PNP KLOKKENLUIDERSBELEID

LEGAL

België heeft de EU-richtlijn 2019/1973 van het Europees Parlement en de Raad van 23/10/2019 omgezet in de wet van 28 november 2022 betreffende de bescherming van personen die schendingen van het recht van de Unie of het nationale recht binnen een privaatrechtelijke rechtspersoon melden. Deze wet treedt in werking op 15/02/2023.

Deze wet beoogt de meldingskanalen in te stellen om klokkenluiders (whistleblower) die getuige zijn van feitelijke of potentiële schendingen op bepaalde gebieden in staat te stellen deze aan te geven en stelt een verbod in op elke vorm van vergelding tegen hen.

In het kader daarvan stelt PNP deze procedure ter beschikking van de personen onderworpen aan het toepassingsgebied van de wet, om een melding te doen. PNP wil op deze manier garanderen dat de regelgeving en de interne regels worden nageleefd.

De bepalingen van de wet zijn van openbare orde en vullen de reeds bestaande en van toepassing zijnde wettelijke en reglementaire bepalingen aan.

De integrale versie van de wet kan geraadpleegd worden via
https://www.ejustice.just.fgov.be/eli/wet/2022/11/28/2022042980/staatsblad

OPGELET

Het interne meldingskanaal mag niet verward worden met de klachtenprocedure.

Om een klacht (ontevredenheid over de verzekeringsovereenkomst of de door u ontvangen dienst) te melden, verwijzen wij u naar de rubriek "Klachtenmanagement" van de website die u oorspronkelijk bezocht heeft.

1. Scope van de klokkenluidersprocedure

1.1. Materieel toepassingsgebied

De meldingen kunnen betrekking hebben op :

a) inbreuken betreffende de overtredingen in de volgende domeinen :
   1. Overheidsopdrachten
   2. financiële diensten, producten en markten en het voorkomen van het witwassen van geld en terrorismefinanciering
   3. productveiligheid en productconformiteit
   4. vervoersveiligheid
   5. milieubescherming
   6. stralingsbescherming en nucleaire veiligheid
   7. voedsel- en voederveiligheid, gezondheid en welzijn van dieren
   8. volksgezondheid
   9. consumentenbescherming
   10. bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen
   11. bestrijding van belastingfraude
   12. bestrijding van sociale fraude

b) schendingen waarbij de financiële belangen van de Unie worden geschaad.

c) schendingen betreffende de interne markt.

Een inbreuk wordt gedefinieerd als het handelen of niet-handelen dat

- onrechtmatig is en
- betrekking heeft op de domeinen van het materieel toepassingsgebied en
- in strijd is met het doel of de toepassing van de regels voorzien in de betrokken beleidsterreinen.

De wet is niet van toepassing op onder meer :

- Informatie gedekt door het medisch beroepsgeheim;
- Informatie gedekt door het beroepsgeheim van advocaten.

1.2. Personeel toepassingsgebied

De wet is van toepassing op :

- Melders van inbreuken die in de private sector werken en die informatie over schendingen in een professionele context hebben verkregen, waaronder ten minste:
  - Personen met het statuut van werknemer of van zelfstandige;
  - Aandeelhouders en leden van het bestuurs-, leidinggevend of toezichthoudend orgaan van een onderneming, met inbegrip van niet-uitvoerende leden;
  - Vrijwilligers en bezoldigde of onbezoldigde stagiairs;
  - Eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers.

- Melders wiens arbeidsverhouding inmiddels werd beëindigd sinds de melding of openbaarmaking.

- Melders wiens arbeidsverhouding nog niet is begonnen (sollicitanten) en voor zover de informatie over de schending werd verkregen tijdens het aanwervingsproces of andere precontractuele onderhandelingen.

- Alsook op :
  - Facilitators (een persoon die de melder bijstaat in het meldingsproces en wiens bijstand vertrouwelijk moet zijn);
  - Derden die verbonden zijn met de melders en die het risico lopen op represailles in een professionele context (zoals collega's of familieleden van de melder);
  - Juridische entiteiten die eigendom zijn van, of in een werk gerelateerde context verbonden zijn met de melders.

  Indien de bescherming wordt genoten door een facilitator, een derde of een juridische entiteit, moeten ze redelijke gronden hebben om aan te nemen dat de klokkenluider binnen de bescherming van de wet valt.

- Melders die buiten een professionele context verkregen informatie doorgeven, voor zover het een schending op het gebied van financiële diensten, producten en markten of een schending op het gebied van het voorkomen van het witwassen van geld en de financiering van terrorisme betreft.

- Elke organisatie, met of zonder rechtspersoonlijkheid, die valt onder de bevoegdheid van de deelstaten voor zover een kwestie niet door de wetgeving van de gewesten en gemeenschappen wordt geregeld en onder de bevoegdheid van de federale Staat valt, onder voorbehoud van de toepassing van gunstiger beschermingsmaatregelen voor de melder.

2. Beschermingsmaatregelen en sancties

2.1. Verbod op represailles

De klokkenluider wordt beschermd tegen elke vorm van represailles of bedreiging.

Om in aanmerking te komen voor het bij de wet ingestelde beschermingsmechanisme, moet de melder :

- ter goede trouw zijn en dus gegronde redenen hebben gehad om aan te nemen dat de gemelde informatie m.b.t. de inbreuken, op het moment van de melding juist was;
- dat de informatie binnen het toepassingsgebied van de wet viel en
- een interne of externe melding, dan wel een openbaarmaking hebben gedaan, overeenkomstig de wet.

De eerste twee criteria worden beoordeeld ten overstaan van een persoon die zich in een vergelijkbare situatie bevindt en over een vergelijkbare kennis beschikt.

De melder verliest het voordeel van de bescherming niet op de enkele grond dat de te goeder trouw gedane melding onjuist of ongegrond is bevonden.

Elke beschermde persoon die meent slachtoffer te zijn van of bedreigd te worden met een represaille, kan een met redenen omklede klacht indienen bij de federale coördinator, die een buitengerechtelijke beschermingsprocedure opstart.

2.2. Sancties

De wetgeving voorziet in aanzienlijke sancties ten aanzien van de juridische entiteit in geval van represailles.

De wetgever heeft eveneens voorzien in sancties ten aanzien van de melder wanneer wordt vastgesteld dat hij/zij bewust valse informatie heeft gemeld of openbaar gemaakt heeft.

3. Ondersteuningsmaatregelen

De melder heeft toegang tot het Federaal Instituut voor de bescherming en bevordering van de Rechten van de Mens (FIRM) wat betreft de wettelijk voorziene ondersteuningsmaatregelen.

Dit instituut is het gekwalificeerd en centrale informatiepunt inzake de bescherming van klokkenluiders en is verantwoordelijk voor hun ondersteuning.

4. Meldingskanalen

4.1. Interne meldingskanalen

4.1.1. Algemeen

Zoals wettelijk voorgeschreven, heeft PNP, kanalen en procedures voor interne melding en opvolging opgezet.

De interne kanalen en procedures zijn toegankelijk voor degenen die onder het toepassingsgebied van de wet vallen en een melding willen doen.

Het intern beheer van het intern meldingskanaal werd toevertrouwd aan Lieven De Cock, die de functie van meldingsbeheerder (Whistleblowing officer) heeft.

Lieven De Cock heeft een volledige onafhankelijkheid voor de afhandeling van de concrete meldingen/dossiers en heeft geen enkele mogelijkheid tot belangenconflicten. Bij (potentiële) risico's of belemmeringen voor de uitvoering van zijn taken heeft hij het recht dit rechtstreeks aan het hoogste directieniveau te rapporteren.

4.1.2. De procedure voor de interne melding – het intern meldingskanaal

1) Het is mogelijk om zowel schriftelijk als mondeling een inbreuk te melden:

schriftelijk:
- via e-mail : klokkenluider@pnp.be
- per post : PNP t.a.v. de Meldingbeheerder – Casinoplein 6 – 8500 Kortrijk met vermelding "Strikt vertrouwelijk"

Hiervoor beschikt de melder over de mogelijkheid om gebruik te maken van het "Aangifteformulier Whistleblowing" dat beschikbaar is als bijlage aan deze beleidsnota.

mondeling :

- per telefoon op het nummer 056/26.61.25
- het is eveneens mogelijk om een inbreuk te melden door middel van een fysieke ontmoeting, na afspraak met de PNP Meldingsbeheerder. Deze ontmoeting dient binnen een redelijke termijn plaats te vinden

2) binnen de 7 dagen na de melding wordt aan de melder een ontvangstmelding verzonden;
3) de meldingsbeheerder zorgt voor een zorgvuldige opvolging van de melding;
4) binnen maximaal een termijn van 3 maanden na de ontvangstmelding wordt aan de melder een feedback gegeven over de voorgenomen maatregelen als opvolging en de redenen van deze opvolging;
5) duidelijke en gemakkelijk toegankelijke informatie over de externe meldingsprocedures zal worden medegedeeld aan de melder.

4.1.3. Geheimhouding en veiligheidsmaatregelen

PNP garandeert een strikte geheimhouding van de identiteit van de melder.

Dit houdt in dat de identiteit van de melder in geen geval zonder diens vrije en uitdrukkelijke toestemming mag worden bekendgemaakt aan andere personen dan de meldingsbeheerders. Dit geldt ook voor alle andere informatie waaruit de identiteit van de melder direct of indirect kan worden afgeleid.

De interne kanalen zijn zoveel als mogelijk beveiligd om de vertrouwelijkheid van de identiteit van de melder en de in de melding genoemde derden te waarborgen, alsook de toegang door onbevoegde personeelsleden te verhinderen.

4.1.4. Verwerking van persoonsgegevens

Elke verwerking van persoonsgegevens wordt uitgevoerd in overeenstemming met de Europese Verordening 2016/679 "AVG" (GDPR) en de wettelijke bepalingen inzake de bescherming van personen met betrekking tot de verwerking van hun persoonsgegevens.

Persoonsgegevens die duidelijk niet relevant zijn voor de verwerking van een specifieke melding moeten (overeenkomstig het beginsel van minimale gegevensverwerking) niet verzameld worden, of indien onbedoeld verzameld, onmiddellijk gewist worden.

De naam, de functie en de contactgegevens van de melder, alsmede van eenieder tot wie de beschermings- en ondersteuningsmaatregelen zich uitstrekken, worden beveiligd totdat het gemelde strafbare feit verjaard is.

4.1.5. Registratie van de meldingen

Alle ontvangen meldingen worden geregistreerd op een veilige en confidentiële wijze. Daartoe wordt door de meldingsbeheerder een specifiek register bijgehouden met alle ontvangen meldingen.

4.2. Externe meldingskanalen

De melders kunnen eveneens gebruik maken van een extern meldingskanaal, hetzij nadat zij een melding via de interne kanalen hebben gedaan, hetzij door rechtstreeks een beroep te doen op externe meldingskanalen, als zij deze geschikter achten.

De Federale Ombudsman werd door de Belgische wetgever belast met de taak om de meldingen via externe meldingskanalen te coördineren. Hij vervult dus de rol van federale coördinator.

De door de wetgever aangewezen bevoegde autoriteiten, zoals de FSMA, de NBB, de GBA of, bij ontstentenis daarvan, de Federale Ombudsman, zijn derhalve belast met het ontvangen van externe meldingen voor de financiële sector.

BIJLAGE :DOCUMENT INTERNE MELDING KLOKKENLUIDER/WHISTLEBLOWER

VERTROUWELIJK
INTERNE MELDING KLOKKENLUIDER/WHISTLEBLOWER

Naam en voornaam van de melder:
Contactgegevens (emailadres, telefoonnummer, …):

Datum van de 1ste vaststelling van de inbreuk:

Inbreuk(en) op de volgende domeinen van de wet:

- ☐ Overheidsopdrachten
- ☐ Financiële diensten, producten en markten, voorkoming van witwassen van geld en terrorismefinanciering
- ☐ Productveiligheid en productconformiteit
- ☐ Veiligheid van het vervoer
- ☐ Bescherming van het milieu
- ☐ Stralingsbescherming en nucleaire veiligheid
- ☐ Veiligheid van levensmiddelen en diervoeders, dierengezondheid en dierenwelzijn
- ☐ Volksgezondheid
- ☐ Consumentenbescherming
- ☐ Bescherming van de persoonlijke levenssfeer en persoonsgegevens en beveiliging van netwerk- en informatiesystemen
- ☐ Bestrijding van belastingfraude
- ☐ Sociale fraudebestrijding
- ☐ Schending van de financiële belangen van de EU
- ☐ Schending betreffende de Interne markt van de EU, met inbegrip van de Unieregels inzake mededinging en staatsteun

Hoedanigheid melder :

Omstandige omschrijving van de inbreuk(en) :

Aantal bijlagen :
Datum van de melding :
Handtekening

Als verwerkingsverantwoordelijke stellen we alles in het werk om uw persoonsgegevens op een veilige en integere manier te verwerken en dit conform de geldende regelgeving inzake de persoonlijke levenssfeer en in het bijzonder de AVG, Algemene Verordening Gegevensverwerking (Verordening EU nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens). Alle details over ons privacybeleid vindt u terug op onze website www.pnp.be.