Beleid omtrent het melden van inbreuken

1 Doel

Groep PSA bestaande uit de volgende entiteiten:

- PSA Antwerp – Napelsstraat 79, 2000 Antwerpen – 0442.652.075
- PSA Finance Europe – Napelsstraat 79, 2000 Antwerpen - 0882.346.048
- MPET – Napelsstraat 79, 2000 Antwerpen - 0552.527.539
- ATS – Napelsstraat 79, 2000 Antwerpen - 0506.666.137
- PSA Breakbulk – Napelsstraat 79, 2000 Antwerpen - 0689.746.214
- PSA Zeebrugge – Caxtonweg Q140-143, 8380 Zeebrugge - 0808.254.478
- PSA Baltics – Napelsstraat 79, 2000 Antwerpen – 0715.850.397
- PSA Supply Chain Solutions – Napelsstraat 79, 2000 Antwerpen – 0776.990.091
- PSA Investments – Napelsstraat 79, 2000 Antwerpen – 0671.672.441
- PSA Genoa Investments – Napelsstraat 79, 2000 Antwerpen – 0751.776.823

hierna genaamd "de Ondernemingen" willen in hun activiteiten integer en ethisch handelen en willen er daarom voor zorgen dat hun medewerkers de mogelijkheid hebben, conform de hierna vastgestelde modaliteiten en voorwaarden, om in de Ondernemingen vastgestelde of vermoede inbreuken op de in punt 2.2 van dit beleid bedoelde wettelijke en regelgevende normen, op de meest serene en vertrouwelijke manier te kunnen melden.

Het zijn vaak de eigen medewerkers die als eerste op de hoogte zijn van bedreigingen of inbreuken die zich binnen een onderneming voordoen. Zij zouden echter tegengehouden kunnen worden om hun bezorgdheid of vermoedens te uiten uit angst voor reacties of represailles.

Deze mogelijke vrees zou er uiteindelijk toe kunnen leiden dat de Ondernemingen in het ongewisse blijven over mogelijke inbreuken en niet de nodige stappen kunnen ondernemen om deze inbreuken aan te pakken. Dit zou dan ook de belangen van de Ondernemingen, die hoogstaande normen van goed bestuur en beroepsethiek nastreven, kunnen inperken.

Het doel van dit beleid is om deze situatie te voorkomen door alle werknemers en andere personen die een contractuele relatie met de Ondernemingen hebben, sterk aan te moedigen om elke inbreuk, illegale, onethische of frauduleuze activiteit met betrekking tot de activiteiten van de Ondernemingen te melden zonder angst voor sancties of andere maatregelen.

Dit beleid is vastgesteld overeenkomstig de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of het nationale recht vastgesteld binnen een juridische entiteit in de privésector, waarmee de Europese richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het unierecht melden, wordt omgezet, hierna vermeld als “de Wet”.

Dit beleid heeft tot doel:

- de vertrouwelijke, al dan niet anonieme melding van informatie over mogelijke of daadwerkelijke inbreuken mogelijk te maken;
- een bescherming te bieden aan personen die een inbreuk melden of de melder bijstaan;
- de procedure vast te leggen die de melder van een inbreuk daartoe moet volgen.

Dit beleid is beschikbaar op het intranet van de Ondernemingen (Be Connect), en kan van tijd tot tijd gewijzigd worden. Dit beleid is een aanvulling op de 'Code of Conduct' en specifiek in uitwerking van de Belgische wetgeving omtrent klokkenluiders (zie hierboven).

Dit beleid sluit uiteraard op geen enkele wijze de directe dialoog en communicatie van informatie, buiten de meldingsprocedure om, uit. De Ondernemingen willen benadrukken dat werknemers met bezorgdheden of vermoedens zich ten allen tijde kunnen richten tot hun direct leidinggevenden, HR of de Compliance afdeling (Legal).

2 Toepassingsgebied

2.1 Wie valt onder dit beleid?

Dit beleid is van toepassing op de volgende personen:

- huidige en vroegere werknemers, die verbonden zijn of waren in het kader van een arbeidsovereenkomst met de Ondernemingen;
- kandidaten die betrokken zijn of waren in een rekruteringsprocedure in de Ondernemingen;
- personen die op zelfstandige basis samenwerken of hebben samengewerkt met de Ondernemingen en de kandidaten voor een zelfstandige samenwerking in het kader van precontractuele onderhandelingen;
- vrijwilligers en stagiairs (bezoldigd of onbezoldigd);
- aandeelhouders en leden van het bestuurs-, leidinggevend of toezichthoudend orgaan van de Ondernemingen (met inbegrip van niet-uitvoerende leden);
- elke persoon die werkt of gewerkt heeft onder toezicht en leiding van aannemers, onderaannemers en/of leveranciers van de Ondernemingen;
- eenieder die informatie heeft over inbreuken in de Ondernemingen op het gebied van financiële diensten, producten en markten zelfs buiten een werkgerelateerde context.

2.2 Welke inbreuken kunnen gemeld worden?

Er kunnen slechts inbreuken gemeld worden die betrekking hebben op één van de hierna vermelde gebieden zoals omschreven in 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, diergezondheid en dierenwelzijn;
- Volksgezondheid;
- Consumentenbescherming;
- Bescherming van de persoonlijke levenssfeer en persoonsgegevens, en beveiliging van netwerk- en informatiesystemen;
- Bestrijding van belastingfraude;
- Sociale fraudebestrijding.

Bovendien kunnen inbreuken gemeld worden waardoor de financiële belangen van de Europese Unie kunnen geschaad worden alsook inbreuken in verband met de Europese interne markt met inbegrip van de Unieregels inzake mededinging en staatssteun.

Onder inbreuk wordt verstaan de handeling of nalatigheid die onrechtmatig is of ingaat tegen het doel of de toepassing van de regels in de bovenvermelde gebieden. Het betreft elke inbreuk op de wettelijke of reglementaire bepalingen terzake of de bepalingen genomen in uitvoering van voornoemde bepalingen.

3 De melding

3.1 Doel van de melding

Elke inbreuk met betrekking tot de in punt 2.2 bedoelde gebieden alsook elke informatie over dergelijke inbreuken, met inbegrip van elk redelijk vermoeden van daadwerkelijke of potentiële inbreuken die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden binnen de Ondernemingen, en pogingen om dergelijke inbreuken binnen de Ondernemingen te verbergen, kunnen schriftelijk of mondeling worden aangemeld via een van de in punt 4 bedoelde kanalen.

3.2 De voorwaarden voor een melding en bescherming

De melding moet te goeder trouw gebeuren en mag niet gebaseerd zijn op loutere geruchten of roddels noch mag de melding tot doel hebben de Ondernemingen schade te berokkenen.

De melder moet redelijke gronden hebben om aan te nemen dat de informatie over de overtredingen op het moment van de melding waar was.

Wanneer de melding valse, ongefundeerde of opportunistische aantijgingen bevat, of uitsluitend wordt gedaan met het doel anderen te benadelen of schade toe te brengen, kunnen de Ondernemingen passende disciplinaire en/of gerechtelijke maatregelen nemen tegen de melder, waaronder het opleggen van sancties overeenkomstig het arbeidsreglement van de Ondernemingen.

4 Meldingskanalen

Elke persoon die onder dit beleid valt en die informatie heeft over reële of vermoede inbreuken bedoeld in punt 2.2 wordt aangemoedigd om dit zo spoedig mogelijk te goeder trouw en overeenkomstig de principes zoals opgenomen in punt 3.2 aan de Ondernemingen te melden. Vooraleer onderstaande specifieke meldingskanalen gebruikt worden, verdient het de voorkeur dat de medewerker in eerste instantie melding maakt bij de directe leidinggevende, het afdelingshoofd, HR of bij Legal.

4.1 Interne meldingskanalen

4.1.1 Wie kan gebruik maken van het intern meldingskanaal?

Alle medewerkers of andere personen die onder dit beleid vallen, kunnen gebruik maken van de door de Ondernemingen ter beschikking gestelde interne meldkanalen.

4.1.2 Welke kanalen staan ter beschikking?

Indien een medewerker of andere persoon geen melding kan of wenst te maken bij de directe leidinggevende, het afdelingshoofd, HR of bij Legal, kunnen onderstaande specifieke kanalen gebruikt worden:

- psaantwerp.sdwhistle.com
- psa.sdwhistle.com
- mpet.sdwhistle.com
- ats.sdwhistle.com

Of:

- Per post naar het volgende adres: HR, Napelsstraat 79, 2000 Antwerpen
- Per telefoon of per email naar de gekende vertrouwenspersonen binnen de Ondernemingen

De melding vindt bij voorkeur plaats in het Nederlands, Frans of Engels. Elke melding die in een andere taal gebeurt, zal eerst moeten worden vertaald aangezien dit de nauwkeurigheid van de inhoud van de melding kan aantasten.

Deze meldingskanalen zijn te allen tijde toegankelijk, 24 uur per dag, 7 dagen per week.

Het is ook mogelijk om te verzoeken om een persoonlijke ontmoeting met de meldingsbeheerder zoals hieronder vermeld in punt **4.1.4** van dit beleid.

Elk van de bovengenoemde kanalen wordt op een vertrouwelijke en beveiligde manier beheerd, zodat de vertrouwelijkheid van de identiteit van de melder en eventuele in de melding genoemde derden gewaarborgd is. De toegang tot de kanalen is strikt beperkt tot werknemers die er toegang toe hebben op basis van verantwoordelijkheden en/of bevoegdheden.

4.1.3 Hoe verloopt de melding?

Een melding omvat een korte omschrijving van de redelijke vermoedens over een gepleegde of mogelijke inbreuk op één van de in artikel 2.2. vermelde domeinen die heeft plaatsgevonden of die zeer waarschijnlijk zal plaatsvinden alsmede over de eventuele pogingen tot het verhullen of verbergen van dergelijke inbreuken.

De melding kan naar keuze van de melder al dan niet anoniem geschieden op via de vermelde kanalen in artikel 4.1.2.

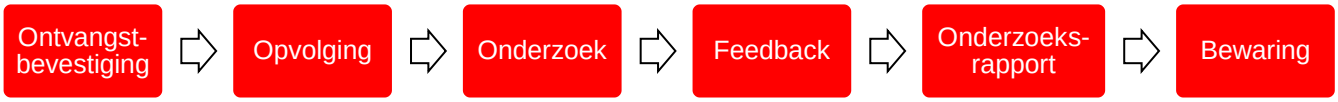
De Ondernemingen moedigen meldingen op een anonieme wijze niet aan, aangezien dit de Ondernemingen belet om de melding naar behoren te onderzoeken en te behandelen. Indien de melder zich echter toch niet comfortabel zou voelen, kan de melder er uiteraard voor kiezen om anoniem te blijven. De Ondernemingen zullen uiteraard deze keuze van de melder respecteren en een anonieme melding zal even ernstig genomen worden als een niet-anonieme melding.

De melding moet voldoende gedetailleerd en gedocumenteerd zijn en moet de volgende gegevens bevatten (wanneer de relevante informatie bekend is):

- een gedetailleerde beschrijving van de gebeurtenissen en hoe deze onder de aandacht van de melder zijn gekomen;

- de datum en plaats van de gebeurtenis;
- de namen en functies van de betrokken personen, of informatie die hun identificatie mogelijk maakt;
- de namen van andere personen, indien van toepassing, die de gemelde feiten kunnen bevestigen;
- bij het doen van een melding, de naam van de melder (deze informatie wordt niet gevraagd wanneer een anonieme melding kan worden gedaan); en
- alle andere informatie of elementen die het onderzoeksteam kunnen helpen om de feiten te verifiëren.

4.1.4 Wat gebeurt er na de melding?



1-Ontvangstbevestiging
De opsteller van de melding zal binnen 7 dagen na melding een ontvangstbevestiging ontvangen.

2-Opvolging
Opvolging verwijst naar elk optreden van de ontvanger van een melding om de juistheid van de in de melding gedane beweringen na te gaan en de gemelde inbreuk zo nodig aan te pakken, onder meer via maatregelen zoals een intern vooronderzoek, onderzoek, vervolging, een terugvordering van middelen of het beëindigen van de procedure.

De meldingsbeheerder volgt meldingen op, onderhoudt de communicatie met de melder, vraagt indien nodig bijkomende informatie op, koppelt terug naar de melder en neemt eventueel nieuwe meldingen in ontvangst.

3-Onderzoek
De meldingsbeheerder kan beslissen een melding wel of niet te onderzoeken na hierover te hebben overlegd met het management binnen de organisatie.

De melding zal snel en zorgvuldig worden onderzocht in overeenstemming met dit beleid. Alle onderzoeken worden grondig uitgevoerd met inachtneming van de beginselen van vertrouwelijkheid, onpartijdigheid en eerlijkheid ten opzichte van alle betrokken personen. De meldingsbeheerder stelt, indien nodig, een onderzoeksteam samen.

Personen die betrokken zijn bij de (mogelijke) inbreuken die door de melder worden gemeld, worden uitgesloten van het onderzoeksteam en mogen ook niet deelnemen aan de beoordeling van de melding of de vaststelling van de te ondernemen acties met betrekking tot de melding.

Belangenconflicten worden gerapporteerd aan de raad van bestuur indien de directie/het dagelijks bestuur wordt geviseerd in de melding. Indien de raad van bestuur betrokken lijkt, dan wordt de algemene vergadering van de Ondernemingen ingelicht.

4-Feedback
De meldingsbeheerder zal de melder passende feedback geven binnen een redelijke termijn, en ten hoogste binnen drie maanden vanaf de datum van de ontvangstbevestiging van de melding. Deze

feedback bevat informatie voor de melder over de geplande en/of ondernomen maatregelen en de redenen voor deze maatregelen. Hij/zij informeert de melder via het gekozen interne meldingskanaal.

5-Onderzoeksrapport
Na afloop van het onderzoek stelt het onderzoeksteam een overzichtsrapport op, waarin de uitgevoerde onderzoeksmaatregelen worden beschreven. Een geredigeerde, niet- vertrouwelijke en geanonimiseerde versie van dit overzichtsrapport kan, uitsluitend op 'need- to-know'-basis, buiten het onderzoeksteam worden gedeeld met het lokale of executive management om tot een definitieve beslissing te komen.

Een lid van het onderzoeksteam stelt een eindrapport op met een beschrijving van de feiten en de uiteindelijke beslissing:

i. In het geval dat de (mogelijke) inbreuk wordt aangetoond, worden relevante acties vastgesteld met het oog op het tegengaan van de (mogelijke) inbreuk en het beschermen van de Onderneming; of
ii. In het geval dat uit het onderzoek blijkt dat er onvoldoende of geen bewijs is van de (mogelijke) inbreuk, wordt er geen verdere actie ondernomen.

De melder wordt via het door gekozen intern meldingskanaal geïnformeerd over de afsluiting van de melding en de genomen beslissing.

4.1.5 De meldingsbeheerder

Als meldingsbeheerders van de Ondernemingen worden de gekende vertrouwenspersonen binnen de Ondernemingen aangeduid.

De meldingsbeheerders voeren hun taak onafhankelijk en zonder belangenconflict uit. Zij zijn onderworpen aan een geheimhoudingsplicht.

4.1.6 Registratie van de meldingen

De Ondernemingen houden een register bij van alle ontvangen meldingen, in overeenstemming met de vertrouwelijkheidsmaatregelen die in paragraaf 5.1 van dit beleid worden uiteengezet.

Deze meldingen en de ermee verbonden informatie worden bewaard zolang de contractuele relatie tussen de melder en de Ondernemingen loopt en voor een maximale termijn van vijf jaar.

Wanneer voor het melden, met de instemming van de melder, een telefoonlijn met gespreksopname of een ander spraakberichtsysteem met gespreksopname wordt gebruikt, zullen de Ondernemingen de mondelinge melding als volgt registreren:

- door een opname van het gesprek in een duurzame en opvraagbare vorm; of
- door een volledige en nauwkeurige schriftelijke weergave van het gesprek opgesteld door de meldingsbeheerders. De melder zal de mogelijkheid worden geboden deze schriftelijke weergave te controleren, corrigeren en voor akkoord te tekenen.

Indien voor de melding een telefoonlijn zonder gespreksopname of een ander spraakberichtsysteem zonder gespreksopname wordt gebruikt, zullen de Ondernemingen de mondelinge melding registreren in de vorm van een nauwkeurig verslag van het gesprek, opgesteld door het voor het behandelen van

de melding verantwoordelijke personeelslid. De melder zal de mogelijkheid worden geboden dit verslag te controleren, corrigeren en voor akkoord te tekenen.

In geval een persoonlijke ontmoeting plaatsvindt met een meldingsbeheerder zal, mits de melder hiermee instemt, een volledig en nauwkeurig verslag van het onderhoud worden bijgehouden in een duurzame en opvraagbare vorm. De Ondernemingen hebben het recht om het onderhoud te registeren als volgt:

- door een gespreksopname in een duurzame en opvraagbare vorm;
- door een nauwkeurig verslag van het onderhoud. De melder zal de mogelijkheid worden geboden dit verslag te controleren, corrigeren en voor akkoord te tekenen.

4.2 Externe meldingskanalen

1-
Melders kunnen gebruik maken van een extern meldingskanaal na melding via de interne kanalen of rechtstreeks via de externe meldingskanalen indien zij dit geschikter achten.

2-
De Federale Coördinator is door de Belgische wetgever belast met de coördinatie van meldingen die via externe kanalen worden ingevoerd.

Hij/zij is verantwoordelijk voor het ontvangen van externe meldingen, het controleren van de ontvankelijkheid ervan en het doorsturen naar de bevoegde autoriteit voor onderzoek, die verschillend zal zijn naargelang het voorwerp van de melding.

Deze autoriteit kan bijvoorbeeld de FOD Beleid & Ondersteuning zijn (op het gebied van overheidsopdrachten), de Autoriteit voor Financiële Diensten en Markten (FSMA), de Nationale Bank van België (NBB) of het College van Toezicht op de Bedrijfsrevisoren (op het gebied van financiële diensten, producten en markten), de FOD Economie (op het gebied van consumentenbescherming), de Gegevensbeschermingsautoriteit (op het gebied van de bescherming van de persoonlijke levenssfeer en persoonsgegevens), enz.

In uitzonderlijke gevallen kan de Federale Coördinator ook het onderzoek ten gronde voeren.

De contactgegevens van de Federale Coördinator zijn als volgt:

Adres: Leuvenseweg 48 bus 6, 1000 Brussel
Online klacht: https://www.federaalombudsman.be/nl/klachten/dien-een-klacht-in
E-mail: contact@federaalombudsman.be
Telefoon: 0800 99 961
Fax: 02 289 27 28

5 Beschermingsmaatregelen

De Ondernemingen engageren zich ertoe om alles in het werk te stellen om de personen die onder dit beleid vallen, een gepaste en effectieve bescherming te bieden voor zover de melding voldoet aan de voorwaarden van de Wet met name door de volgende maatregelen te nemen:

5.1 Waarborg van de vertrouwelijkheid

De Ondernemingen garanderen de nodige maatregelen te nemen opdat werknemers en andere door dit beleid beoogde personen in alle vertrouwen een melding kunnen neerleggen bij de Ondernemingen.

De Ondernemingen verbinden zich ertoe de nodige maatregelen te voorzien zodat de identiteit van de melder niet zonder zijn vrije en uitdrukkelijke toestemming kan worden bekend gemaakt aan andere personen dan de personeelsleden die bevoegd zijn om meldingen te ontvangen of op te volgen.

Dit geldt ook voor alle informatie waaruit de identiteit van de melder rechtstreeks of onrechtstreeks kan worden afgeleid.

In afwijking van het vorige lid kan de identiteit van de melder van de inbreuk worden bekendgemaakt wanneer dit krachtens bijzondere wetgeving in het kader van een onderzoek door de nationale autoriteiten of in het kader van een gerechtelijke procedure noodzakelijk en evenredig is, met name ter bescherming van de rechten van de verdediging van de betrokkene.

In het laatste geval wordt de melder geïnformeerd over de bekendmaking van zijn of haar identiteit voordat deze plaatsvindt, tenzij deze informatie lopende onderzoeken of gerechtelijke procedures in gevaar zou brengen. Dit is bijvoorbeeld het geval als de melder een belangrijke getuige in de rechtbank vertegenwoordigt of in geval van ongerechtvaardigde of onrechtmatige aangifte om de rechten van de verdediging van de betrokkene te beschermen.

5.2 Bescherming tegen represaillemaatregelen

Elke vorm van represailles tegen de in artikel 2.1 bedoelde personen die krachtens dit beleid bescherming genieten, met inbegrip van het dreigen met represailles en pogingen tot represailles, is verboden, met name in de volgende vormen:

- schorsing, tijdelijke buitendienststelling, ontslag of soortgelijke maatregelen
- degradatie of weigering tot promotie;
- wijziging van functie, verandering van werkplaats, vermindering van loon, wijziging van werktijden;
- schorsing van of weigering tot opleiding
- negatieve prestatiebeoordeling of negatieve referentie;
- het opleggen of toepassen van een disciplinaire maatregel, berisping of andere sanctie, met inbegrip van een financiële sanctie;
- dwang, intimidatie, pesterijen of uitsluiting;
- discriminatie, nadelige of ongelijke behandeling;
- het niet omzetten van een tijdelijke arbeidsovereenkomst in een arbeidsovereenkomst voor onbepaalde tijd, terwijl de werknemer de gerechtvaardigde verwachting had dat hem een arbeidsovereenkomst voor onbepaalde tijd zou worden aangeboden;
- niet-verlenging of vervroegde beëindiging van een tijdelijke arbeidsovereenkomst;
- schade, waaronder reputatieschade, met name op sociale media, of financieel nadeel, waaronder omzetderving en inkomstenderving;
- opname op een zwarte lijst op basis van een informele of formele overeenkomst voor een hele sector of bedrijfstak, waardoor de melder geen werk meer kan vinden in de sector of bedrijfstak;

- vroegtijdige beëindiging of opzegging van een overeenkomst voor de levering van goederen of diensten;
- intrekking van een licentie of vergunning;
- psychiatrische of medische verwijzingen.

6 Verwerking van persoonsgegevens

In het kader van de interne meldingsprocedure worden de Ondernemingen beschouwd als de verantwoordelijke voor de verwerking van de persoonsgegevens.

Elke verwerking van persoonsgegevens in het kader van dit beleid wordt uitgevoerd overeenkomstig de toepasselijke wetgeving inzake de bescherming van persoonsgegevens, met inbegrip van de Europese Algemene Verordening Gegevensbescherming ("AVG" of "GDPR").

De volgende persoonsgegevens kunnen worden verwerkt in het kader van een melding: naam, functie, datum van indiensttreding, contactgegevens en e-mailadres van de melder en van personen, betrokken bij de inbreuk, alle geïdentificeerde of identificeerbare informatie die de melder levert en die wordt verzameld in het kader van het intern onderzoek. Deze verwerking van gegevens gebeurt in het kader van de naleving van een wettelijke verplichting en/of het gerechtvaardigd belang van de ondernemingen, in de mate het intern meldkanaal de wettelijke doelstellingen overstijgt, met name de detectie van inbreuken, het waarborgen van de veiligheid en het ethisch handelen van de Ondernemingen.

Persoonsgegevens die duidelijk niet relevant zijn voor de verwerking van een melding worden niet verzameld of, indien verzameld, zo spoedig mogelijk verwijderd. Deze gegevens worden bijgehouden tot wanneer de inbreuk waarvan melding werd gedaan, is verjaard en in elk geval gedurende een termijn van vijf jaar na de melding.

De identiteit van de melder kan enkel bekend worden gemaakt met de toestemming van de melder. Andere gegevens blijven eveneens strikt confidentieel en worden enkel gedeeld op een strikte need-to-know basis.

Alle personen van wie persoonsgegevens worden verwerkt in het kader van meldingen van inbreuken hebben recht op inzage en kopie, recht op rectificatie, recht op gegevenswissing, recht van bezwaar en recht om een klacht in te dienen bij de toezichthoudende autoriteit overeenkomstig de toepasselijke wetgeving. Deze rechten kunnen evenwel beperkt worden door de rechten en vrijheden van anderen, in het bijzonder het recht van de melder op geheimhouding en het recht van de Ondernemingen op een correcte opvolging van de melding.

7 Inwerkingtreding

Dit beleid gaat in op 15 februari 2023 voor onbepaalde tijd.

De Ondernemingen behouden zich het recht voor om dit beleid te allen tijde te wijzigen, onder meer maar niet uitsluitend naar aanleiding van wijzigingen in relevante wetgeving en/of operationele behoeften.