

Procedura Grupy dotycząca przekazywania i przetwarzania zgłoszeń



01. CEL DOKUMENTU	3
02. ZAKRES ZASTOSOWANIA	4
03. KTO MOŻE DOKONAĆ ZGŁOSZENIA?.....	5
04. JAKIEGO RODZAJU DZIAŁANIA LUB ZACHOWANIA MOŻNA ZGŁOSIĆ?	5
05. KOORDYNATOR SYSTEMU I OSOBY ODPOWIEDZIALNE ZA PRZYJMOWANIE I PRZETWARZANIE ZGŁOSZEŃ	6
06. JAKĄ OCHRONĄ OBJĘCI SĄ SYGNALIŚCI, OSOBY POMAGAJĄCE W DOKONANIU ZGŁOSZENIA I OSOBY, KTÓRYCH DOTYCZY ZGŁOSZENIE?	6
07. PRZEKAZANIE INFORMACJI OSOBIE, KTÓREJ DOTYCZY ALERT	8
08. ZGŁOSZENIE ALERTU	8
09. PRZETWARZANIE ALERTÓW ZGŁOSZONYCH KANAŁEM WEWNĘTRZNYM.....	10
10. POUFNOŚĆ.....	11
11. MONITOROWANIE I STEROWANIE.....	12
ZAŁĄCZNIK 1: INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH	13

01. CEL DOKUMENTU

Celem *emeis* jest ciągle wzmacnianie własnych zasad etycznych i zapewnienie łatwo dostępnych narzędzi każdej osobie pragnącej zgłosić sytuację, która jest niewłaściwa lub niezgodna z zasadami *emeis* albo z obowiązującym prawem. W związku z tym ***emeis* udostępnia swoim pracownikom i interesariuszom System Zgłaszania Nieprawidłowości (*Whistleblowing System*)**.

System ten uzupełnia istniejące kanały i wzmacnia podejście wynikające z Kodeksu Etyki *emeis*. **Daje on każdej osobie, która chce zgłosić daną sytuację, możliwość dokonania takiego zgłoszenia przy zachowaniu poufności i – w razie potrzeby – anonimowości.**

System etycznego zgłaszania nieprawidłowości w żadnym razie nie jest systemem do przekazywania zgłoszeń w nagłych przypadkach i nie zastępuje istniejących systemów zgłaszania zdarzeń, które stanowią bezpośrednie zagrożenie dla ludzi lub mienia. Korzystanie z Systemu Zgłaszania Nieprawidłowości jest dobrowolne.

Niniejsza procedura obowiązuje w *emeis* S.A. oraz wszystkich jej spółkach zależnych.

W związku z tym zasady przedstawione w niniejszym dokumencie określono z uwzględnieniem prawa francuskiego.

emeis wprowadziła zmiany do istniejącego Systemu Zgłaszania Nieprawidłowości oraz dostosowała procedurę zgodnie z dyrektywą europejską z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa (dalej zwanej „Dyrektywą Europejską”). Transpozycji Dyrektywy Europejskiej do prawa polskiego dokonano ustawą z dnia 14 czerwca 2024 r. o ochronie signalistów.

Poza tym *emeis* dokłada wszelkich starań, aby zapewnić bezpieczeństwo i poufność przesyłanych danych, w tym danych osobowych, które mogą być zbierane w związku z przyjmowaniem i przetwarzaniem zgłoszeń dotyczących potencjalnych nieprawidłowości.

02. ZAKRES ZASTOSOWANIA

System wdrożony w *emeis* służy zgłaszaniu potencjalnych nieprawidłowości wynikających z następujących naruszeń:

Naruszeń Kodeksu Antykorupcyjnego (art. 17 Ustawy Sapin II)

- ▶ Zachowania lub sytuacji, które są sprzeczne z Kodeksem Antykorupcyjnym Grupy w takim zakresie, w jakim potencjalnie wykazują one cechy czynów korupcyjnych lub płatnej protekcji.

Innych naruszeń (art. 6 Ustawy Sapin II)

- ▶ Przestępstwa, wykroczenia.
- ▶ Zagrożenia dla interesu publicznego lub naruszenia interesu publicznego.
- ▶ Naruszenia lub próby ukrycia naruszenia zobowiązania międzynarodowego należycie ratyfikowanego przez Francję, jednostronnego aktu organizacji międzynarodowej wydanego na podstawie takiego zobowiązania, prawa Unii Europejskiej albo ustawy lub rozporządzenia.

Ryzyka poważnej szkody w kontekście obowiązku dołożenia staranności przez grupę (art. 1 ustawy z dnia 27 marca 2017 r. określonej jako ustawa o „obowiązku dołożenia staranności”)

- ▶ Istnienie lub materializacja ryzyka poważnych naruszeń praw człowieka lub podstawowych wolności (na przykład dyskryminacja, mobbing i molestowanie seksualne), zagrożenia dla zdrowia i bezpieczeństwa osób fizycznych i środowiska wynikającego z działalności Grupy albo jej podwykonawców lub dostawców, z którymi utrzymuje trwale relacje biznesowe, jeśli taka działalność związana jest z taką relacją.

Innych naruszeń Kodeksu Etyki i CSR Grupy.

03. KTO MOŻE DOKONAĆ ZGŁOSZENIA?

Wewnętrznie 	Zewnętrznie 
- Pracownicy Grupy - Byli pracownicy, jeśli informacja, której dotyczy zgłoszenie została uzyskana w kontekście takiej relacji - Kandydaci na pracowników, jeśli informacja, której dotyczy zgłoszenie została uzyskana w kontekście takiej relacji - Wspólnicy, partnerzy i osoby uprawnione do głosowania na zgromadzeniu wspólników - Członkowie organów administracyjnych - Organy zarządzające i nadzorcze - Pracownicy tymczasowi	- Pracownicy zewnętrzni - Współwykonawcy i podwykonawcy (dostawcy, usługodawcy, partnerzy itp.) lub personel i członkowie organów administracyjnych, zarządzających lub nadzorczych takich współwykonawców i podwykonawców

04. JAKIEGO RODZAJU DZIAŁANIA LUB ZACHOWANIA MOŻNA ZGŁOSIĆ?

Każde naruszenie naszych zasad etyki oraz wszelkie inne naruszenia praw i przepisów, jak również wszelkie incydenty dotyczące między innymi:

- korupcji, płatnej protekcji i konfliktów interesów;
- dyskryminacji, mobbingu i molestowania, bezpieczeństwa i higieny pracy;
- oszustwa, sprzeniewierzenia i kradzieży;
- praktyk ograniczających konkurencję;
- praw i ochrony osób fizycznych;
- ochrony środowiska;
- nieprzestrzegania ustaw i rozporządzeń albo naruszenia interesów publicznych.

System nie służy do przetwarzania faktów, informacji i dokumentów dotyczących opieki nad pacjentami lub rezydentami, a takie fakty, informacje i dokumenty podlegają w *emeis* specjalnym procedurom stosowanym na platformie www.emeis.com/plateforme-ecoute i/lub w systemie mediacji www.emeis.com/dispositif-mediation.

05. KOORDYNATOR SYSTEMU I OSOBY ODPOWIEDZIALNE ZA PRZYJMOWANIE I PRZETWARZANIE ZGŁOSZEŃ

Odpowiedzialność za przyjmowanie i przetwarzanie zgłoszeń w swoim zakresie ponoszą Dział Zgodności (Compliance) we Francji oraz Dział Zgodności (Compliance) w Polsce, które pełnią funkcję Głównego Referenta ds. Alertów (*Principal Alert Referent*, PAR).

Podczas realizacji postępowań wyjaśniających w celu zapewnienia skutecznego przetwarzania alertów PAR może zwracać się do innych działów (HR, Prawnego, Finansów, IT itp.) lub zewnętrznych osób trzecich, uwzględniając ich możliwości i niezależność.

Wszystkie osoby odpowiedzialne za przyjmowanie i przetwarzanie zgłoszeń mają obowiązek zachowania poufności.

06. JAKĄ OCHRONĄ OBJĘCI SĄ SYGNALIŚCI, OSOBY POMAGAJĄCE W DOKONANIU ZGŁOSZENIA I OSOBY, KTÓRYCH DOTYCZY ZGŁOSZENIE?

Krajowa ustawa dotycząca ochrony Sygnalistów i Dyrektywa Europejska chronią Sygnalistów przed działaniami odwetowymi i sankcjami.

Aby skorzystać ze statusu Sygnalisty, osoba dokonująca zgłoszenia musi spełnić jednak wszystkie wymienione poniżej warunki:

- ▶ **być osobą fizyczną**, a nie podmiotem prawnym (spółką, stowarzyszeniem lub związkiem zawodowym);
- ▶ **nie otrzymywać bezpośredniego wynagrodzenia finansowego**, tj. nie oczekiwać zapłaty za dokonane zgłoszenie;
- ▶ **działać w dobrej wierze**, tj. nie działać w złej wierze lub w celu zemsty poprzez zgłoszenie informacji, o których wie, że są fałszywe lub wprowadzają w błąd;
- ▶ **znać fakty** w kontekście profesjonalnym (Sygnalista może zgłosić fakty, które zna osobiście lub które zostały mu zgłoszone) lub poza kontekstem profesjonalnym (Sygnalista musi znać osobiście fakty, które zgłasza); oraz
- ▶ **podlegać identyfikacji**: platforma do celów zgłoszeń wymaga zidentyfikowania Sygnalisty. W wyjątkowych przypadkach dopuszcza się anonimowość, jeśli potwierdzono istotność zgłoszonych faktów lub fakty są przedstawione przy zachowaniu wystarczającej szczegółowości. Sygnalista może skorzystać ze środków ochrony (zobacz poniżej) dopiero po zniesieniu anonimowości.

Ochrona tożsamości Sygnalisty – tożsamość nie zostanie ujawniona

System zapewnia ścisłą poufność tożsamości Sygnalisty, osoby, której dotyczy zgłoszenie oraz otrzymanych informacji na każdym etapie przetwarzania zgłoszenia potencjalnej nieprawidłowości. Informacje umożliwiające zidentyfikowanie Sygnalisty:

- ▶ **nie mogą być ujawnione osobie, której dotyczy alert**, nawet jeśli wykonuje ona swoje prawa dostępu wynikające z przepisów o ochronie danych;
- ▶ **mogą być zawsze ujawnione organowi sądowemu na wezwanie**;
- ▶ poza organem sądowym – **mogą być ujawnione każdej osobie po uzyskaniu wcześniejszej zgody Sygnalisty**.

Ochrona przed potencjalnymi działaniami odwetowymi

Pod warunkiem zgłoszenia alertu zgodnie z postanowieniami niniejszego dokumentu, Sygnalista nie może być przedmiotem działań odwetowych, gróźb ani prób takich działań, nawet jeśli później fakty okażą się niedokładne lub nie dają podstawy do podjęcia działań następczych.

Ochrona przed odpowiedzialnością karną i cywilną (brak odpowiedzialności karnej i cywilnej)

Sygnalista nie może być pociągnięty do odpowiedzialności karnej, jeżeli zgłoszenie jest niezbędne i proporcjonalne, biorąc pod uwagę interesy, których dotyczy.

Sygnalista nie może być również pociągnięty do odpowiedzialności cywilnej w razie spowodowania szkody przez zgłoszenie, jeśli Sygnalista miał zasadne podstawy, aby stwierdzić, że ochrona interesów, których dotyczy zgłoszenie, była konieczna.

Inne zainteresowane strony

Ochrona obejmuje również:

- ▶ **osoby pomagające w dokonaniu zgłoszenia**, czyli wszelkie osoby fizyczne lub podmioty prawne non-profit działające na podstawie prawa prywatnego (związki zawodowe i stowarzyszenia), które zgodnie z prawem pomagają Sygnaliście dokonać zgłoszenia;
- ▶ **osoby fizyczne powiązane z Sygnalistą** (współpracownicy i rodzina);
- ▶ **podmioty prawne kontrolowane przez Sygnalistę**, na rzecz których Sygnalista pracuje lub z którymi jest powiązany w kontekście zawodowym (na przykład dostawca lub podwykonawca zewnętrzny, członkiem zarządu lub pracownikiem którego jest Sygnalista).

W razie niespełnienia powyższych warunków osoba dokonująca zgłoszenia nie korzysta z chronionego statusu Sygnalisty. Nawet bez statusu Sygnalisty **zgłoszenie dokonane w dobrej wierze nie stanowi jednak podstawy działań odwetowych**.

Sygnalista musi działać w dobrej wierze, nie może celowo przedstawiać fałszywych oskarżeń ani działać wyłącznie w celu wyrządzenia szkody i uzyskania korzyści osobistych. Każde niewłaściwe wykorzystanie Systemu Zgłaszania Nieprawidłowości lub jego wykorzystanie w złej wierze może spowodować działania dyscyplinarne, jeśli osoba dokonująca zgłoszenia jest pracownikiem. Możliwe jest także wszczęcie postępowania prawnego.

07. PRZEKAZANIE INFORMACJI OSOBIE, KTÓREJ DOTYCZY ALERT

Istniejący system obsługi alertów profesjonalnych wymaga przetwarzania danych dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych. Każda osoba będąca przedmiotem zgłoszenia, które kwalifikuje się jako dopuszczalne i staje się alertem (na przykład świadek, ofiara lub domniemany sprawca), musi otrzymać informację o przetwarzaniu jej danych w tym celu zgodnie z obowiązującymi przepisami o ochronie danych osobowych (RODO i ustawa o ochronie danych), co ma zapewnić przejrzystość. Poza tym takie osoby muszą mieć możliwość wykonywania swojego prawa dostępu, prawa do wyrażenia sprzeciwu, prawa do sprostowania danych lub prawa do usunięcia danych (zobacz: Załącznik 1).

Przekazanie takich informacji można odroczyć, jeśli takie odroczenie uznawane jest za konieczne w celu zastosowania środków ochrony ograniczających ryzyko zniszczenia dowodów.

Ze względu na poufność i w celu zachowania zgodności z przepisami o ochronie danych **osoba, której dotyczy zgłoszenie, nie może w żadnych okolicznościach uzyskać od emeis – na podstawie swojego prawa dostępu – informacji dotyczących tożsamości Sygnalisty ani żadnej innej osoby, której dotyczy postępowanie wyjaśniające.**

Tożsamość osoby, której dotyczy alert, będzie **stanowiąc informację ściśle poufną**. Elementy umożliwiające zidentyfikowanie takiej osoby mogą być ujawnione wyłącznie po ustaleniu, że zgłoszenie potencjalnej nieprawidłowości jest odpowiednio uzasadnione (o ile takich informacji nie trzeba przekazać organowi sądowemu).

08. ZGŁOSZENIE ALERTU

8.1 Kanały zgłaszania nieprawidłowości

W razie uzyskania, w kontekście swojej działalności zawodowej informacji o faktach, które zaistniały lub z wysokim prawdopodobieństwem zaistnieją w danym podmiocie, Sygnalista może zgłosić potencjalną nieprawidłowość wewnętrznie lub zewnętrznie albo wewnętrznie i zewnętrznie:

Wewnętrznie →	Zewnętrznie
Zgodnie z niniejszą procedurą dotyczącą przekazywania i przetwarzania zgłoszeń (zobacz: pkt 8.2 i 8.3 poniżej).	Zgodnie z obowiązującym prawem Sygnalista może również przekazać swój alert po zgłoszeniu go wewnętrznie albo bezpośrednio: - właściwym organom zewnętrznym wymienionym; - do Rzecznika Praw, który skieruje Sygnalistę do organu lub organów, które najlepiej zajmą się zgłoszeniem; - do organu sądowego; - do instytucji, organu lub jednostki unijnej właściwej do zbierania informacji o naruszeniach objętych zakresem wymienionej powyżej Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r.

8.2 Wewnętrzne zgłoszenie nieprawidłowości

W praktyce pracownik może zgłosić alert swojemu przełożonemu (bezpośredniemu lub pośredniemu, o ile nie jest on/on(a) przedmiotem zgłoszenia) albo za pośrednictwem platformy zgłaszania nieprawidłowości opisanej w niniejszej polityce.



Za pośrednictwem
swojego przełożonego



Za pośrednictwem platformy
do zgłaszania nieprawidłowości

Jeżeli pracownik skontaktuje się ze swoim przełożonym, rolą takiego menedżera jest pokierowanie pracownikiem oraz przekierowanie go i doradzenie mu, jak również zachęcenie go do skorzystania z Systemu Zgłaszania Nieprawidłowości w celu skontaktowania się z PAR.

emeis zachęca wszystkich Sygnalistów do korzystania z platformy do zgłaszania nieprawidłowości opisanej w pkt. 8.3, w szczególności z następujących przyczyn:

- ▶ w celu zachowania poufności i bezpieczeństwa wymiany informacji;
- ▶ w celu zapewnienia efektywności, weryfikowalności i ciągłości zarządzania zgłoszeniem nieprawidłowości;
- ▶ w celu zapewnienia przejrzystości w odniesieniu do przestrzegania zasad opisanych w niniejszym dokumencie;
- ▶ w celu ochrony Sygnalisty.

W razie dokonania zgłoszenia poza systemem zgłaszania nieprawidłowości, takie zgłoszenie może być zarejestrowane na platformie zgłaszania nieprawidłowości przez odbiorcę alertu po zawiadomieniu Sygnalisty i z poszanowaniem jego anonimowości, jeśli takie jest życzenie Sygnalisty.

8.3 Alert wewnętrzny przy pomocy platformy zgłaszania nieprawidłowości

Alerty przekazuje się za pośrednictwem platformy dostępnej pod następującym adresem:

> emeis.signalement.net

LUB

> przy pomocy następującego numeru telefonu: 01 86 47 77 67, po wpisaniu kodu 1989

Osoba dokonująca zgłoszenia ma obowiązek realizacji wymienionych poniżej kroków.

1. wybrania kategorii zgłaszanej nieprawidłowości;
2. wprowadzenia danych kontaktowych lub zachowania anonimowości;
3. dokładnego i obiektywnego opisanie faktów;
4. odpowiednio – załączenia dokumentów;
5. dokładnego przeczytania i przesłania zgłoszenia.

Podczas korzystania z platformy do zgłaszania nieprawidłowości osoba dokonująca zgłoszenia zostanie poproszona o zaklasyfikowanie swojego zgłoszenia do jednej z kategorii wymienionych w pkt. 4. Taka klasyfikacja może zostać zmieniona po analizie zgłoszenia przez PAR.

Ważne jest, aby podczas dokonywania zgłoszenia uwzględnić możliwie najwięcej informacji (dowody, dokumenty itp.), aby umożliwić PAR analizę, przetworzenie i wyjaśnienie zgłoszenia tak skutecznie, jak będzie to możliwe.

Postępowanie wyjaśniające może być trudniejsze, w szczególności, jeżeli PAR odpowiedzialny za alert nie będzie w stanie uzyskać informacji dodatkowych od anonimowego Sygnalisty. Anonimowość może również utrudnić potwierdzenie wiarygodności podejrzeń i ograniczyć skuteczność ochrony zapewnianej Sygnaliście. W każdym razie Sygnalista, który chce zachować anonimowość, powinien zapewnić PAR środki umożliwiające wymianę informacji w celu ułatwienia postępowania wyjaśniającego dotyczącego faktów, które spowodowały raport.

Po opracowaniu raportu i przesłaniu go online.

- ▶ **platforma automatycznie wydaje osobie, która dokonała zgłoszenia, poufny kod.** Kod ten stanowi osobisty identyfikator tej osoby i zapewnia poufność oraz ochronę przesłanych danych. Kod ten będzie wymagany w razie każdego nowego otwarcia zgłoszenia w celu sprawdzenia działań następnych, wprowadzenia zmian lub udzielenia odpowiedzi oraz wymiany informacji z osobą odpowiedzialną za przetworzenie zgłoszenia.
- ▶ Jednocześnie **platforma automatycznie wysyła zawiadomienie do PAR odpowiedzialnego za dany zakres.**

09. PRZETWARZANIE ALERTÓW ZGŁOSZONYCH KANAŁEM WEWNĘTRZNYM

9.1 Potwierdzenie otrzymania zgłoszenia i zawiadomienie Sygnalisty

Po dokonaniu zgłoszenia PAR ma maksymalnie **7 dni** na wysłanie pisemnego potwierdzenia otrzymania osobie, które dokonała zgłoszenia. Przesłana wiadomość będzie między innymi zawierać:

- ▶ **potwierdzenie otrzymania zgłoszenia;**
- ▶ **zasadny i przewidywalny termin** weryfikacji dopuszczalności zgłoszenia (zwykle **30 dni**, z wyjątkiem okoliczności nadzwyczajnych).

9.2 Analiza dopuszczalności zgłoszenia

PAR dokonuje niezależnej i obiektywnej weryfikacji dopuszczalności zgłoszenia, sprawdzając czy jest ono objęte zakresem Systemu.

Osoba, która dokonała zgłoszenia, może być poproszona o przedstawienie informacji dodatkowych do celów takiej analizy. Bez odpowiedzi od osoby dokonującej zgłoszenia lub jeśli przekazane informacje dodatkowe okażą się niezadowalające, zgłoszenie uznane zostanie za niedopuszczalne.

Zgłoszenia uznane za **niedopuszczalne** podlegają zamknięciu ze względu na niedopuszczalność.

Zgłoszenia uznane za **dopuszczalne** stają się alertami i przedmiotem postępowania wyjaśniającego (zobacz: pkt 9.3 poniżej).

Osoba dokonująca zgłoszenia w ciągu 30 dni od daty potwierdzenia otrzymania zgłoszenia dostaje informację o decyzji dotyczącej **dopuszczalności lub niedopuszczalności** przekazanego przez nią zgłoszenia.

9.3 Postępowanie wyjaśniające w odniesieniu do alertu

W ramach przetwarzania alertu przeprowadza się wewnętrzne i zewnętrzne postępowania wyjaśniające w celu ustalenia, czy wszystkie fakty są prawdziwe.

W zależności od alertu PAR może:

- ▶ **przetworzyć alert bezpośrednio** ze wsparciem właściwych osób z podmiotu *emeis* lub osoby z zewnątrz;
- ▶ **przekazać alert** do właściwego działu.

Termin przetworzenia alertu może różnić się w zależności od złożoności alertu, a także wymaganych badań i działań weryfikacyjnych.

9.4 Zamknięcie potencjalnego zgłoszenia

PAR zawiadomi Sygnalistę i osoby, których dotyczy alert, o wyniku i wnioskach, oraz w razie potrzeby o podjętych środkach.

Sygnalista powinien otrzymać informację w ciągu trzech [3] miesięcy od potwierdzenia otrzymania jego zgłoszenia.

10. POUFNOŚĆ

PAR i osoby zaangażowane w przetwarzanie alertu stosują **wszelkie odpowiednie środki w celu zapewnienia zgodności z obowiązującymi przepisami o ochronie danych i tajemnicy medycznej**, a także w celu **zachowania poufności informacji** podczas zbierania, przetwarzania lub przechowywania/archiwizacji.

Wszystkie alerty będą przetwarzane przy **zachowaniu ścisłej poufności** i nie będą ujawniane żadnym osobom poza odbiorcami upoważnionymi do otrzymania lub wyjaśnienia wątpliwości.

Odbiorcy alertu podlegają **rozszerzonemu zobowiązaniu do zachowania poufności**.

Elementy umożliwiające zidentyfikowanie Sygnalisty **mogą być ujawnione wyłącznie za zgodą Sygnalisty** (o ile takich informacji nie trzeba przekazać organowi sądowemu).

Elementy umożliwiające zidentyfikowanie osoby wskazanej jako sprawca w alercie mogą być ujawnione wyłącznie po ustaleniu, że alert jest dobrze uzasadniony (chyba że takie informacje trzeba przekazać organowi sądowemu).

11. MONITOROWANIE I STEROWANIE

We Francji utworzono Komitet Sterujący, który zajmuje się monitorowaniem alertów i spotyka się raz w miesiącu. Jego rola obejmuje zapewnienie należytego wdrożenia niniejszej procedury. Ma on dostęp do zestawień zgłoszeń opracowanych przez PAR. Te zestawienia zawierają otrzymane zgłoszenia potencjalnych nieprawidłowości i ich status.

W razie potrzeby Dział Zgodności (Compliance) Grupy może wprowadzić zmiany do niniejszej polityki. Takie zmiany mogą być dokonane w dowolnym momencie w celu uwzględnienia zmian przepisów oraz włączenia ustalonych nowych informacji szczegółowych.

Pierwszą wersję opracowano w 2018 r.

Wersja obowiązująca od 31 lipca 2023 r.

ZAŁĄCZNIK 1: INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH

Administrator danych

Zebrane dane osobowe są przetwarzane pod nadzorem administratora danych, którym jest emeis Polska sp. z o.o. (ul. Prosta 69, 00-838 Warszawa) oraz *emeis* S.A. (12 rue Jean Jaurès, 92800 – Puteaux - Francja).

Cele i podstawy prawne przetwarzania

Celem Systemu Zgłaszania Nieprawidłowości jest przyjmowanie zgłoszeń dotyczących postępowania i sytuacji sprzecznych z obowiązującym prawem i przepisami albo Kodeksem Etyki i CSR, a także zarządzanie tymi zgłoszeniami.

System jest wdrożony przez Grupę w celu zachowania zgodności z postanowieniami Ustawy Sapin II oraz Ustawą o obowiązku dołożenia staranności, jak również – odpowiednio – w prawnie uzasadnionym celu polegającym na zapewnieniu *emeis* i/lub spółkom zależnym *emeis* możliwości uzyskiwania informacji i podejmowania terminowych i właściwych czynności w razie naruszenia obowiązującego prawa lub przepisów.

Obowiązek prawny Grupy

System Zgłaszania Nieprawidłowości został ustanowiony przez Grupę w celu zachowania zgodności z postanowieniami Ustawy Sapin II, tak aby umożliwić „pracownikom wewnętrznym albo pracownikom zewnętrznym lub tymczasowym” podmiotu zgłaszanie:

- ▶ przestępstw lub wykroczeń;
- ▶ poważnych i oczywistych naruszeń zobowiązań międzynarodowych należycie ratyfikowanych lub zatwierdzonych przez Francję;
- ▶ poważnych i oczywistych naruszeń jednostronnych aktów organizacji międzynarodowych wydanych na podstawie takich regularnie ratyfikowanych zobowiązań międzynarodowych;
- ▶ poważnych i oczywistych naruszeń ustaw lub rozporządzeń;
- ▶ poważnych zagrożeń lub uszczerbku dla interesu ogólnego, o których osoba zgłaszająca alert ma osobistą wiedzę.

System Zgłaszania Nieprawidłowości został ustanowiony przez Grupę w celu zachowania zgodności z postanowieniami francuskiej Ustawy „o obowiązku dołożenia staranności” i umożliwieniu zgłaszania alertów dotyczących istnienia lub materializacji ryzyka poważnych naruszeń praw człowieka i podstawowych wolności, zdrowia i bezpieczeństwa osób fizycznych i środowiska, wynikających z działalności spółki oraz stron kontrolowanych bezpośrednio lub pośrednio przez spółkę w rozumieniu art. L. 233-16 ust. II, jak również z działalności podwykonawców lub dostawców, z którymi nawiązaliśmy relację komercyjną, jeśli ta działalność jest związana z tą relacją.

Prawnie uzasadniony interes realizowany przez Grupę lub przez odbiorcę danych

System Zgłaszania Nieprawidłowości jest ustanowiony przez Grupę dobrowolnie, poza wszelkimi szczególnymi zobowiązaniami prawnymi, w celu umożliwienia *emeis* i/lub spółkom zależnym *emeis* uzyskiwania informacji oraz zapewnienia im możliwości podejmowania terminowych i właściwych czynności w razie naruszenia lub podejrzanego naruszenia obowiązującego prawa lub przepisów albo kodeksu postępowania.

Odnosne danych osobowych

Dane, które mogą być przetwarzane w ramach procedury dotyczącej alertów w *emeis*, są ograniczone do:

- ▶ tożsamości, stanowiska i danych kontaktowych osoby dokonującej zgłoszenia;
- ▶ tożsamości, stanowiska i danych kontaktowych osób, których dotyczy alert;
- ▶ tożsamości, stanowiska i danych kontaktowych osób zaangażowanych w przyjęcie i/lub przetwarzanie alertu;
- ▶ zgłoszonych faktów;
- ▶ elementów zbieranych w celu weryfikacji zgłoszonych faktów;
- ▶ sprawozdania z działań weryfikacyjnych;
- ▶ dalszych podejmowanych działań;
- ▶ danych dotyczących stanu zdrowia, danych ujawniających pochodzenie rasowe lub etniczne i przekonania religijne, danych dotyczących życia i orientacji seksualnej, poglądów politycznych lub przynależności do związków zawodowych, jeżeli przetwarzanie tych danych jest niezbędne w celu ustalenia, dochodzenia lub obrony prawa w sądzie;
- ▶ informacji odnoszących się do naruszeń prawa lub wyroków wydanych wobec danej osoby, jeśli przetwarzanie jest dozwolone przez prawo krajowe lub w celu umożliwienia Grupie przygotowania, podjęcia i realizacji postępowania prawnego w charakterze ofiary lub pozwanego albo w imieniu ofiary lub pozwanego.

Odbiorcy danych

Dane osobowe przetwarzane w ramach Systemu Zgłaszania Nieprawidłowości są przeznaczone wyłącznie dla osób upoważnionych, czyli:

- ▶ wewnątrz: osób odpowiedzialnych w szczególności za zarządzanie alertami w ramach Grupy, PAR, komitetu sterującego zajmującego się monitorowaniem alertów (we Francji i na poziomie lokalnym);
- ▶ zewnątrz: organów sądowych, podwykonawcy administrującego platformę do zarządzania alertami.

Przekazywanie poza Unię Europejską (UE)

Do celów zarządzania profesjonalną platformą do zgłaszania nieprawidłowości Grupa korzysta z podwykonawcy znajdującego się we Francji, który częściowo musi podzlecać tę usługę osobie trzeciej znajdującej się poza UE. Pracownicy tej osoby trzeciej fizycznie znajdują się poza UE.

W celu zapewnienia ram tego przekazywania danych oraz zgodnie z RODO podpisano standardowe klauzule umowne i zapewniono poziom ochrony danych osobowych odpowiadający przynajmniej poziomowi ochrony zapewnianemu w krajach UE.

Okresy przechowywania danych osobowych

Dane osobowe zbierane i przetwarzane w związku z Systemem Zgłaszania Nieprawidłowości są przechowywane wyłącznie przez okres niezbędny w zamierzonym celu, jak opisano poniżej:

- ▶ Jeżeli zgłoszenie zostanie uznane za niedopuszczalne (co oznacza, że nie stanowi ono alertu), dane zostaną bezzwłocznie usunięte lub zanonimizowane.
- ▶ Jeżeli zgłoszenie zostanie uznane za dopuszczalne (czyli będzie stanowić alert), ale zostanie zamknięte bez dalszych działań po postępowaniu wyjaśniającym, dane zostaną zachowane przez dwa (2) miesiące od zamknięcia weryfikacji, a następnie zostaną usunięte lub zanonimizowane.
- ▶ Jeżeli fakty wynikające z alertu zostaną potwierdzone, ale nie będą stanowić podstawy postępowania dyscyplinarnego lub prawnego, dane zostaną zachowane przez 6 (sześć) lat, a następnie zostaną usunięte (lub zanonimizowane).
- ▶ Jeżeli alert spowoduje podjęcie postępowania dyscyplinarnego lub prawnego przeciwko osobie, której dotyczy, lub osobie, która zgłosiła niewłaściwy alert, dane zostaną zachowane do końca postępowania oraz do wygaśnięcia terminu na wniesienie potencjalnego odwołania od decyzji.

Wykonywanie praw związanych z przetwarzaniem danych osobowych

Zgodnie z art. 15 *et seq.* RODO każda osoba, której dane dotyczą i której dane są zbierane i przetwarzane przy pomocy Systemu Zgłaszania Nieprawidłowości ma prawo do żądania od *emeis* lub dowolnej spółki zależnej *emeis*, jeśli zgłoszenie dokonywane jest przez pracownika albo jednego z jej współpracowników zewnętrznych albo zgłoszone fakty dotyczą takiej spółki zależnej, dostępu do swoich danych, ich sprostowania oraz – pod warunkiem spełnienia określonych warunków – usunięcia danych, jak również ograniczenia ich przetwarzania, a poza tym ma prawo do wniesienia sprzeciwu wobec takiego przetwarzania i prawo do przenoszenia danych osobowych.

Poza tym zgodnie z francuską Ustawą o ochronie danych i wolności obywatelskiej każda osoba, której dane dotyczą, ma prawo do wydania instrukcji dotyczących zachowania, usunięcia i przekazywania jej danych osobowych po jej śmierci.

Każda osoba, której dane dotyczą, może wykonać swoje prawa poprzez przesłanie pisemnej wiadomości na adres e-mail: dpo@emeis.com, przedstawiając w wiadomości swoje żądanie i dowód tożsamości. Takie żądanie można również przekazać na piśmie na następujący adres korespondencyjny: *emeis* – Inspektor Ochrony Danych, 12 rue Jean Jaurès, CS 10032, 92 813 Puteaux Cedex.

Każda osoba może również wnieść skargę do Commission Nationale de l'Informatique et des Libertés („Cnil”) na następujący adres: 3 place de Fontenoy – TSA 80715 – 75334 Paryż Cedex 07.