. Anyone who, contrary to the provisions of the Act, discloses the identity of a whistleblower, a person assisting in making a report, or a person associated with the whistleblower, is subject to a fine, restriction of liberty, or imprisonment for up to one year.
6. Anyone who makes a report or public disclosure knowing that no breach of law has occurred, is subject to a fine, restriction of liberty, or imprisonment for up to 2 years.
7. Anyone responsible for establishing the internal reporting procedure who, contrary to the provisions of the Act, does not establish it or establishes it with significant violations of the requirements arising from the Act, is subject to a fine.

Additionally:

1. A whistleblower who has been subjected to retaliatory actions has the right to compensation in an amount not less than the average monthly salary in the national economy in the previous year, announced for pension purposes in the Official Journal of the Republic of Poland "Monitor Polski" by the President of the Central Statistical Office, or the right to redress.
2. A person who has suffered damage due to the deliberate report or public disclosure of false information by a whistleblower has the right to compensation or redress for the violation of personal rights from the whistleblower who made such a report or public disclosure.

9. INFORMATION

The procedure for reporting irregularities is available to everyone and is published both in the Company's internal computer network, on the Company's website www.ethosenergy.com/pl, and in the Company's intranet for all employees, at the following link: https://ethosenergygroup.sharepoint.com/sites/Home

The Company provides periodic training for members of the Whistleblowing Team and all personnel who may participate 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 integrity and responsibility within the Company.

Signed by / Podpisano przez:
Murat Demirel
Date / Data: 2024-09-14 11:05

Murat Demirel – President of the Management Board

Signed by / Podpisano przez:
Ian Charles Stanley
Date / Data: 2024-09-13 16:01

Ian Stanley – Member of the Management Board