

English version below

**PROCEDURA ZGŁOSZEŃ WEWNĘTRZNYCH**  
**(procedura dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych)**  
**BP Europa SE Spółka Europejska Oddział w Polsce**  
**z dnia 23 września 2024 roku**

**ROZDZIAŁ PIERWSZY: POSTANOWIENIA OGÓLNE**

**§ 1**

1. Procedura została stworzona w wykonaniu obowiązków wynikających z:
  - a) ustawy z dnia z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. z 2024 r., poz. 928), dalej: „ustawa”;
  - b) aktów normatywnych ustanowionych przez instytucje Unii Europejskiej, wymienione w części II załącznika do dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L. 305 z 26.11.2019, str. 17, z późn. zm.).
2. Procedura wprowadza zasady ujawniania przypadków nieprawidłowości, podejmowania stosownych działań naprawczych w związku z zaistniałymi naruszeniami oraz ochronę Sygnalisty.

**§ 2**

Ileokroć w Procedurze jest mowa o:

1. **„Sygnaliście”** - należy przez to rozumieć osobę fizyczną, która zgłasza lub ujawnia publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, w tym: pracownika; pracownika tymczasowego; osobę świadczącą pracę na innej podstawie niż stosunek pracy, w tym na podstawie umowy cywilnoprawnej; przedsiębiorcę; prokurenta; akcjonariusza lub wspólnika; członka organu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej; osobę świadczącą pracę pod nadzorem i kierownictwem wykonawcy, podwykonawcy lub dostawcy; stażystę; wolontariusza; praktykanta;
2. **„Spółce”** – należy przez to rozumieć spółkę BP Europa SE Spółka Europejska Oddział w Polsce z siedzibą w Krakowie,
3. **„działaniu następczym”** – należy przez to rozumieć działanie podjęte przez Spółkę lub organ publiczny w celu oceny prawdziwości informacji zawartych w zgłoszeniu oraz w celu przeciwdziałania naruszeniu prawa będącemu przedmiotem zgłoszenia, w szczególności przez postępowanie wyjaśniające, wszczęcie kontroli lub postępowania administracyjnego, wniesienie oskarżenia, działanie podjęte w celu odzyskania środków finansowych lub zamknięcie procedury realizowanej w ramach wewnętrznej procedury dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych lub procedury przyjmowania zgłoszeń zewnętrznych i podejmowania działań następczych;

4. **„działaniu odwetowym”** – należy przez to rozumieć bezpośrednie lub pośrednie działanie lub zaniechanie w kontekście związanym z pracą, które jest spowodowane zgłoszeniem lub ujawnieniem publicznym i które narusza lub może naruszyć prawa Sygnalisty lub wyrządza lub może wyrządzić nieuzasadnioną szkodę sygnaliście, w tym bezpodstawne inicjowanie postępowań przeciwko sygnaliście;
5. **„informacji o naruszeniu prawa”** – należy przez to rozumieć informację, w tym uzasadnione podejrzenie dotyczące zaistniałego lub potencjalnego naruszenia prawa, do którego doszło lub prawdopodobnie dojdzie w podmiocie prawnym, w którym Sygnalista uczestniczył w procesie rekrutacji lub innych negocjacji poprzedzających zawarcie umowy, pracuje lub pracował, lub w innym podmiocie prawnym, z którym Sygnalista utrzymuje lub utrzymywał kontakt w kontekście związanym z pracą, lub informację dotyczącą próby ukrycia takiego naruszenia prawa;
6. **„informacji zwrotnej”** – należy przez to rozumieć przekazaną sygnaliście informację na temat planowanych lub podjętych działań następczych i powodów takich działań;
7. **„kontekście związanym z pracą”** – należy przez to rozumieć przeszłe, obecne lub przyszłe działania związane z wykonywaniem pracy na podstawie stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji w Spółce lub na rzecz Spółki, w ramach, których uzyskano informację o naruszeniu prawa oraz istnieje możliwość doświadczenia działań odwetowych;
8. **„organie publicznym”** - należy przez to rozumieć 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 w dziedzinach wskazanych w art. 3 ust. 1 ustawy;
9. **„osobie, której dotyczy zgłoszenie”** – należy przez to rozumieć osobę fizyczną, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, której ustawa przyznaje zdolność prawną, wskazaną w zgłoszeniu lub ujawnieniu publicznym jako osoba, która dopuściła się naruszenia prawa lub jako osoba, z którą osoba, która dopuściła się naruszenia prawa, jest powiązana;
10. **„osobie pomagającej w dokonaniu zgłoszenia”** – należy przez to rozumieć osobę fizyczną, która pomaga sygnaliście w zgłoszeniu lub ujawnieniu publicznym w kontekście związanym z pracą i której pomoc nie powinna zostać ujawniona;
11. **„osobie powiązanej z Sygnalistą”** – należy przez to rozumieć osobę fizyczną, która może doświadczyć działań odwetowych, w tym współpracownika lub osobę najbliższą Sygnalisty w rozumieniu art. 115 § 11 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. z 2024 r. poz. 17);
12. **„Pełnomocniku ds. zgodności”** – należy przez to rozumieć osobę wskazaną przez Spółkę, upoważnioną do przyjmowania zgłoszeń wewnętrznych i realizacji Procedury w Spółce;

13. **„Pracowniku”** – należy przez to rozumieć pracownika w rozumieniu art. 2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy oraz pracownika tymczasowego w rozumieniu art. 2 pkt 2 ustawy z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych (t.j.: Dz.U. z 2023 r. poz. 1110 z późn. zm.);
14. **„ujawnieniu publicznym”** – należy przez to rozumieć podanie informacji o naruszeniu prawa do wiadomości publicznej;
15. **„zgłoszeniu”** – należy przez to rozumieć ustne lub pisemne zgłoszenie wewnętrzne lub zgłoszenie zewnętrzne, przekazane zgodnie z wymogami określonymi w ustawie;
16. **„zgłoszeniu wewnętrznym”** – należy przez to rozumieć ustne lub pisemne przekazanie Spółce informacji o naruszeniu prawa;
17. **„zgłoszeniu zewnętrznym”** – należy przez to rozumieć ustne lub pisemne przekazanie Rzecznikowi Praw Obywatelskich albo organowi publicznemu informacji o naruszeniu prawa.

### **§ 3**

1. Przed dopuszczeniem do pracy każdy Pracownik otrzymuje tekst Procedury, celem zapoznania się z jego treścią. Bezpośredni przełożony Pracownika jest odpowiedzialny za zapoznanie się podwładnego z Procedurą.
2. Dane osobowe Sygnalisty, pozwalające na ustalenie jego tożsamości, nie podlegają ujawnieniu nieupoważnionym osobom, chyba że za wyraźną zgodą Sygnalisty.
3. Przepisu ust. 2 powyżej nie stosuje się w przypadku, gdy 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. Przed dokonaniem takiego ujawnienia, 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.
4. Dane osobowe Sygnalisty, osoby, której dotyczy zgłoszenie, osoby pomagającej w dokonaniu zgłoszenia, osoby powiązanej z Sygnalistą oraz osób wymienionych w treści zgłoszenia podlegają ochronie zgodnie z przepisami o ochronie danych osobowych, w szczególności zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO).
5. Uniemożliwia się dostęp do danych osobowych Sygnalisty, osoby, której dotyczy zgłoszenie, osoby pomagającej w dokonaniu zgłoszenia, osoby powiązanej z Sygnalistą oraz osób wymienionych w treści zgłoszenia podmiotom do tego nieupoważnionym oraz zapewnia ochronę

poufności tożsamości tych osób. Ochrona poufności dotyczy informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość tych osób.

6. Spółka lub podmiot zewnętrzny upoważniony przez Spółkę, po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.

## **ROZDZIAŁ DRUGI: ZGŁOSZENIA WEWNĘTRZNE**

### **§ 4**

1. Osoby, które podejmą informacje o naruszeniu prawa mogą dokonać zgłoszenia wewnętrznego.
2. Naruszeniem prawa jest działanie lub zaniechanie niezgodne z prawem lub mające na celu obejście prawa dotyczące:
  - a) korupcji;
  - b) zamówień publicznych;
  - c) usług, produktów i rynków finansowych;
  - d) zapobiegania praniu pieniędzy i finansowaniu terroryzmu;
  - e) bezpieczeństwa produktów i ich zgodności z wymogami;
  - f) bezpieczeństwa transportu;
  - g) ochrony środowiska;
  - h) ochrony radiologicznej i bezpieczeństwa jądrowego;
  - i) bezpieczeństwa żywności i pasz;
  - j) zdrowia i dobrostanu zwierząt;
  - k) zdrowia publicznego;
  - l) ochrony konsumentów;
  - m) ochrony prywatności i danych osobowych;
  - n) bezpieczeństwa sieci i systemów teleinformatycznych;
  - o) interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, jednostek samorządu terytorialnego oraz Unii Europejskiej;
  - p) rynku wewnętrznego Unii Europejskiej, w tym publicznoprawnych zasad konkurencji i pomocy państwa oraz opodatkowania osób prawnych;
  - q) konstytucyjnych wolności i praw człowieka i obywatela – występujące w stosunkach jednostki z organami władzy publicznej i niezwiązane z dziedzinami wskazanymi w pkt. a-p.
3. Pełnomocnik ds. zgodności jest upoważniony w szczególności do:
  - a) przyjmowania zgłoszeń wewnętrznych,
  - b) podejmowania działań następczych,
  - c) weryfikacji zgłoszeń,

- d) komunikacji z Sygnalistą (w tym występowanie o dodatkowe informacje i przekazywanie Sygnaliście informacji zwrotnej).
4. Spółka zapewnia następujące kanały zgłoszeń wewnętrznych:
- a) w formie e-maila, na adres poczty elektronicznej: **wartoscibpzgloszenia@bp.com**,
  - b) w postaci papierowej - na adres do korespondencji: **BP Europa SE Oddział w Polsce Dział Prawny ul. Pawia 9 (31-154 Kraków)**,
  - c) na wniosek Sygnalisty, za pomocą bezpośredniego spotkania zorganizowanego w terminie 14 dni od dnia otrzymania takiego wniosku,
  - d) za pośrednictwem linii telefonicznej, w dni robocze od poniedziałku do piątku, w godzinach od 08:00 do 16:00, pod numerem telefonu centrali: **+48 12 881 40 00** i połączeniu z Pełnomocnikiem ds. zgodności.
5. Spółka nie przyjmuje zgłoszeń anonimowych. Zgłoszenie anonimowe pozostawia się bez rozpatrzenia, tj. Spółka nie podejmuje żadnych działań w związku z dokonaniem zgłoszenia anonimowego.
6. Pełnomocnik ds. zgodności przesyła Sygnaliście w ciągu 7 dni od otrzymania zgłoszenia, potwierdzenie przyjęcie zgłoszenia (na adres korespondencyjny lub adres poczty elektronicznej wskazany przez Sygnalistę jako adres do kontaktu), chyba że Sygnalista nie podał adresu, na który należy przekazać potwierdzenie.
7. Zgłoszenie powinno zawierać przejrzyste i pełne wyjaśnienie przedmiotu zgłoszenia, w tym co najmniej:
- a) datę oraz miejsce zaistnienia naruszenia prawa lub datę i miejsce pozyskania informacji o naruszeniu prawa;
  - b) opis konkretnej sytuacji lub okoliczności stwarzających możliwość wystąpienia naruszenia prawa;
  - c) wskazanie osoby/osób, których dotyczy zgłoszenie lub danych pozwalających na ich identyfikację
  - d) wskazanie ewentualnej osoby pokrzywdzonej;
  - e) wskazanie ewentualnych świadków naruszenia prawa;
  - f) wskazanie wszystkich dowodów i informacji, jakimi dysponuje Sygnalista, które mogą okazać się pomocne w procesie rozpatrywania zgłoszenia;
  - g) wskazanie preferowanego sposobu kontaktu zwrotnego (adresu do kontaktu).

## **ROZDZIAŁ TRZECI: DOCHODZENIE WEWNĘTRZNE – DZIAŁANIA NASTĘPCZE**

### **§ 5**

1. Spółka podejmuje działania następcze w celu zweryfikowania informacji o naruszeniach prawa.
2. Spółka może zwrócić się do Sygnalisty na adres do kontaktu, o wyjaśnienia lub dodatkowe informacje w zakresie przekazanych informacji, jakie mogą być w jego posiadaniu.

3. Jeżeli Sygnalista sprzeciwia się przesłaniu żądanych wyjaśnień lub dodatkowych informacji lub przesłanie takich informacji może zagrozić ochronie tożsamości Sygnalisty, Spółka odstępuje od takich żądań.
4. Działania następcze nie będą podejmowane, jeżeli w zgłoszeniu dotyczącym sprawy będącej już przedmiotem wcześniejszego zgłoszenia nie zawarto istotnych nowych informacji na temat naruszeń w porównaniu z wcześniejszym zgłoszeniem wewnętrznym. Spółka jednak odnotowuje ten fakt w Rejestrze zgłoszeń wewnętrznych.
5. W przypadku stwierdzenia naruszenia prawa, Spółka odpowiednio:
  - a) dokona stosownych zmian w dokumentach (umowach, regulaminach, procedurach, innych),
  - b) przeprowadzi audyt obszaru będącego przedmiotem zgłoszenia wewnętrznego i działań następczych,
  - c) uwzględni wyniki przeprowadzonego audytu w sposób pozwalający uniknąć naruszeń prawa,
  - d) podejmie inne działania, o ile będą konieczne.
6. Spółka zobowiązana jest przekazać Sygnaliście informację zwrotną w terminie nieprzekraczającym 3 miesięcy od potwierdzenia przyjęcia zgłoszenia lub w przypadku nieprzekazania potwierdzenia sygnaliście, 3 miesięcy od upływu 7 dni od dokonania zgłoszenia.
7. Każde zgłoszenie, za wyjątkiem anonimowego, podlega zarejestrowaniu w Rejestrze zgłoszeń wewnętrznych.
8. Za prowadzenie Rejestru zgłoszeń wewnętrznych odpowiada Pełnomocnik ds. zgodności.
9. Rejestr zgłoszeń wewnętrznych zawiera co najmniej: numer zgłoszenia, przedmiot naruszenia prawa, dane osobowe Sygnalisty oraz osoby, której dotyczy zgłoszenie – niezbędne do identyfikacji tych osób, adres do kontaktu Sygnalisty, datę dokonania zgłoszenia, informację o podjętych działaniach następczych, datę zakończenia sprawy. Rejestr prowadzony jest z zachowaniem zasad poufności, a dane osobowe oraz pozostałe informacje w rejestrze zgłoszeń są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze lub po zakończeniu postępowań zainicjowanych tymi działaniami.

## **ROZDZIAŁ CZWARTY: ZGŁOSZENIA ZEWNĘTRZNE**

### **§ 6**

1. Sygnalista może dokonać zgłoszenia zewnętrznego bez uprzedniego dokonania zgłoszenia wewnętrznego.
2. Zgłoszenie zewnętrzne jest przyjmowane przez Rzecznika Praw Obywatelskich albo organ publiczny, którego właściwość obejmuje podejmowanie odpowiednich działań następczych obejmujących przedmiot zgłoszenia. W stosownych przypadkach zgłoszenia zewnętrzne są dokonywane także do instytucji, organów lub jednostek organizacyjnych Unii Europejskiej.
3. Zgłoszenie dokonane do Rzecznika Praw Obywatelskich lub organu publicznego z pominięciem zgłoszenia wewnętrznego nie skutkuje pozbawieniem Sygnalisty ochrony gwarantowanej przepisami ustawy.

4. Zgłoszenie zewnętrzne może być dokonane do Rzecznika Praw Obywatelskich lub organu publicznego ustnie lub pisemnie.
5. Na żądanie Sygnalisty organ publiczny właściwy do podjęcia działań następczych wydaje nie później niż w terminie miesiąca od dnia otrzymania żądania zaświadczenie, w którym potwierdza, że Sygnalista podlega ochronie określonej ustawie.
6. Rzecznik Praw Obywatelskich oraz organ publiczny gwarantują, że procedura przyjmowania zgłoszeń zewnętrznych i procedura zgłoszeń zewnętrznych oraz związane z przyjmowaniem zgłoszeń przetwarzanie danych osobowych:
  - a) uniemożliwiają uzyskanie dostępu do informacji objętych zgłoszeniem nieupoważnionym osobom;
  - b) zapewniają ochronę poufności tożsamości Sygnalisty oraz osoby, której dotyczy zgłoszenie. Ochrona poufności, dotyczy informacji, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość Sygnalisty oraz osoby, której dotyczy zgłoszenie.
7. Organ publiczny umieszcza na swojej stronie w Biuletynie Informacji Publicznej w oddzielnej, łatwo identyfikowalnej i dostępnej sekcji oraz w sposób zrozumiały dla Sygnalisty w szczególności informacje o:
  - a) danych kontaktowych umożliwiających dokonanie zgłoszenia zewnętrznego, w szczególności adres do korespondencji, adres poczty elektronicznej, adres do doręczeń elektronicznych, odrębny adres elektronicznej skrzynki podawczej, adres strony internetowej, na której znajduje się formularz elektroniczny w rozumieniu art. 3 pkt 25 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307), lub numer telefonu wraz ze wskazaniem, czy rozmowy są nagrywane;
  - b) warunkach objęcia Sygnalisty ochroną;
  - c) trybie postępowania mającym zastosowanie w przypadku zgłoszenia zewnętrznego, w tym o wymaganym sposobie wyjaśnienia informacji będących przedmiotem zgłoszenia lub przedstawienia dodatkowych informacji;
  - d) terminie przekazania informacji zwrotnej oraz rodzaju i zawartości takiej informacji;
  - e) zasadach poufności mających zastosowanie do zgłoszeń zewnętrznych;
  - f) zasadach przetwarzania danych osobowych,
  - g) charakterze działań następczych podejmowanych w związku ze zgłoszeniem zewnętrznym;
  - h) środkach ochrony prawnej i procedurach służących ochronie przed działaniami odwetowymi oraz dostępności poufnej porady dla osób rozważających dokonanie zgłoszenia zewnętrznego;
  - i) warunkach, na jakich Sygnalista jest chroniony przed ponoszeniem odpowiedzialności za naruszenie poufności;
  - j) zachęcie do korzystania z procedury zgłoszeń wewnętrznych podmiotu prawnego w przypadku, gdy naruszeniu prawa można skutecznie zaradzić w ramach struktury organizacyjnej podmiotu prawnego, a Sygnalista uważa, że nie zachodzi ryzyko działań odwetowych;

- k) danych kontaktowych Rzecznika Praw Obywatelskich.
8. Rzecznik Praw Obywatelskich umieszcza na swojej stronie w Biuletynie Informacji Publicznej w oddzielnej, łatwo identyfikowalnej i dostępnej sekcji oraz w sposób zrozumiały dla Sygnalisty w szczególności informacje, o których mowa w ust. 8 pkt a) – c), e) i f) oraz h) – j).

## **ROZDZIAŁ PIĄTY: UJAWNIENIE PUBLICZNE**

### **§ 7**

1. Sygnalista dokonujący ujawnienia publicznego podlega ochronie, jeżeli dokona:
  - a) zgłoszenia wewnętrznego, a następnie zgłoszenia zewnętrznego, a podmiot prawny, a następnie organ publiczny w terminie na przekazanie informacji zwrotnej ustalonym w procedurze wewnętrznej, a następnie w terminie na przekazanie informacji zwrotnej ustalonym w procedurze zewnętrznej organu publicznego nie podejmą żadnych odpowiednich działań następczych ani nie prześlą Sygnaliście informacji zwrotnej lub
  - b) od razu zgłoszenia zewnętrznego, a organ publiczny w terminie na przekazanie informacji zwrotnej ustalonym w swojej procedurze zewnętrznej nie podejmie żadnych odpowiednich działań następczych ani nie prześle Sygnaliście informacji zwrotnej- chyba że Sygnalista nie podał adresu do kontaktu, na który należy przekazać taką informację.
2. Sygnalista dokonujący ujawnienia publicznego podlega ochronie także w przypadku, gdy ma uzasadnione podstawy sądzić, że:
  - a) naruszenie może stanowić bezpośrednie lub oczywiste zagrożenie interesu publicznego, w szczególności, gdy istnieje ryzyko nieodwracalnej szkody, lub
  - b) dokonanie zgłoszenia zewnętrznego narazi Sygnalistę na działania odwetowe, lub
  - c) w przypadku dokonania zgłoszenia zewnętrznego istnieje niewielkie prawdopodobieństwo skutecznego przeciwdziałania naruszeniu prawa z uwagi na szczególne okoliczności sprawy, takie jak możliwość ukrycia lub zniszczenia dowodów, istnienia zмовы między organem publicznym a sprawcą naruszenia lub udziału organu publicznego w naruszeniu.
3. Przy ocenie, czy działanie następcze jest odpowiednie, uwzględnia się w szczególności czynności podjęte w celu zweryfikowania informacji o naruszeniu, prawidłowość oceny informacji o naruszeniu oraz adekwatność środków podjętych w następstwie stwierdzenia naruszenia, w tym - w odpowiednim przypadku - w celu zapobiegnięcia dalszym naruszeniom, z uwzględnieniem wagi naruszenia.

## **ROZDZIAŁ SZÓSTY: OCHRONA SYGNALISTY**

### **§ 8**

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



2. Jeżeli praca była, jest lub ma być świadczona na podstawie stosunku pracy, wobec Sygnalisty (osoby pomagającej w zgłoszeniu oraz osoby powiązanej z Sygnalistą) nie mogą być podejmowane działania odwetowe, polegające w szczególności na:
  - a) odmowie nawiązania stosunku pracy,
  - b) wypowiedzeniu lub rozwiązaniu bez wypowiedzenia stosunku pracy,
  - c) niezawarciu umowy o pracę na czas określony 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 (osoba pomagająca w zgłoszeniu/osoba powiązana z Sygnalistą) miał uzasadnione oczekiwanie, że zostanie z nim zawarta taka umowa,
  - d) obniżeniu wynagrodzenia za pracę,
  - e) wstrzymaniu awansu albo pominięciu przy awansowaniu,
  - f) pominięciu przy przyznawaniu innych niż wynagrodzenie świadczeń związanych z pracą lub obniżeniu wysokości tych świadczeń,
  - g) przeniesieniu a na niższe stanowisko pracy,
  - h) zawieszeniu w wykonywaniu obowiązków pracowniczych lub służbowych,
  - i) przekazaniu innemu Pracownikowi dotychczasowych obowiązków Sygnalisty,
  - j) niekorzystnej zmianie miejsca wykonywania pracy lub rozkładu czasu pracy,
  - k) negatywnej ocenie wyników pracy lub negatywnej opinii o pracy,
  - l) nałożeniu lub zastosowaniu środka dyscyplinarnego, w tym kary finansowej, lub środka o podobnym charakterze,
  - m) przymusie, zastraszaniu lub wykluczeniu,
  - n) mobbingu,
  - o) dyskryminacji,
  - p) niekorzystnym lub niesprawiedliwym traktowaniu,
  - q) wstrzymaniu udziału lub pominięciu przy typowaniu do udziału w szkoleniach podnoszących kwalifikacje zawodowe,
  - r) nieuzasadnionym skierowaniu na badanie lekarskie, w tym badania psychiatryczne, o ile przepisy odrębne przewidują możliwość skierowania Pracownika na takie badanie,
  - s) działaniu zmierzającym do utrudnienia znalezienia w przyszłości zatrudnienia w danym sektorze lub branży na podstawie nieformalnego lub formalnego porozumienia sektorowego lub branżowego,
  - t) powodowaniu straty finansowej, w tym gospodarczej lub utraty dochodu;
  - u) wyrządzeniu innej szkody niematerialnej, w tym naruszeniu dóbr osobistych, w szczególności dobrego imienia Sygnalisty.
3. Za działania odwetowe z powodu dokonania zgłoszenia lub ujawnienia publicznego uważa się także próbę lub groźbę zastosowania środka określonego w ust. 2.
4. Na Spółce spoczywa ciężar dowodu, że podjęte działanie, o którym mowa w ust. 2 pkt a) - u), nie jest działaniem odwetowym.

5. Jeżeli praca lub usługi były, są lub mają być świadczone na podstawie innego niż stosunek pracy stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji, , ust. 2-4 stosuje się odpowiednio, o ile charakter świadczonej pracy lub usług lub pełnionej funkcji, nie wyklucza zastosowania wobec Sygnalisty takiego działania.
6. Jeżeli praca lub usługi były, są lub mają być świadczone na podstawie innego niż stosunek pracy stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji, , dokonanie zgłoszenia lub ujawnienia publicznego nie może stanowić podstawy działań odwetowych ani próby lub groźby zastosowania działań odwetowych, obejmujących w szczególności:
  - a) 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;
  - b) nałożenie obowiązku lub odmowę przyznania, ograniczenie lub odebranie uprawnienia, w szczególności koncesji, zezwolenia lub ulgi.
7. 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, pod warunkiem że Sygnalista miał uzasadnione podstawy sądzić, że zgłoszenie lub ujawnienie publiczne jest niezbędne do ujawnienia naruszenia prawa zgodnie z ustawą.
8. W przypadku wszczęcia postępowania prawnego dotyczącego odpowiedzialności, o której mowa w ust. 7, Sygnalista może wystąpić o umorzenie takiego postępowania.
9. 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.
10. Ochronie nie podlega Sygnalista, który świadomie dokonuje zgłoszenia wewnętrznego, wiedząc, że do naruszenia nie doszło (zła wiara). Zgłoszenie może być dokonane wyłącznie w dobrej wierze. Zakazuje się świadomego składania nieprawdziwych zgłoszeń. Zgodnie z treścią ustawy, osoba dokonująca zgłoszenia nieprawdziwych informacji podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

## **ROZDZIAŁ SIÓDMY: PRZEPISY KOŃCOWE**

### **§ 9**

1. W sprawach nieuregulowanych niniejszą Procedurą, mają zastosowanie przepisy ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. z 2024 r., poz. 928).
2. Procedura wchodzi w życie po upływie 7 dni od dnia podania jej do wiadomości osób wykonujących pracę, w sposób przyjęty w Spółce.
3. Zmiana treści Procedury wymaga zachowania trybu wprowadzenia niniejszej Procedury.

**INTERNAL NOTIFICATION PROCEDURE**  
**(whistleblowing and follow-up procedure)**  
**BP Europa SE European Company Branch in Poland**  
**from 23/09/2024**

**CHAPTER ONE: GENERAL PROVISIONS**

**§ 1**

1. The procedure has been created in fulfilment of obligations under:
  - a) Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928), hereinafter: 'the Act';
  - b) normative acts established by the institutions of the European Union, as listed in Part II of the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting infringements of Union law (OJ L 305, 26.11.2019, p. 17, as amended).
2. The procedure introduces rules for disclosing cases of irregularities, taking appropriate corrective action in relation to the violations that have occurred and protecting the Whistleblower.

**§ 2**

Whenever the Procedure refers to:

1. **"Whistleblower"** - is to be understood as an individual who reports or publicly discloses information about a violation of the law obtained in a work-related context, including: an employee; a temporary employee; a person providing work on a basis other than an employment relationship, including under a civil law contract; an entrepreneur; a proxy; a shareholder or partner; a member of a body of a legal entity or organisational unit without legal personality; a person providing work under the supervision and direction of a contractor, subcontractor or supplier; an intern; a volunteer; an apprentice;
2. **"Company"** - shall mean the company BP Europa SE Spółka Europejska Oddział w Polsce with its registered office in Krakow ,
3. **"follow-up action"** - is to be understood as an action taken by the Company or a public authority in order to assess the veracity of the information contained in a report and to counteract the infringement of the law that is the subject of the report, in particular through an investigation, the initiation of an audit or administrative proceeding, the filing of a charge, an action taken to recover funds or the closure of a procedure carried out under the internal procedure for reporting infringements of the law and taking follow-up action or the procedure for receiving external reports and taking follow-up action;
4. **"Retaliatory action"** - is to be understood as a direct or indirect act or omission in a work-related context which is caused by a report or public disclosure and which violates or is likely

- to violate the rights of the whistleblower or causes or is likely to cause undue harm to the whistleblower, including the unwarranted initiation of proceedings against the whistleblower;
5. **"information about a breach of law"** - this should be understood to mean information, including a reasonable suspicion of an actual or potential breach of law that has occurred or is likely to occur at a legal entity with which the Signaller has participated in the recruitment process or other pre-contract negotiations, works or has worked, or at another legal entity with which the Signaller has or has had contact in a work-related context, or information concerning an attempt to conceal such a breach of law;
  6. **"feedback"** - means the information provided to the whistleblower on the follow-up actions planned or taken and the reasons for such actions;
  7. **"work-related context"** - shall mean past, present or future work-related activities under an employment or other legal relationship underpinning the provision of work or services or the performance of functions in or for the Company, in the course of which information about a breach of the law has been obtained and the possibility of experiencing retaliation exists;
  8. **"public authority"** - shall be understood as the chief and central government administration bodies, field government administration bodies, bodies of local self-government units, other state bodies and other entities performing public administration tasks by virtue of the law, competent to take follow-up actions in the areas indicated in Article 3(1) of the Act;
  9. **"notified person"** - means a natural person, a legal person or an organisational unit without legal personality, to which the law confers legal capacity, identified in a notification or public disclosure as a person who has committed an infringement of the law or as a person with whom the infringer is associated;
  10. **"whistleblower helper"** - means an individual who assists a whistleblower with a report or public disclosure in a work-related context and whose assistance should not be disclosed;
  11. **"person associated with the Signaller"** - it should be understood to mean a natural person who may experience retaliatory actions, including a co-worker or a person close to the Signaller within the meaning of Article 115 § 11 of the Act of 6 June 1997. - Penal Code (Journal of Laws of 2024, item 17);
  12. **"Compliance Officer"** - means the person designated by the Company and authorised to receive internal calls and implement the Procedure in the Company;
  13. **"Employee"** - shall be understood as an employee within the meaning of Article 2 of the Act of 26 June 1974. - Labour Code and a temporary employee within the meaning of Article 2(2) of the Act of 9 July 2003 on the employment of temporary employees (i.e.: Journal of Laws of 2023, item 1110, as amended);
  14. **"Public disclosure"** - means the making of information about an infringement to the public;
  15. **"notification"** - means an oral or written internal notification or an external notification provided in accordance with the requirements of the Act;
  16. **"internal notification"** - means the oral or written communication to the Company of a breach of the law;

17. **"external notification"** - means the oral or written communication to the Ombudsman or to a public authority of a violation of the law.

### **§ 3**

1. Each Employee shall be provided with the text of the Procedure for familiarisation with its contents before being allowed to work. The Employee's immediate supervisor is responsible for making the subordinate familiar with the Procedure.
2. The Signaller's personal data, which allows the identification of the Signaller, shall not be disclosed to unauthorised persons, except with the Signaller's express consent.
3. Paragraph 2 above shall not apply where disclosure is a necessary and proportionate legal obligation in connection with investigations carried out by public authorities or investigations or prosecutions carried out by courts, including for the purpose of safeguarding the rights of defence of the reported person. Before making such a disclosure, the competent public authority or the competent court shall notify the Whistleblower by sending, in paper or electronic form, an explanation of the reasons for the disclosure of his or her personal data, unless such notification would jeopardise the investigation or pre-trial or judicial proceedings.
4. The personal data of the Whistleblower, the person to whom the notification relates, the person assisting in the notification, the person associated with the Whistleblower and the persons mentioned in the content of the notification shall be protected in accordance with data protection legislation, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - RODO).
5. Access to the personal data of the Whistleblower, the person to whom the report relates, the person assisting in making the report, the person associated with the Whistleblower and the persons mentioned in the content of the report shall be prevented to unauthorised persons and the confidentiality of their identity shall be protected. The confidentiality protection applies to information from which the identity of these persons can be directly or indirectly identified.
6. The Company, or an external entity authorised by the Company, shall, upon receipt of a notification, process personal data to the extent necessary for the acceptance of the notification or any follow-up action. Personal data that are not relevant to the processing of the notification shall not be collected and, if accidentally collected, shall be deleted immediately. The deletion of such personal data shall take place within 14 days of the determination that it is not relevant.

## **CHAPTER TWO: INTERNAL NOTIFICATIONS**

### **§ 4**

1. Persons who take up information about a breach of the law can make an internal report.

2. An infringement is an act or omission that is unlawful or intended to circumvent the law concerning:
  - a) corruption;
  - b) public procurement;
  - c) financial services, products and markets;
  - d) prevention of money laundering and terrorist financing;
  - e) product safety and compliance;
  - f) transport security;
  - g) environmental protection;
  - h) radiological protection and nuclear safety;
  - i) food and feed safety;
  - j) animal health and welfare;
  - k) public health;
  - l) consumer protection;
  - m) privacy and data protection;
  - n) security of ICT networks and systems;
  - o) financial interests of the State Treasury of the Republic of Poland, local government units and the European Union;
  - p) the internal market of the European Union, including public law competition and state aid rules and corporate taxation;
  - q) constitutional freedoms and rights of the human being and the citizen - occurring in the relations of the individual with public authorities and not related to the areas indicated in points a-p.
3. The compliance officer is authorised in particular to:
  - a) acceptance of internal applications,
  - b) follow up,
  - c) verification of applications,
  - d) communication with the Signaller (including requesting additional information and providing feedback to the Signaller).
4. The Company provides the following channels for internal notifications:
  - a) by e-mail to: **wartoscibpzgloszenia@bp.com**,
  - b) in paper form - to the mailing address: **BP Europa SE Branch in Poland Legal Department ul. Pawia 9 (31-154 Kraków)**,
  - c) at the request of the Signaller, by means of a face-to-face meeting organised within 14 days of receipt of such a request,
  - d) via telephone line, on working days from Monday to Friday, between 08:00 and 16:00, at the switchboard telephone number: **+48 12 881 40 00** and connecting to the Compliance Officer.

5. The Company does not accept anonymous submissions. An anonymous report shall be left unprocessed, i.e. the Company shall not take any action in connection with an anonymous report.
6. The Compliance Officer sends the Signaller, within 7 days of receipt of the notification, an acknowledgement of receipt of the notification (to the postal or email address indicated by the Signaller as the contact address), unless the Signaller has not provided an address to which the acknowledgement should be forwarded.
7. The notification should contain a clear and complete explanation of the subject matter of the notification, including at least:
  - a) the date and place of the infringement or the date and place where the information about the infringement was obtained;
  - b) a description of the specific situation or circumstances giving rise to the possibility of an infringement;
  - c) identification of the person(s) concerned by the notification or data allowing for their identification
  - d) the identification of a possible victim;
  - e) identification of possible witnesses to the infringement;
  - f) identify all evidence and information available to the Signaller that may be helpful in the process of dealing with the application;
  - g) indication of the preferred method of contact back (contact address).

### **CHAPTER THREE: INTERNAL INVESTIGATION - FOLLOW-UP**

#### **§ 5**

1. The Company follows up to verify information on violations.
2. The Company may ask the Signaller at the contact address, for clarification or additional information on the information provided, as may be in its possession.
3. If the Signaller objects to sending the requested clarifications or additional information or the sending of such information may jeopardise the protection of the Signaller's identity, the Company shall waive such requests.
4. Follow-up action will not be taken if a report concerning a matter already the subject of an earlier report does not contain significant new information on violations compared to the earlier internal report. However, the Company will note this fact in the Register of Internal Notifications.
5. If a breach is found, the Company shall accordingly:
  - a) make appropriate amendments to documents (contracts, regulations, procedures, others),
  - b) carry out an audit of the area subject to the internal notification and follow-up,
  - c) take into account the results of the audit carried out in such a way as to avoid infringements of the law,
  - d) take other action if necessary.

6. The Company is obliged to provide feedback to the Signaller within a period not exceeding 3 months from the acknowledgement of the notification or, if no acknowledgement is provided to the Signaller, 3 months from the expiry of 7 days from the notification.
7. Every report, with the exception of anonymous reports, is subject to registration in the Register of Internal Reports.
8. The Compliance Officer is responsible for maintaining the Register of Internal Notifications.
9. The register of internal notifications contains at least: the notification number, the subject of the infringement, the personal data of the Signaller and the person to whom the notification refers - necessary to identify those persons, the Signaller's contact address, the date on which the notification was made, information on the follow-up actions taken, the date on which the case was closed. The register is kept confidential and the personal data and other information in the register of notifications are kept for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or the proceedings initiated by those actions were terminated.

#### **CHAPTER FOUR: EXTERNAL NOTIFICATIONS**

##### **§ 6**

1. A whistleblower may make an external filing without first making an internal filing.
2. An external notification shall be received either by the Ombudsman or by a public authority whose competence includes appropriate follow-up action on the subject of the notification. Where appropriate, external notifications shall also be made to European Union institutions, bodies, offices or agencies.
3. A notification made to the Ombudsman or a public body bypassing an internal notification does not have the effect of depriving the Signaller of the protection guaranteed by the Act.
4. An external notification may be made to the Ombudsman or a public body orally or in writing.
5. At the request of the Signaller, the public authority competent to take follow-up action shall issue, no later than one month from the date of receipt of the request, a certificate confirming that the Signaller is subject to the protection set out in the Act.
6. The Ombudsman and the public authority shall ensure that the procedure for the acceptance of external reports and the procedure for external reports and the processing of personal data related to the acceptance of reports:
  - a) prevent access to the reported information by unauthorised persons;
  - b) ensure that the confidentiality of the identity of the Whistleblower and of the person concerned is protected.The protection of confidentiality, applies to information from which the identity of the Whistleblower and the reported person can be directly or indirectly identified.
7. The public authority shall post on its website in the Public Information Bulletin in a separate, easily identifiable and accessible section and in a manner understandable to the Signaller, in particular, information on:



- a) contact data enabling the filing of an external notification, in particular the correspondence address, e-mail address, address for electronic delivery, separate address for electronic mailbox, address of the website where the electronic form is located, within the meaning of Article 3(25) of the Act of 17 February 2005 on Informatisation of the Activity of Entities Performing Public Tasks (Journal of Laws of 2024, item 307), or telephone number, along with an indication whether the calls are recorded;
  - b) the terms of the Signaller's coverage;
  - c) the procedure to be followed in the case of an external notification, including the required means for clarifying the information which is the subject of the notification or for providing additional information;
  - d) the timing of the feedback and the type and content of such feedback;
  - e) confidentiality rules applicable to external notifications;
  - f) principles for processing personal data,
  - g) nature of the follow-up to the external notification;
  - h) legal remedies and procedures to protect against retaliation and the availability of confidential advice for those considering making an external report;
  - i) conditions under which the Signaller is protected from incurring liability for breach of confidentiality;
  - j) to encourage the use of the legal entity's internal notification procedure in cases where the violation of the law can be effectively remedied within the organisational structure of the legal entity and the Whistleblower considers that there is no risk of retaliation;
  - k) contact details of the Ombudsman.
8. The Ombudsman shall post on his website in the Public Information Bulletin in a separate, easily identifiable and accessible section and in a way that is comprehensible to the signatory, in particular the information referred to in points (a) to (c), (e) and (f) and (h) to (j) of paragraph 8.

## **CHAPTER FIVE: PUBLIC DISCLOSURE**

### **§ 7**

1. A whistleblower making a public disclosure is protected if he or she makes:
- a) an internal notification and then an external notification, and the legal entity and then the public authority fail to take any appropriate follow-up action or provide feedback to the Signatory within the timeframe for feedback set by the internal procedure and then the timeframe for feedback set by the public authority's external procedure; or
  - b) immediately of the external notification, and the public authority does not take any appropriate follow-up action or provide feedback to the Signatory within the deadline for feedback set in its external procedure
- unless the Signaller has not provided a contact address to which such information should be forwarded.

2. A whistleblower making a public disclosure is also protected if he or she has reasonable grounds to believe that:
  - a) the breach is likely to constitute a direct or obvious threat to the public interest, in particular where there is a risk of irreparable harm, or
  - b) making an external report will expose the Signaller to reprisals, or
  - c) where an external notification is made, there is little likelihood of successfully addressing the infringement due to the particular circumstances of the case, such as the possibility of concealing or destroying evidence, the existence of collusion between the public authority and the infringer, or the involvement of the public authority in the infringement.
3. In assessing the appropriateness of the follow-up action, account shall be taken, in particular, of the steps taken to verify the information concerning the breach, the correctness of the assessment of the information concerning the breach and the adequacy of the measures taken following the discovery of the breach, including, where appropriate, to prevent further breaches, having regard to the gravity of the breach.

## **CHAPTER SIX: PROTECTION OF THE WHISTLEBLOWER**

### **§ 8**

1. No retaliatory action or attempt or threat of such action may be taken against the Signaller.
2. If the work was, is or is to be provided on the basis of an employment relationship, no retaliatory action may be taken against the Signaller (the person assisting in the reporting and the person associated with the Signaller) , consisting in particular of:
  - a) refusal to establish an employment relationship,
  - b) termination or termination without notice of the employment relationship,
  - c) failure to conclude a fixed-term employment contract after the termination of the probationary contract, failure to conclude another fixed-term employment contract or failure to conclude an indefinite-term employment contract after the termination of the fixed-term contract - where the Signaller (the person assisting in the notification/person associated with the Signaller) had a legitimate expectation that such a contract would be concluded with him/her,
  - d) reduction in remuneration for work,
  - e) withholding of promotion or omission from promotion,
  - f) omission in the award of work-related benefits other than wages or reduction in the amount of such benefits,
  - g) transfer a to a lower post,
  - h) suspension from employment or official duties,
  - i) transferring to another Employee the existing duties of the Signaller,
  - j) an unfavourable change in the place of work or working time schedule,
  - k) negative performance appraisal or negative job review,

- l) the imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature,
  - m) coercion, intimidation or exclusion,
  - n) bullying,
  - o) discrimination,
  - p) unfavourable or unjust treatment,
  - q) withholding participation or being overlooked for selection for professional qualification training,
  - r) unjustified referral for medical examination, including psychiatric examination, insofar as separate regulations provide for the possibility of referring an Employee for such examination,
  - s) action to make it more difficult to find future employment in a particular sector or industry on the basis of an informal or formal sectoral or industry agreement,
  - t) causing financial, including economic, loss or loss of income;
  - u) the infliction of other non-material damage, including damage to personal rights, in particular to the Signaller's good name.
3. Retaliation for making a report or making a public disclosure shall also be deemed to be an attempt or threat to take the measure set out in paragraph 2.
  4. The Company shall bear the burden of proof that the action taken, as referred to in paragraph 2(a) to (u), is not a retaliatory action.
  5. Where work or services have been, are being or are intended to be provided on the basis of a legal relationship other than an employment relationship forming the basis for the provision of work or services or the performance of a function, , paragraphs 2 to 4 shall apply mutatis mutandis, insofar as the nature of the work or services provided or the performance of a function does not preclude the application of such action to the Signatory.
  6. Where work or services have been, are being or are intended to be provided on the basis of a legal relationship other than an employment relationship giving rise to the provision of work or services or the performance of functions, , the making of a report or public disclosure may not give rise to retaliation or an attempt or threat of retaliation, including, in particular:
    - a) the termination of a contract to which the Signatory is a party, in particular concerning the sale or supply of goods or the provision of services, the withdrawal from such a contract or its termination without notice;
    - b) the imposition of an obligation or the refusal to grant, limit or withdraw an entitlement, in particular a concession, permit or relief.
  7. The making of a report or public disclosure may not give rise to liability, including disciplinary liability or liability for damages for infringement of the rights of others or obligations set out in the law, in particular on the subject of defamation, infringement of personal rights, copyright, protection of personal data and the obligation to maintain secrecy, including business secrets, having regard to Article 5 of the Act, provided that the Signaller had reasonable grounds to believe that the report or public disclosure was necessary to disclose a breach of the law in accordance with the Act.

8. In the event that legal proceedings are instituted in respect of the liability referred to in paragraph 7, the Signaller may request that such proceedings be discontinued.
9. Obtaining or accessing information which is the subject of a report or public disclosure may not give rise to liability, provided that such obtaining or such access does not constitute a prohibited act.
10. Protection is not granted to a whistleblower who knowingly makes an internal notification knowing that an infringement has not occurred (bad faith). A notification may only be made in good faith. Knowingly making a false notification is prohibited. According to the law, a person who makes a false report is liable to a fine, restriction of liberty or imprisonment for up to two years.

## **CHAPTER SEVEN: FINAL PROVISIONS**

### **§ 9**

1. In matters not regulated by this Procedure, the provisions of the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928) shall apply.
2. The procedure comes into force 7 days after it is made known to those performing the work, in the manner adopted by the Company.
3. An amendment to the content of the Procedure shall follow the procedure for the introduction of this Procedure.