

**Zarządzenie nr 2/2024**

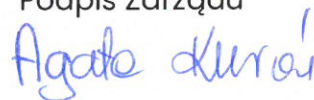
**Prezesa Zarządu Spółki Liber Sp. z o. o.**

**z dnia 25.09.2024 r.**

w sprawie przyjęcia wewnętrznej procedury zgłaszania naruszeń i podejmowania działań następczych.

Zarząd Spółki Liber Sp. z o. o. z dniem 25.09.2024 roku ustanawia wewnętrzną procedurę zgłaszania naruszeń i podejmowania działań następczych na podstawie ustawy z dnia 14 czerwca 2024 roku o ochronie sygnalistów, w związku z przepisami art. 8 i 9 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r.

Podpis Zarządu





# **Procedura zgłaszania naruszeń prawa i podejmowania działań następnych w Liber Spółka z ograniczoną odpowiedzialnością**

Na podstawie ustawy z dnia 14 czerwca 2024 o ochronie sygnalistów, w związku z przepisami art. 8 i 9 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii, ustanawia się wewnętrzną procedurę zgłaszania naruszeń prawa i podejmowania działań następnych, zwaną dalej „procedurą zgłoszeń wewnętrznych”, w brzmieniu określonym niżej.

25.09.2024r. *Apade kund*

data i podpis osoby / osób uprawnionych w spółce

## **1. Postanowienia ogólne**

### **1.1 Powierzenie zadań**

Zadania związane z przyjmowaniem zgłoszeń oraz prowadzeniem działań następnych wykonują:

- a) Administrator Systemu Zgłoszeniowego (dalej „Administrator”),

Administradora wyznacza zarząd spółki.

### **1.2 Obowiązek pomocy**

Pracownicy i zleceniobiorcy spółki są zobowiązani do udzielania pomocy Administratorowi w realizacji zadań przewidzianych procedurą.

### **1.3 Kim jest sygnalista?**

Sygnalistą jest osoba przekazująca zgłoszenie:

- a) wyznaczonym kanałem zgłoszeniowym,
- b) w dobrej wierze (przekazuje informacje, które uważa za prawdziwe),
- c) w kontekście związanym z pracą (mające związek z funkcjonowaniem zakładu pracy).

### **1.4 Ochrona tożsamości sygnalisty**

Tożsamość sygnalisty, który podał swoje imię i nazwisko, podlega ochronie. Dostęp do danych sygnalisty posiada wyłącznie Administrator.

Tożsamość sygnalisty może zostać ujawniona właściwym organom państwowym na ich żądanie oparte w przepisach prawa.

Ujawnienie tożsamości sygnalisty w innych przypadkach lub innym osobom jest możliwe jedynie za jego wyraźną, udokumentowaną zgodą, chyba że ujawnienie jest koniecznym i proporcjonalnym obowiązkiem wynikającym z przepisów prawa w związku z postępowaniami wyjaśniającymi prowadzonymi przez organy publiczne lub postępowaniami przygotowawczymi lub sądowymi

prowadzonymi przez sądy, w tym w celu zagwarantowania prawa do obrony przysługującego osobie, której dotyczy zgłoszenie.

Zakazuje się ujawniania tożsamości sygnalisty oraz danych pozwalających na jej ustalenie innym osobom. Zakaz obowiązuje wszystkie osoby, bez względu na to w jaki sposób weszły w posiadanie danych o tożsamości sygnalisty lub innych danych pozwalających na ustalenie tożsamości sygnalisty.

Wszystkie osoby, które wykonując czynności służbowe lub w innych okolicznościach zapoznały się ze zgłoszeniem sygnalisty, jak również innymi informacjami dotyczącymi zgłoszenia, są zobowiązane do zachowania poufności.

Powyższe zasady ochrony tożsamości odnoszą się także do osób pomagających dokonać zgłoszenia, jeżeli ich dane są znane osobom przyjmującym zgłoszenie.

### **1.5 Zakaz działań odwetowych**

Sygnaliści podlegają ochronie.

Zakazuje się podejmowania wobec sygnalistów działań odwetowych i prób takich działań, w szczególności w następujących formach:

**W stosunku do osób, które są, były lub mają być związane stosunkiem pracy:**

- 1) odmowie nawiązania stosunku pracy;
- 2) wypowiedzeniu lub rozwiązaniu bez wypowiedzenia stosunku pracy;
- 3) niezawarciu umowy o pracę na czas określony lub umowy o pracę na czas nieokreślony po rozwiązaniu umowy o pracę na okres próbny, niezawarciu kolejnej umowy o pracę na czas określony lub niezawarciu 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;
- 4) obniżeniu wysokości wynagrodzenia za pracę;
- 5) wstrzymaniu awansu albo pominięciu przy awansowaniu;
- 6) pominięciu przy przyznawaniu innych niż wynagrodzenie świadczeń związanych z pracą lub obniżeniu wysokości tych świadczeń;
- 7) przeniesieniu na niższe stanowisko pracy;
- 8) zawieszeniu w wykonywaniu obowiązków pracowniczych lub służbowych;
- 9) przekazaniu innemu pracownikowi dotychczasowych obowiązków sygnalisty;
- 10) niekorzystnej zmianie miejsca wykonywania pracy lub rozkładu czasu pracy;
- 11) negatywnej ocenie wyników pracy lub negatywnej opinii o pracy;
- 12) nałożeniu lub zastosowaniu środka dyscyplinarnego, w tym kary finansowej, lub środka o podobnym charakterze;
- 13) przymusie, zastraszaniu lub wykluczeniu;
- 14) mobbingu;
- 15) dyskryminacji;
- 16) niekorzystnym lub niesprawiedliwym traktowaniu;

- 17) wstrzymaniu udziału lub pominięciu przy typowaniu do udziału w szkoleniach podnoszących kwalifikacje zawodowe;
- 18) nieuzasadnionym skierowaniu na badania lekarskie, w tym badania psychiatryczne, chyba że przepisy odrębne przewidują możliwość skierowania pracownika na takie badania;
- 19) działaniu zmierzającym do utrudnienia znalezienia w przyszłości pracy w danym sektorze lub w danej branży na podstawie nieformalnego lub formalnego porozumienia sektorowego lub branżowego;
- 20) spowodowaniu straty finansowej, w tym gospodarczej, lub utraty dochodu;
- 21) wyrządzeniu innej szkody niematerialnej, w tym naruszeniu dóbr osobistych, w szczególności dobrego imienia sygnalisty.

**W stosunku do osób, które są, były lub mają być związane stosunkiem innym niż stosunek pracy:**

- 1) wypowiedzenie umowy, której stroną jest sygnalista, w szczególności dotyczącej sprzedaży lub dostawy towarów lub świadczenia usług, odstąpienie od takiej umowy lub rozwiązanie jej bez wypowiedzenia;
- 2) nałożenie obowiązku lub odmowę przyznania, ograniczenie lub odebranie uprawnienia, w szczególności koncesji, zezwolenia lub ulgi.

Z ochrony przed działaniami odwetowymi korzystają także:

- a) osoby pomagające dokonać zgłoszenia,
- b) inne osoby powiązane z sygnalistami, które mogą doświadczyć działań odwetowych w kontekście związanym z pracą, takie jak współpracownicy lub krewni sygnalistów,
- c) osoby prawne, które stanowią własność sygnalisty,
- d) osoby fizyczne i prawne, dla których sygnalista pracuje lub które są w inny sposób z nim powiązane w kontekście związanym z pracą,
- e) osoby wykonujące czynności przewidziane niniejszą procedurą,
- f) świadkowie składający wyjaśnienia podczas postępowania wyjaśniającego.

## **1.6 Zgłaszanie ujawnienia tożsamości lub działań odwetowych**

Sygnaliści i inne osoby korzystające z ochrony, wobec których podejmowane są działania odwetowe lub których chroniona tożsamość została ujawniona - zgłaszają ten fakt Administratorowi lub zarządowi spółki, w celu podjęcia stosownych działań.

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.

## **1.7 Pomówienia**

Świadome zgłaszanie informacji nieprawdziwych, w szczególności w celu pomówienia innej osoby lub w celu uzyskania własnych korzyści, traktowane jest jako działanie niezgodne z zasadami etyki obowiązującymi w firmie i godzące w zasady współżycia społecznego obowiązujące w zakładzie pracy.

W stosunku do osoby, która w sposób celowy i świadomy dokonuje zgłoszenia w trybie niniejszej procedury w celu pomówienia innej osoby lub w celu uzyskania własnych korzyści, mogą zostać

wyciągnięte konsekwencje dyscyplinarne lub inne przewidziane umową lub powszechnie obowiązującymi przepisami prawa.

### **1.8 Przetwarzanie danych osobowych**

- a) Po otrzymaniu zgłoszenia, dane osobowe przetwarzane są w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnych działań następnych. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia nie są zbierane, a w razie przypadkowego zebrania, są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.
- b) Dane osobowe oraz pozostałe informacje w rejestrze zgłoszeń wewnętrznych są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następne lub po zakończeniu postępowań zainicjowanych tymi działaniami.
- c) W przypadku złożenia wniosku o sprostowanie danych, w celu zachowania wartości dowodowej stosuje się zasadę dodatkowych wpisów uzupełniających dokumentację z postępowania, a nie zastępowania danych zawartych w zgłoszeniu lub dokumentacji.
- d) W zakresie nieokreślonym procedurą, zasady ochrony i przetwarzania danych osobowych w procesie przyjmowania zgłoszeń i prowadzenia działań następnych, w tym wydawania upoważnień do ich przetwarzania, określone są w dokumentach spółki regulujących przetwarzanie i ochronę danych osobowych.

### **1.9 Informacja o kanałach zgłoszeniowych**

Administrator lub osoba przez niego wyznaczona informuje o kanałach zgłoszeniowych pracowników i zleceniobiorców spółki oraz zamieszcza informację o kanałach na stronie internetowej spółki.

## **2. Zakres stosowania procedury**

### **2.1 Jakie naruszenia są rozpatrywane?**

W trybie niniejszej procedury rozpatruje się zgłoszenia naruszeń:

- a) przepisów prawa powszechnie obowiązującego, polegające na działaniu lub zaniechaniu niezgodnym z prawem lub mającym na celu obejście prawa w zakresie:
  - 1) korupcji;
  - 2) zamówień publicznych;
  - 3) usług, produktów i rynków finansowych;
  - 4) przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
  - 5) bezpieczeństwa produktów i ich zgodności z wymogami;
  - 6) bezpieczeństwa transportu;
  - 7) ochrony środowiska;
  - 8) ochrony radiologicznej i bezpieczeństwa jądrowego;
  - 9) bezpieczeństwa żywności i pasz;
  - 10) zdrowia i dobrostanu zwierząt;
  - 11) zdrowia publicznego;
  - 12) ochrony konsumentów;
  - 13) ochrony prywatności i danych osobowych;
  - 14) bezpieczeństwa sieci i systemów teleinformatycznych;
  - 15) interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, jednostki samorządu terytorialnego oraz Unii Europejskiej;



- 16) rynku wewnętrznego Unii Europejskiej, w tym publicznoprawnych zasad konkurencji i pomocy państwa oraz opodatkowania osób prawnych;
- 17) konstytucyjnych wolności i praw człowieka i obywatela – występujące w stosunkach jednostki z organami władzy publicznej i niezwiązane z dziedzinami wskazanymi w pkt 1–16.

- b) regulacji wewnętrznych obowiązujących w spółce,
- c) standardów etycznych obowiązujące w spółce.

Rozpatrywane są jedynie naruszenia, które mają związek lub mogą mieć wpływ na działalność spółki.

Nie są rozpatrywane zgłoszenia dotyczące spraw prywatnych pracowników, które nie mają związku z funkcjonowaniem zakładu pracy.

Zgłoszenia dotyczące podejrzenia prania pieniędzy i finansowania terroryzmu (AML) są przekazywane do rozpatrzenia w trybie osobnej procedury.

## **2.2 Czyje zgłoszenia są rozpatrywane?**

Procedurę stosuje się do zgłoszeń dokonanych przez osoby fizyczne, które uzyskały informacje na temat naruszeń w kontekście związanym z pracą, sygnalistą może być:

- 1) pracownik;
- 2) pracownik tymczasowy;
- 3) osoba świadcząca pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej;
- 4) przedsiębiorca;
- 5) prokurent;
- 6) akcjonariusz lub wspólnik;
- 7) członek organu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej;
- 8) osoba świadcząca pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy;
- 9) stażysta;
- 10) wolontariusz;
- 11) praktykant;
- 12) funkcjonariusz w rozumieniu art. 1 ust. 1 ustawy z dnia 18 lutego 1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin (Dz. U. z 2023 r. poz. 1280, 1429 i 1834);
- 13) żołnierz w rozumieniu art. 2 pkt 39 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2024 r. poz. 248 i 834). Administrator może zdecydować, aby niniejszą procedurę zastosować odpowiednio do zgłoszeń pochodzących z innych źródeł wewnętrznych i zewnętrznych.

Ustawę stosuje się także do osoby fizycznej, o której mowa w punkcie 2.2, w przypadku zgłoszenia lub ujawnienia publicznego informacji o naruszeniu prawa uzyskanej w kontekście związanym z pracą

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 pełnienia służby w podmiocie prawnym lub już po ich ustaniu.

### **2.3 Zgłoszenia podpisane i anonimowe**

Procedurę stosuje się do rozpatrywania zgłoszeń podpisanych i anonimowych.

W przypadku zgłoszeń anonimowych, jeśli nie ma możliwości kontaktu z sygnalistą, nie stosuje się punktów procedury dotyczących informowania sygnalisty.

## **3. Kanały zgłoszeniowe i przyjmowanie zgłoszeń**

### **3.1 Kanały zgłoszeniowe**

Sygnalista ma możliwość dokonania zgłoszeń:

- a) Wewnętrznych
  - Poufnym kanałem zgłoszeni firmy znajdującym się pod adresem:  
<https://panel.amlex.pl/SygnFirmy/SecurePage/678c4d0c1ce2497d828748aa94a7fba0>

Zgłoszenia wewnętrzne przyjmuje Administrator.

- b) Zewnętrznych

- Kierowanych do odpowiednich organów publicznych, takich jak:

Rzecznik Praw Obywatelskich

Urzędy regulacyjne dla danej branży (np. zdrowotnej)

Instytucje państwowe nadzorujące i egzekwujące przestrzeganie prawa

Zgłoszenia Zewnętrznego sygnalista może dokonać w dowolnym momencie, nie ma obowiązku dokonywania w pierwszej kolejności zgłoszenia Wewnętrznego.

Informacje o kanałach zgłoszeń zewnętrznych dla każdej z instytucji znajdują się na ich stronach internetowych. W przypadku Rzecznika Praw Obywatelskich znajduje się ona pod adresem: <https://bip.brpo.gov.pl/pl/content/zlozenie-wniosku-do-rzecznika-praw-obywatelskich>.

### **3.2 Rekomendowany zakres informacji w zgłoszeniu**

Aby zgłoszenie mogło zostać skutecznie rozpatrzone powinno zawierać informacje umożliwiające jego zbadanie.

Zgłoszenie powinno zawierać następujące dane:

- a) imię i nazwisko oraz kontakt do osoby zgłaszającej (chyba, że sygnalista chce pozostać anonimowy lub nie chce podać danych do kontaktu)
- b) zakres naruszeń – jakich przepisów prawnych lub standardów wewnętrznych dotyczyło naruszenie?
- c) kto jest podejrzewany o dokonanie naruszenia?
- d) kiedy / w jakim okresie / od kiedy dochodzi do naruszeń?
- e) gdzie dochodzi lub dochodziło do naruszeń?
- f) jaki jest sposób ich popełniania?
- g) jakie mogą być motywy sprawców?



- h) czy sygnalista ma jakieś dowody na popełnianie naruszeń (np. dokumenty, zdjęcia)? Jeśli tak - należy je dołączyć do zgłoszenia.

Niezależnie od formy zgłoszenia sygnalista powinien postarać się odpowiedzieć na jak najwięcej z powyższych pytań i załączyć posiadane dowody.

Należy jednak pamiętać, że sygnalista może nie znać odpowiedzi na wszystkie powyższe pytania. Nie wstrzymuje to rozpatrywania zgłoszenia.

## **4. Rejestr zgłoszeń i przechowywanie dokumentacji**

### **4.1 Zakres danych w rejestrze**

Rejestr zgłoszeń prowadzony jest w formie elektronicznej w programie AMLEX przez podmiot wspierający. Zawiera następujące dane:

- 1) numer zgłoszenia;
- 2) przedmiot naruszenia prawa;
- 3) dane osobowe sygnalisty oraz osoby, której dotyczy zgłoszenie, niezbędne do identyfikacji tych osób;
- 4) adres do kontaktu sygnalisty;
- 5) datę dokonania zgłoszenia;
- 6) informację o podjętych działaniach następnych;
- 7) datę zakończenia sprawy.

Rejestr prowadzi się w sposób zapewniający bezpieczeństwo i integralność, w tym ochronę przed nieuprawnionym dostępem i poufność danych osobowych.

### **4.2 Przechowywanie dokumentacji**

Dokumentację zgłoszeń i prowadzonych działań następnych przechowuje się w sposób zapewniający jej bezpieczeństwo i integralność, w tym ochronę przed nieuprawnionym dostępem i poufność danych osobowych.

### **4.3 Dostęp do rejestru i dokumentacji**

Prawo dostępu do rejestru zgłoszeń i dokumentacji posiadają:

- Administrator,

## **5. Ochrona osób, których dotyczy zgłoszenie**

### **5.1 Ochrona dobrego imienia i tożsamości**

Zgłoszenie może dotyczyć konkretnej osoby (osób) lub osób nieustalonych co do tożsamości. Podejrzenia odnośnie do konkretnych osób mogą pojawić się także w trakcie czynności wyjaśniających.

Osoby te mają prawo do ochrony swojego dobrego imienia oraz ochrony tożsamości przez cały okres prowadzenia działań następnych, a jeżeli zarzuty się nie potwierdzą – także po ich zakończeniu.

## **5.2 Domniemanie niewinności**

Osoby, których dotyczy zgłoszenie lub odnośnie do których podejrzenia naruszeń pojawiają się później – korzystają z domniemanie niewinności. Oznacza to, że ewentualne konsekwencje służbowe wobec nich można zastosować dopiero wtedy, gdy wyniki postępowania wyjaśniającego potwierdzą, że są winne naruszeń.

Nie stanowi naruszenia domniemanie niewinności podjęcie czynności mających na celu zabezpieczenie prawidłowego toku postępowania, jak np. czasowe ograniczenie uprawnień dostępu do pomieszczeń lub systemów informatycznych, przeprowadzone w sposób, który nie dyskredytuje danej osoby w oczach współpracowników.

## **5.3 Prawo do obrony**

Osoby, których dotyczy zgłoszenie lub odnośnie do których podejrzenia naruszeń pojawiają się później – korzystają z prawa do obrony.

Na właściwym etapie postępowania, przed formułowaniem ostatecznych wniosków, mają prawo do zapoznania się z zebranymi dowodami, przedstawienia swoich argumentów oraz korzystania z pomocy prawnej.

Prawo do zapoznania się z dowodami nie obejmuje dostępu do zgłoszenia przekazanego przez sygnalistę.

## **5.4 Naruszenie zasad**

W przypadku naruszenia wymienionych wyżej zasad, osoby pokrzywdzone mogą złożyć skargę do zarządu spółki lub do właściwych organów zewnętrznych.

## **6. Ocena właściwości zgłoszenia**

Po wpłynięciu zgłoszenia Administrator sprawdza czy podlega ono rozpatrzeniu w ramach niniejszej procedury. A mianowicie, czy zgłoszenie spełnia warunki określone w punktach 2.1 i 2.2.

Jeżeli podlega ono rozpatrzeniu w ramach innej procedury, przekazuje się je do rozpatrzenia w innym trybie wewnętrznym.

Jeżeli do rozpatrzenia sprawy właściwy jest organ zewnętrzny – zgłoszenie przekazuje się temu organowi.

Jeżeli zgłoszenie dotyczy Administratora lub naruszeń występujących przy realizacji niniejszej procedury – decyzję o sposobie dalszego postępowania podejmuje prezes zarządu spółki.

Jeżeli zgłoszenie zawiera zbyt mało informacji, aby móc je prawidłowo zakwalifikować – Administrator prosi sygnalistę o uzupełnienie przekazanych informacji.

## **7. Rejestracja zgłoszenia**

Administrator rejestruje w rejestrze zgłoszeń zgłoszenia wpływające wszystkimi kanałami zgłoszeniowymi.

W przypadku zgłoszeń niepodlegających rozpatrzeniu wg. niniejszej procedury wpisuje się do rejestru informację o przekazaniu zgłoszenia wg. właściwości (kiedy i komu) lub o zamknięciu zgłoszenia bez rozpatrzenia.

W przypadku ponowienia zgłoszenia, które zostało już wcześniej wyjaśnione, gdy ponowione zgłoszenie nie zawiera dodatkowych informacji – Administrator może zdecydować o pozostawieniu zgłoszenia bez rozpatrzenia lub natychmiastowym jego zamknięciu.

## **8. Potwierdzenie przyjęcia zgłoszenia**

Bez zbędnej zwłoki, w terminie nie dłuższym niż 7 dni kalendarzowych od wpłynięcia zgłoszenia (lub uzupełnienia informacji pozwalających na jego zakwalifikowanie), Administrator:

- informuje sygnalistę o przyjęciu zgłoszenia
- informuje nadawcę o skierowaniu sprawy do rozpatrzenia w innym trybie wewnętrznym lub do organu zewnętrznego (w przypadku zgłoszeń, które są rozpatrywane na podstawie innych procedur wewnętrznych lub innych przepisów prawnych),
- może poinformować nadawcę o pozostawieniu zgłoszenia bez rozpatrzenia wraz z podaniem przyczyn (w przypadku pozostałych zgłoszeń).

Powyższe czynności podejmuje się, jeżeli sposób zgłoszenia umożliwia kontakt z sygnalistą lub nadawcą (np. podano dane kontaktowe).

## **9. Zasada należytej staranności**

Każde zgłoszenie należy rozpatrywać z należytą starannością, obiektywnie i dociekliwie, bez względu na to, kogo i jakiej sprawy dotyczy.

## **10. Zasady prowadzenia działań następnych**

### **10.1 Co to są działania następne?**

Działania następne to działania podejmowane po przyjęciu zgłoszenia w celu jego zbadania i wyjaśnienia. Składają się z dwóch etapów:

- a) postępowania przygotowawczego
- b) postępowania wyjaśniającego

### **10.2 Kto prowadzi działania następne?**

Działania następne prowadzi Administrator.

Jeśli jest to konieczne, może korzystać z pomocy ekspertów będących pracownikami firmy lub ekspertów zewnętrznych. Eksperci wykonują czynności na podstawie pisemnego upoważnienia Administratora w zakresie nadanego upoważnienia.

W przypadku ekspertów zewnętrznych podstawą współpracy jest zawarta umowa wraz z oświadczeniami w zakresie ochrony danych osobowych oraz zachowania poufności.

Ekspertem nie może zostać sygnalista ani osoba, której dotyczy zgłoszenie.

### **10.3 Uprawnienia osób prowadzących działania następne**

W trakcie prowadzenia działań następnych Administrator oraz eksperci mają prawo:

- dostępu do dokumentów i danych spółki,
- uzyskiwania ustnych i pisemnych wyjaśnień od pracowników i zleceniobiorców spółki oraz innych osób mających wiedzę w sprawie,
- dostępu do danych z monitoringu wizyjnego,

- dostępu do pomieszczeń spółki w celu dokonania wizji lokalnej lub przeszukania i zabezpieczenia dowodów,
- korzystania z pomocy inspektora ochrony danych osobowych,
- korzystania z pomocy kadry kierowniczej i pracowników spółki w trakcie prowadzonych czynności,
- konsultowania, w niezbędnym zakresie, uzyskanych informacji i danych z sygnalistą.

#### **10.4 Uprawnienia dodatkowe**

W uzasadnionych przypadkach, Administrator oraz eksperci mogą otrzymać upoważnienie do zbadania lub monitorowania informacji i danych służbowych przetwarzanych przez pracownika firmy na sprzęcie służbowym, a w szczególności:

- służbowej poczty elektronicznej,
- danych na dyskach służbowych komputerów i w służbowej chmurze,
- aktywności sieciowej i komputerowej użytkownika,
- bilingów i danych na służbowych telefonach,
- logowania użytkowników do aplikacji,
- wykorzystywania nielegalnego oprogramowania,
- nadużycia nadanych uprawnień w systemach informatycznych.

Upoważnienia udziela prezes zarządu spółki w formie pisemnej, po konsultacji z inspektorem ochrony danych osobowych (jeżeli taki został powołany). W upoważnieniu określa się zakres badanych lub monitorowanych informacji i danych.

#### **10.5 Ograniczenia i poufność**

W ramach działań następczych nie wolno stosować środków zarezerwowanych dla uprawnionych służb państwowych, takich jak np. zakładanie podsłuchów czy kontrola operacyjna (prowokacje).

Osoby prowadzące działania następcze prowadzą je w sposób zapewniający ochronę informacji przed dostępem osób nieupoważnionych. Są zobowiązane do zachowania uzyskanych informacji w poufności.

### **11. Postępowanie przygotowawcze**

#### **11.1 Cel i zakres**

Celem postępowania przygotowawczego jest wstępna analiza zgłoszenia.

Przeprowadza ją Administrator na podstawie danych i dokumentów dostępnych w spółce oraz dostępnych publicznie. Na tym etapie nie prowadzi rozmów wyjaśniających.

W razie potrzeby może konsultować się z sygnalistą.

Postępowanie przygotowawcze powinno zostać przeprowadzone w sposób ograniczający ryzyko zniszczenia dowodów w sprawie, której dotyczy zgłoszenie.

#### **11.2 Postępowanie w przypadku zgłoszenia zbyt ogólnego**

Jeżeli informacje przekazane przez sygnalistę są zbyt ogólne, aby móc je zweryfikować i nie udaje się otrzymać od niego informacji bardziej szczegółowych – można zawiesić sprawę do czasu uzyskania niezbędnych informacji, a po 3 miesiącach ją zamknąć.

Jeżeli po zamknięciu sprawy wpłyną skonkretyzowane informacje umożliwiające zbadanie zgłaszanych naruszeń – wznowia się działania następcze tworząc nowe zgłoszenie z datą uzyskania tych informacji.

### **11.3 Postępowanie w przypadku wyjaśnienia sprawy na tym etapie**

Jeżeli analiza danych i dokumentów jest wystarczająca do oceny stanu faktycznego, a zarzuty wobec osoby, której dotyczy zgłoszenie, się nie potwierdzają, to Administrator zamyka zgłoszenie zamieszczając w nim informacje o podjętych działaniach następczych.

### **11.4 Pozostałe przypadki**

Jeżeli analiza danych i dokumentów na etapie postępowania przygotowawczego nie jest wystarczająca do ustalenia stanu faktycznego, a w szczególności zachodzi konieczność umożliwienia prawa do obrony osobie, której dotyczy zgłoszenie – należy przejść do etapu postępowania wyjaśniającego.

## **12. Postępowanie wyjaśniające**

### **12.1 Cel i zakres**

Celem postępowania wyjaśniającego jest ustalenie stanu faktycznego.

Postępowanie jest prowadzone z uwzględnieniem postanowień procedury w sprawie ochrony tożsamości sygnalisty oraz innych osób przewidzianych w procedurze.

W przypadku wpłynięcia kilku zgłoszeń o podobnych naruszeniach można w ramach jednego postępowania wyjaśniającego badać kilka zgłoszeń jednocześnie.

### **12.2 Zabezpieczenie prawidłowego toku postępowania**

W razie potrzeby zapewnienia prawidłowego toku postępowania Administrator może wystąpić do prezesa zarządu spółki z wnioskiem o:

- zabezpieczenie i przekazanie określonych dowodów,
- odsunięcie od określonych zadań pracownika / pracowników, których dotyczy / może dotyczyć zgłoszenie,
- czasowe pozbawienie ich określonych uprawnień dostępu do danych lub pomieszczeń,
- inne działania zabezpieczające prawidłowy tok postępowania.

Jeżeli Administratorem jest prezes zarządu spółki – to podejmuje takie decyzje samodzielnie.

### **12.3 Uzyskiwanie wyjaśnień**

Częścią postępowania wyjaśniającego jest uzyskiwanie ustnych i pisemnych wyjaśnień od pracowników i zleceńbiorców spółki oraz innych osób mających wiedzę w sprawie.

Na odpowiednim etapie, przed zamknięciem zgłoszenia, należy umożliwić prawo do obrony osobom, które są podejrzewane o dokonanie naruszeń, zgodnie z punktem 5.3 procedury.

## **13. Działania związane ze zgłoszeniem**

Administrator na skutek zgłoszenia podejmuje decyzje o podjęciu działań w organizacji. Mogą one obejmować między innymi:



- zamknięcie procedury bez podejmowania dalszych działań (w wypadku niepotwierdzenia się zgłoszenia),
- przeprowadzenie rozmowy, zwrócenie uwagi pracownikowi,
- upomnienie pracownika, pozbawienie nagrody, premii itp.
- zmiany lub rotacje na stanowiskach,
- wnioski prewencyjne o charakterze zarządczym lub organizacyjnym,
- zmiany w wewnętrznych procedurach,
- podjęcie działań cywilnoprawnych, dotyczących np. zawartych umów, naprawienia szkody, wypłacenia odszkodowania,
- złożenie wniosku o wszczęcie postępowania dyscyplinarnego / służbowego,
- złożenie zawiadomienia do UOKiK lub innych właściwych organów i urzędów,
- złożenie zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa (w przypadku zgromadzenia dowodów),
- poinformowanie właściwych służb (w przypadku zgromadzenia poszlak),
- podjęcie działań prawnych w przypadku uzasadnionego podejrzenia, że osoba dokonująca zgłoszenia nie miała uzasadnionych podstaw sądzić, że będąca przedmiotem zgłoszenia informacja o naruszeniu prawa jest prawdziwa w momencie dokonywania zgłoszenia.

Prezes zarządu spółki zatwierdza działania oraz wyznacza osoby odpowiedzialne za ich realizację.

## **14. Działania końcowe**

Administrator uzupełnia w zgłoszeniu wykonane i planowane działania następne, a następnie w terminie maksymalnie 3 miesięcy od przyjęcia zgłoszenia przekazuje sygnaliście informacje zwrotne. Czynności te wykonywane są za pomocą elektronicznego systemu zgłoszeń wewnętrznych obowiązującego w organizacji.

W przypadku, jeżeli wyjaśnianie zgłoszenia trwa dłużej – sygnalista w terminie 3 miesięcy od zgłoszenia otrzymuje informację zwrotną i ma możliwość dalszego monitorowania zgłoszenia w elektronicznym systemie zgłoszeń.

Administrator może zamknąć zgłoszenie:

- niezwłocznie, w przypadku gdy nie spełnia ono kryteriów przyjęcia,
- po zakończeniu działań następnych.

W momencie zamknięcia zgłoszenia sygnalista zostanie o tym poinformowany za pośrednictwem systemu, oraz jeśli podał w zgłoszeniu adres email również za pomocą poczty elektronicznej.

Załącznik nr 1

Warszawa, 25.09.2024 r.

**Wyznaczenie Administratora Systemu Zgłoszeniowego**

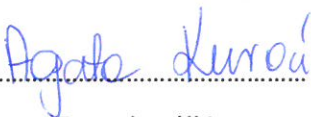
**Liber Spółka z ograniczoną odpowiedzialnością**

**04-639 Warszawa, ul. Zorzy 34/23**

**NIP 5322050992**

Na Administratora Systemu Zgłoszeniowego wyznacza się Agatę Kuroń.

Administrator będzie pełnił swoją funkcję od dnia 25.09.2024 r. do odwołania.

  
.....  
Zarząd spółki



# **Polityka prywatności Liber Spółka z ograniczoną odpowiedzialnością**

## **&1.**

### **POSTANOWIENIA OGÓLNE**

1. Administratorem danych osobowych jest Liber Spółka z ograniczoną odpowiedzialnością z siedzibą 04-639 Warszawa, ul. Zorzy 34/23, Nip 5322050992, Regon 360988604, Krs 0000547583 (dalej określany jako „Operator”). Ochrona danych osobowych podmiotów korzystających z wewnętrznego kanału zgłoszeń Operatora (dalej określanych jako „Sygnaliści”) jest realizowana przez Operatora zgodnie z wymogami powszechnie obowiązujących przepisów prawa, a ich przechowywanie ma miejsce na zabezpieczonych serwerach.

2. Operator szanuje prywatność Sygnalistów dokonujących zgłoszeń wewnętrznych za pomocą aplikacji AMLEX (dalej określaną jako „Portal”). Operator oświadcza, że nie zbiera adresów IP komputerów Sygnalistów ani nie używa usługi geolokalizacji.

Operator nie usiłuje identyfikować Sygnalistów. Używany jest m.in. bezpieczny protokół szyfrowania komunikacji (SSL).

3. Dane osobowe podawane w formularzu Portalu są traktowane jako poufne i nie są widoczne dla osób nieuprawnionych.

## **& 2.**

### **ADMINISTRATOR DANYCH OSOBOWYCH**

1. Operator jest administratorem danych osobowych Użytkowników (dalej określanych jako „Dane Osobowe”).

Przetwarzaniu podlegają dane uzupełnione w formularzu zgłaszania takie jak: imię, nazwisko, numer telefonu, adres e-mail, informacje o osobach których dotyczy zgłoszenie.

2. Dane Osobowe są przetwarzane:

- zgodnie z przepisami dotyczącymi ochrony danych osobowych;
- w zakresie i celu niezbędnym do przyjęcia i rozpatrzenia zgłoszenia wewnętrznego Sygnalisty

3. Każda osoba, której dane dotyczą (jeżeli Operator jest ich administratorem) ma prawo dostępu do danych, sprostowania, usunięcia lub ograniczenia przetwarzania, prawo sprzeciwu, prawo wniesienia skargi do organu nadzorczego.

4. Jedyną osobą mającą dostęp do danych przesłanych w zgłoszeniu jest Agata Kuroń.

5. Kontakt z osobą nadzorującą przetwarzanie danych osobowych w organizacji Operatora jest możliwy drogą elektroniczną pod adresem e-mail: [agata.kuron@brliber.pl](mailto:agata.kuron@brliber.pl).

6. Operator zastrzega sobie prawo do przetwarzania Danych Osobowych po rozwiązaniu Umowy lub cofnięciu zgody tylko w zakresie na potrzeby dochodzenia ewentualnych roszczeń przed sądem lub jeżeli przepisy krajowe albo unijne bądź prawa międzynarodowego obligują Operatora do retencji danych.

7. Operator ma prawo udostępniać Dane Osobowe oraz innych jego danych podmiotom upoważnionym na podstawie właściwych przepisów prawa (np. organom ścigania).
8. Usunięcie Danych Osobowych może nastąpić na skutek cofnięcia zgody bądź wniesienia prawnie dopuszczalnego sprzeciwu na przetwarzanie danych osobowych.
9. Operator nie udostępnia Danych Osobowych innym podmiotom aniżeli upoważnionym na podstawie właściwych przepisów prawa, z zastrzeżeniem ust. 13.
10. Operatora wdrożył pseudonimizację, szyfrowanie danych oraz ma wprowadzoną kontrolę dostępu, dzięki czemu minimalizuje skutki ewentualnego naruszenia bezpieczeństwa danych.

### **& 3.**

#### **PLIKI „COOKIES”**

1. Pliki cookies (tzw. ciasteczka) to dane informatyczne, które przechowywane są na urządzeniach Sygnalistów.
2. Operator nie gromadzi plików cookies Sygnalistów, korzystanie z Portalu ma charakter anonimowy i poufny.

### **& 4.**

#### **POSTANOWIENIA KOŃCOWE**

1. Niniejsza Polityka Prywatności obowiązuje od dnia 01.07.2024 roku
2. Operator zastrzega sobie prawo do zmiany Polityki Prywatności w każdym czasie. Jej jednolity tekst będzie dostępny w na stronie głównej Portalu w zakładce „polityka prywatności”.