TOWERS WATSON LIFESIGHT OFP
Organisme voor de Financiering van Pensioenen
Instelling voor bedrijfspensioenvoorziening toegelaten op 25 augustus 2015 (FSMA 50.616)
Da Vincilaan 5 | Building Caprese | 1930 Zaventem | België
Ondernemingsnummer 629 749 932

Procedure voor het melden van inbreuken

(Klokkenluidersbeleid)

1 Inleiding

De wet van 28 november 2022[1] (hierbij de "klokkenluiderswet") verplicht elke instelling voor bedrijfspensioenvoorziening (IBP) te beschikken over een doeltreffende procedure voor het melden van inbreuken die een betere bescherming biedt aan personen die te goeder trouw inbreuken melden in of buiten een werk-gerelateerde context, zonder de normale rapportagekanalen te doorlopen.

Iedere melder ("klokkenluider") vermeld in artikel 2, moet de mogelijkheid hebben om (potentiële) inbreuken te melden aan een bevoegd persoon binnen de IBP, in vertrouwen en zonder vrees voor represailles, in geval van potentiële of daadwerkelijke inbreuken op de in artikel 3 opgesomde wettelijke-en reglementaire bepalingen, die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden, alsook in geval van pogingen om dergelijke inbreuken te verbergen, met inbegrip van redelijke vermoedens.

Dit document beschrijft de door de IBP goedgekeurde procedure, die tot doel heeft iedere persoon vermeld in artikel 2 de gelegenheid te geven om (potentiële) inbreuken te melden aan de IBP, zodat de IBP geschikte maatregelen kan nemen.

2. Beoogde personen- ("Klokkenluiders")

Deze interne meldingsprocedure heeft betrekking op:

- De personen die betrokken zijn bij het beheer van de IBP[2] (zowel de huidige als voormalige personen en personen wiens werkrelatie nog moet aanvangen):
    - (voormalige) leden van de Algemene Vergadering van de IBP en hun (voormalige) vertegenwoordigers;
    - (voormalige) leden van de Raad van Bestuur;
    - (voormalige) leden van het Dagelijks Bestuur (inclusief de 'Pension Fund Coördinator');
    - (voormalige) leden van het Investeringscomité;
    - leden van enig ander operationeel orgaan dat in de toekomst kan worden opgericht,
    - (voormalige) sleutelfunctiehouders;
    - (voormalige) personeelsleden van de onderaannemers van de IBP en (voormalige) werknemers van de bijdragende ondernemingen (met inbegrip van (voormalige)

[1] Zie de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unierecht- of nationale recht vastgesteld binnen een juridische entiteit in de private sector.

[2] Of het om een huidige of vroegere inbreuk gaat, of dat deze nog niet is aangevangen (in dit laatste geval wanneer informatie over Inbreuken is verkregen tijdens het aanwervingsproces of andere precontractuele onderhandelingen).

vrijwilligers, (on)betaalde stagiairs, zelfstandigen) die betrokken zijn bij het beheer van de IBP of die diensten verlenen aan de IBP;
    - Elke persoon die onder toezicht en leiding van aannemers, (onder)aannemers en leveranciers werkt.
- De personen die buiten een professionele context verkregen informatie doorgeven bij de melding van een inbreuk op het gebied van financiële diensten, producten en markten en van inbreuken op het gebied van de voorkoming van het witwassen van geld en de financiering van terrorisme.

3. Beoogde inbreuken

Onder "inbreuken" wordt verstaan handelingen of nalatigheden die onwettig zijn en betrekking hebben op de hierna opgesomde gebieden of handelingen die, het doel of de strekking van de regels op een of meer van de hierna opgesomde gebieden tenietdoen:

Belgische wetgeving	1. Overheidsopdrachten; 2. Financiële diensten, producten en markten en voorkoming van witwassen van geld en terrorismefinanciering; 3. Bescherming van de persoonlijke levenssfeer en de persoonsgegevens, en de beveiliging van netwerk -en informatiesystemen; 4. Productveiligheid en conformiteit; 5. Bestrijding van belastingfraude; 6. Bestrijding van sociale fraude;	7. Stralingsbescherming en nucleaire veiligheid; 8. Volksgezondheid; 9. Veiligheid van het vervoer; 10. Consumentenbescherming; 11. Veiligheid van levensmiddelen, diergezondheid -en welzijn; 12. Milieubescherming
Europese wetgeving	Inbreuken waardoor de financiële belangen van de Europese Unie worden geschaad zoals bedoeld in artikel 325 van het Verdrag betreffende de werking van het Europese Unie (VWEU) namelijk de fraudebestrijding, of inbreuken i.v.m de interne markt zoals bedoeld in artikel 26, §2 VWEU, d.w.z. het vrije verkeer van goederen, personen, diensten en kapitaal, ook op het gebied van mededinging en staatssteun	

“Financiële diensten, producten en markten” betreft, onder meer, de wet -en regelgeving opgenomen in artikel 45 van de Wet van 2 augustus 2002 inzake het toezicht op de financiële sector en de financiële diensten waarop de FSMA toezicht houdt. Het betreft meer bepaald:

- De Wet van 28 april 2003 met betrekking tot de aanvullende pensioenen en diens belastingstelsel evenals dat van bepaalde aanvullende voordelen op het gebied van de sociale zekerheid (WAP);
- De Wet van 27 oktober 2006 met betrekking tot het toezicht op de Instellingen voor Bedrijfspensioenvoorziening) (WIBP);
- De wet van 10 mei 2007 ter bestrijding van discriminatie tussen vrouwen en mannen;
- De wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden;

- De wet van 5 maart 2002 betreffende het principe ter voorkoming van discriminatie van deeltijdse werknemers;
- De wet van 5 juni 2002 betreffende het principe ter voorkoming van discriminatie van werknemers met een arbeidsovereenkomst voor bepaalde duur;
- De wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten;
- De wet van 18 september 2017 ter voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contant geld;
- De wet van 2 juni 2021 betreffende diverse financiële bepalingen inzake fraudebestrijding;
- Verordening (EU) 2015/847 van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie en tot intrekking van Verordening (EG) nr. 1781/2006;

Deze lijst kan worden gewijzigd naarmate nieuwe wetten worden aangenomen en bestaande wetten worden gewijzigd.

Wanneer naar een wet wordt verwezen, wordt (worden) ook het (de) uitvoeringsbesluit(en) ervan genoemd, zonder dat dit nader hoeft te worden bepaald.

Wanneer de melding een gebied betreft dat hierboven niet genoemd is, is er geen geldige interne melding en ook geen bescherming.

4. Meldingsprocedure

Er zijn verschillende procedures voor het melden van potentiële of daadwerkelijke inbreuken.

De melder dient zich te goeder trouw te handelen. Dit betekent dat hij/zij gegronde redenen had om aan te nemen dat de gemelde informatie juist was op het moment van de melding, en dat het binnen het toepassingsgebied van de geldende wetgeving viel (zoals hierboven beschreven).

Als het zou blijken dat de melder bewust valse informatie heeft gemeld of heeft bekendgemaakt, is hij/zij aansprakelijk volgens de in de wet bepaalde (straf)sancties en zal hij/zij de slachtoffers de daaruit voortvloeiende schade moeten vergoeden. Ook verliest de melder in dit geval het voordeel van de beschermingsmaatregelen artikel 7 van deze procedure.

a. Procedure voor interne melding

De personen vermeld in artikel 2 worden verzocht om elke daadwerkelijke of potentiële inbreuk vermeld in artikel 3 waarvan zij op de hoogte zijn, te melden aan de meldingsbeheerder (“Whistleblowing Officer”).

De meldingsbeheerder heeft ook de functie van *Compliance Officer* van de IBP, zoals vermeld in bijlage 2.

Indien de melding betrekking heeft op een inbreuk waarbij de meldingsbeheerder zelf betrokken is of indien de meldingsbeheerder zelf de klokkenluider is, wordt deze vervangen door de voorzitter van de Raad van Bestuur van de IBP, die dan optreedt als "back-up" meldingsbeheerder. Deze wordt vermeld in bijlage 2.

De melding kan schriftelijk en/of mondeling worden gedaan, anoniem of in alle vertrouwelijkheid. Het is mogelijk om schriftelijk per post en/of email een melding in te sturen.

Een mondelinge melding is mogelijk via de telefoon of via andere spraakberichtsystemen en, op verzoek van de melder, door middel van een fysieke ontmoeting binnen een redelijke termijn.

Wanneer een melding mondeling wordt ingediend, zijn de regels opgenomen in artikel 5.c. van toepassing.

De meldingsbeheerder zal de melder vragen om de volgende informatie of documenten te verstrekken (indien beschikbaar): De relevante feiten over de (potentiële) inbreuk, de naam en, indien van toepassing, de functie van de betrokken persoon of instelling, het tijdstip van de inbreuk, bewijs van de inbreuk, en enige andere relevante informatie.[3]

Melders worden aangemoedigd hun identiteit door te geven aan de meldingsbeheerder, wetende dat deze vertrouwelijk zal blijven en alleen bekend zal zijn bij de meldingsbeheerder en niet openbaar zal worden gemaakt, tenzij de melder hiervoor zijn vrije en uitdrukkelijke toestemming geeft, of tenzij dit wettelijk verplicht is. Door het verstrekken van de identiteit kan de meldingsbeheerder de melder informeren over zijn/haar rechten en plichten en zo nodig om aanvullende informatie vragen.

b. Procedure voor externe melding

Melders kunnen het externe meldingskanaal gebruiken om een inbreuk te melden aan een bevoegde vertrouwenspersoon die verantwoordelijk is voor de behandeling van meldingen overeenkomstig de wet, en voor het geven van feedback afhankelijk van het betrokken gebied. Dit kan nadat zij via de interne meldingskanalen hebben gerapporteerd, of door rechtstreeks gebruik te maken van de externe meldkanalen wanneer zij dit meer geschikt achten.

De lijst van bevoegde Belgische autoriteiten met verwijzingen naar de procedures en beschermingsmaatregelen voor externe meldingen zijn beschikbaar op de website van de federale Ombudsman: https://www.mediateurfederal.be. Als de melding rechtstreeks via externe kanalen gebeurt, moedigt de IBP aan om ook (potentiële) inbreuken te melden aan de contactpersoon (anoniem in overeenstemming met dit document), zodat de IBP ook intern alle nodige maatregelen kan nemen om deze (potentiële) inbreuk aan te pakken en eventuele (bijkomende) schade te voorkomen of te beperken.

In overeenstemming met de wet heeft de FSMA aan de melder duidelijke en gemakkelijk toegankelijke informatie ter beschikking gesteld over de externe meldingsprocedures: https://www.fsma.be/nl/faq/contactpunt-klokkenluiders .

De wet heeft ook een extern meldingskanaal opgezet waarop de FSMA toezicht houdt: https://www.fsma.be/nl/contactpunt-klokkenluiders .

[3] De opsteller van de melding wordt verzocht geen informatie of persoonsgegevens door te geven die duidelijk niet relevant zijn voor de behandeling van een specifieke melding. Het is bijvoorbeeld niet nodig informatie te verstrekken over de gezondheidstoestand van een gesignaleerde persoon indien deze gezondheidstoestand niets te maken heeft met de betrokken inbreuk.

5. Verwerking van de melding

Elke melding wordt uiterst vertrouwelijk en zonder represailles behandeld. Represailles zijn strikt verboden en zal door de meldingsbeheerder van de IBP nauwlettend in de gaten worden gehouden.

a. Onderzoek

Na ontvangst van de melding stuurt de contactpersoon de melder binnen zeven dagen na ontvangst van de melding een ontvangstbevestiging. In geval van een anonieme melding zal de meldingsbeheerder niet geacht zijn om een ontvangstbevestiging te sturen, en zal ook geen feedback sturen aan de melder.

De meldingsbeheerder registreert de melding in een daarvoor bestemde meldingsregister en informeert de Raad van Bestuur van het IBP. De meldingen worden bewaard voor de duur van de contractuele relatie met de melder. Na de wettelijke bewaartermijn worden alle gegevens gewist.

De meldingsbeheerder voert een vooronderzoek uit, overeenkomstig de beginselen van vertrouwelijkheid, onpartijdigheid en billijkheid ten aanzien van alle betrokken personen. De meldingsbeheerder kan contact opnemen met de melder om meer informatie en/of bewijsmateriaal over de inbreuk te verkrijgen. Hij/Zij kan ook contact opnemen met alle personen die informatie of documenten hebben die relevant zijn voor het onderzoek. De meldingsbeheerder kan ook raad vragen bij andere sleutelfunctiehouders en/of de DPO, afhankelijk van hun functiegebied en of ze niet in een belangenconflict verkeren. In dit geval zal de melder de informatie delen met de gecontacteerde perso(o)n(en), waarbij de identiteit van de melder en de persoon over wie de melding gaat, evenals de vermeende feiten, zoveel mogelijk worden beschermd. Hij/zij kan zich laten bijstaan door derden wanneer hij/zij dit nodig acht en als deze niet in een situatie van belangenconflict verkeren.

De uitkomst van dit onderzoek wordt samengevat in een schriftelijk verslag dat wordt voorgelegd aan de voorzitter van de raad van bestuur, en in het meldingsregister wordt opgenomen.

b. Opvolging

Indien het onderzoek ernstige aanwijzingen van inbreuken aan het licht brengt, stelt de voorzitter van de Raad van Bestuur, de raad op de hoogte en nodigt deze uit om te beslissen over de te nemen maatregelen.

De meldingsbeheerder wordt in kennis gesteld van het besluit van de raad van bestuur.

Elke melding wordt opgevolgd of de reden waarom er geen gevolg aan een melding werd gegeven, wordt geregistreerd in het meldingsregister.

De meldingsbeheerder geeft feedback (over de overwogen of genomen maatregelen in opvolging en over de redenen voor deze opvolging) binnen een termijn van maximaal drie maanden vanaf de ontvangstbevestiging van de melding (of, bij gebreke van een ontvangstbevestiging aan de melder, drie maanden na het verstrijken van de termijn van zeven dagen na de melding).

Indien de uiteindelijke beslissing van de Raad van Bestuur naar aanleiding van de melding, later valt dan de periode van drie maanden, zal de meldingsbeheerder verdere feedback geven aan de melder.

De meldingsbeheerder zal altijd nagaan of de FSMA of een andere bevoegde instantie op de hoogte moet worden gesteld van de inbreuk.

c. Registratie van de meldingen

Wanneer bij een mondelinge melding een telefoonlijn met gespreksopname of een ander spraakberichtsysteem met gespreksopname wordt gebruikt, heeft de contactpersoon, met instemming van de melder, het recht om het op een van de volgende manieren te registreren:

- door het maken van een opname van het gesprek in een duurzame, opvraagbare vorm; of
- door een volledige en nauwkeurige schriftelijke weergave van het gesprek opgesteld door de contactpersoon die de melding behandelt.

Indien voor de mondelinge melding een telefoonlijn zonder gespreksopname of een ander spraakberichtsysteem zonder gespreksopname wordt gebruikt, heeft de meldingsbeheerder enkel het recht om de mondelinge melding te registreren in de vorm van een nauwkeurig verslag van het gesprek.

Wanneer een persoon verzoekt om een onderhoud met de meldingsbeheerder van de IBP om een interne of externe melding te signaleren, zorgt de IBP, met toestemming van de melder, ervoor dat de bespreking volledig en nauwkeurig wordt geregistreerd in één van de volgende vormen:

- door het maken van een opname van het gesprek in een duurzame en consulteerbare vorm; of
- door een nauwkeurig verslag op te maken van de bespreking, opgesteld door de meldingsbeheerder.

De meldingsbeheerder biedt de melder de mogelijkheid de schriftelijke weergave van het verslag van het onderhoud te controleren, te corrigeren en voor akkoord te tekenen.

6. Bescherming van de persoonlijke levenssfeer

De melding wordt verwerkt in overeenstemming met de wetgeving met betrekking tot de bescherming van de persoonlijke levenssfeer en persoonsgegevens en met Bijlage 1 in het kader van een interne melding.

De IBP is de verwerkingsverantwoordelijke voor de persoonsgegevens die in kader van de interne meldprocedure worden verwerkt. De naam, de functie en de contactgegevens zowel van de melder en elke persoon tot wie de beschermings- en ondersteuningsmaatregelen zich uitstrekken, als van de betrokkene, met inbegrip van, in voorkomend geval, het ondernemingsnummer, worden bijgehouden tot wanneer de gemelde inbreuk is verjaard.

Persoonsgegevens die duidelijk niet relevant zijn voor de behandeling van een specifieke melding, worden niet verzameld, of worden, indien onbedoeld verzameld, onmiddellijk gewist.

Het meldingsregister is enkel toegankelijk voor de meldingsbeheerder en de FSMA. De identiteit van de melder wordt geanonimiseerd.

7. Maatregelen ter bescherming van de klokkenluider

De IBP wil een veilige omgeving creëren waarin een melder zich op zijn gemak voelt om een inbreuk binnen de IBP te melden. Daarom zijn de volgende waarborgen ingevoerd:

Vertrouwelijkheid van de identiteit van de klokkenluider	Het verbod op elke vorm van represailles tegen de klokkenluider en aanverwante partijen
• Verwijzingen worden beheerd door de meldingsbeheerder en dossiers worden bewaard op een plaats die enkel toegankelijk is voor bevoegde personen in het onderzoeksteam; • Alle interne en externe partijen die betrokken zijn bij het onderzoek en de opvolging zijn onderworpen aan geheimhoudingsverplichtingen. Ongeoorloofde bekendmaking van informatie over het onderzoek, de rapportage of de rapporterende partij wordt niet getolereerd en kan leiden tot sancties, waaronder civiele of strafrechtelijke vervolging. • De identiteit van de klokkenluider zal niet openbaar worden gemaakt, tenzij: (i) de klokkenluider expliciet instemt met openbaarmaking; of (ii) De bekendmaking is wettelijk verplicht Een klokkenluider wordt echter ingelicht voordat zijn of haar identiteit bekend wordt gemaakt, tenzij die informatie het betrokken onderzoek of de gerechtelijke procedure in gevaar zou brengen.	De IBP zal geen enkele vorm van "represailles", met inbegrip van dreiging met en poging tot represaille, (zoals beëindiging of niet-verlenging van het contract of de ambtstermijn, ontslag, of soortgelijke maatregelen, enz.) toelaten, gericht tegen: • De klokkenluider; • een facilitator, (dit is een persoon die een klokkenluider bijstaat in het meldingsproces en wiens proces en hulp vertrouwelijk moeten zijn); • Derden die verbonden zijn met klokkenluiders en die het risico lopen op represailles in een werk-gerelateerde context, zoals collega's of familieleden van de klokkenluiders, alsook rechtspersonen die eigendom zijn van of geëxploiteerd worden door de klokkenluiders of waarmee zij verbonden zijn of waarmee zij een professionele relatie hebben, zoals een beheermaatschappij.

Indien een klokkenluider of een van deze personen represailles vreest of het gevoel heeft dat er reeds represailles tegen hem of haar zijn genomen, wordt hij of zij aangemoedigd zijn of haar bezorgdheid onverwijld aan de meldingsbeheerder te melden.

De klokkenluider (of de personen die deze bijstaan) die meent slachtoffer te zijn van of bedreigd wordt met een represaille kan een met redenen omklede klacht indienen bij de federale Ombudsman, door gebruik te maken van de informatie die onder artikel 4.b van deze procedure wordt vermeld.

Elke persoon die slechtoffer wordt van represailles heeft het recht om een beroep in te leiden voor de arbeidsrechtbank overeenkomstig artikel 578 van het Gerechtelijk Wetboek.

8. Mededeling van de onderhavige procedure

Het IBP deelt deze procedure tevens mee aan de beoogde personen die betrokken zijn bij het beheer van het IBPP, haar leveranciers en sleutelfunctiehouders, alsook aan de leden van de operationele organen, en van de Algemene Vergadering en bijdragende ondernemingen. Dienstverleners van de IBP verbinden zich tot het meedelen van deze interne procedure aan elk lid van hun personeel dat voor de IBP werkt.

De Raad van Bestuur zal dit beleid regelmatig evalueren, minstens om de drie jaar, of eerder in geval van belangrijke gebeurtenissen. Indien nodig zal de Raad van Bestuur het beleid bijwerken.

Deze interne procedure werd goedgekeurd door de Raad van Bestuur op 17 maart 2023

Els De Jaeger	Sven Schroven
Voorzitter van de Raad van Bestuur	Vice-voorzitter van de Raad van Bestuur
Towers Watson LifeSight OFP	Towers Watson LifeSight OFP

Bijlage 1: Verwerking van persoonsgegevens in het kader van interne meldingen

In deze bijlage wordt uitgelegd hoe de IBP omgaat met de persoonsgegevens van de melder, van een persoon die het onderwerp is van een melding of van een andere derde die bij die gelegenheid wordt genoemd. Deze bijlage moet worden gelezen in combinatie met de algemene privacyverklaring van de IBP, die beschikbaar is op https://www.lifesight.com/privacy-policy of op verzoek in beide gevallen.

Betreffende de meldingsbeheerder (artikel 13 GDPR)		
Doeleinden	De aan de IBP verstrekte gegevens worden gebruikt om de melder een ontvangstbevestiging van de melding te sturen, normaliter binnen 7 dagen na ontvangst van de melding. De gegevens worden ook verwerkt ten behoeve van de follow-up van de melding, d.w.z. elke actie die door de melder en het onderzoeksteam, of een bevoegde autoriteit, wordt ondernomen om de juistheid van de beweringen in het rapport te beoordelen en, indien nodig, de gemelde inbreuk te herstellen.	
Rechtsgronden	De IBP is krachtens de wet van 28 november 2022 betreffende de bescherming van personen die schendingen van het recht van de Europese Unie of het nationale recht binnen een rechtspersoon in de privésector melden, wettelijk verplicht een procedure voor het melden van schendingen in te stellen. De melder heeft ingestemd met de verwerking van dergelijke gegevens (artikel 6.1.a) GDPR).	
Gegevenscategorieën	Dit omvat naam, functie, relatie tot de IBP, informatie over de overtreding (al dan niet een strafbaar feit) en informatie over mogelijke sancties.	
Duur	Wanneer het verslag leidt tot een bevestigde inbreuk	Totdat de gemelde overtreding is verjaard, met inbegrip van de verjaring van middelen tegen een gerechtelijke, administratieve of andere beslissing. In geval van strafrechtelijke vervolging: 5 jaar voor overtredingen. In geval van burgerlijke aansprakelijkheid: 5 jaar. In geval van contractuele aansprakelijkheid: 10 jaar. De gegevens die nodig zijn om aan de interne registratieverplichting te voldoen, worden bewaard voor de duur van de desbetreffende werkrelatie met de klokkenluider.
Begunstigden	De gegevens van de melder moeten worden meegedeeld aan de IBP en, indien nodig, aan de bevoegde autoriteiten. Deze gegevens kunnen ook geheel of gedeeltelijk worden meegedeeld aan de persoon die het onderwerp is van de melding of aan andere in de melding genoemde derden in de door de geldende wetgeving bepaalde gevallen.	

Betreffende de persoon die het onderwerp is van de melding of enige andere bij die gelegenheid genoemde derde (artikel 14 GDPR)		
Doeleinden	De aan de IBP verstrekte gegevens over de persoon die het voorwerp uitmaakt van de melding of over een andere derde die bij die gelegenheid wordt genoemd, worden gebruikt om na te gaan of er een inbreuk is gepleegd door de persoon die het voorwerp uitmaakt van de melding.	
Gegevenscategorieën	Bij het opstellen van het verslag	De verzamelde en verwerkte gegevens zijn zij die de identificatie mogelijk maakt van de persoon die het onderwerp is van de melding of enige andere bij deze gelegenheid genoemde derde. Dit omvat de naam, functie, relatie tot de IBP, informatie over de overtreding (al dan niet een strafbaar feit) en informatie over sancties.
	Bij het onderzoek van het verslag	Ingeval een onderzoek wordt ingesteld om de door de melder aangevoerde feiten te verifiëren, kunnen alle nodige gegevens betreffende het onderzoek en de vaststelling van passende maatregelen om de inbreuk te herstellen, worden verzameld, met inbegrip van verslagen van de verificatiewerkzaamheden, de follow-up van het verslag en de meldingsmail.
Duur	Wanneer het verslag leidt tot een bevestigde inbreuk.	Totdat de gemelde overtreding is verjaard, met inbegrip van de verjaring van middelen tegen een gerechtelijke, administratieve of andere beslissing. In geval van strafrechtelijke vervolging: 5 jaar voor overtredingen. In geval van burgerlijke aansprakelijkheid: 5 jaar. In geval van contractuele aansprakelijkheid: 10 jaar. De gegevens die nodig zijn om aan de interne registratieverplichting te voldoen, worden bewaard voor de duur van de desbetreffende werkrelatie met de klokkenluider.
	Wanneer naar aanleiding van de melding geen daadwerkelijke schending wordt vastgesteld	Vernietiging of anonimisering van gegevens binnen 2 maanden na het einde van het onderzoek (d.w.z. vanaf het moment dat de Raad van Bestuur daartoe heeft besloten), met uitzondering van gegevens die het mogelijk maken te voldoen aan de eis om rapporten te bewaren voor de duur van de overeenkomstige werkrelatie met de melder.
Begunstigden	De gegevens moeten worden meegedeeld aan de IBP en, indien nodig, aan de bevoegde autoriteiten. Deze gegevens kunnen ook geheel of gedeeltelijk aan de melder worden meegedeeld in het kader van een terugkoppeling en follow-up van de procedure, op voorwaarde dat deze mededeling de vertrouwelijkheid van de bij de melding betrokken persoon niet in gevaar brengt of tenzij er wettelijke uitzonderingen zijn.	

Bijlage 2: Contactgegevens van de meldingsbeheerder & interne rapportagekanalen

1. Contactgegevens van de meldingsbeheerder

"Priority" meldingsbeheerder
Younity Vertegenwoordigd door Corinne Merla Compliance Officer
"back up" meldingsbeheerder in het geval dat "priority" meldingsbeheerder niet bevoegd is om op te treden:
Els De Jaeger Voorzitter van de Raad van Bestuur

2. Interne rapportagekanalen

"Priority" rapportagekanaal	
E-mail	corinne.merla@younity.be[4]
Adres[5]	Younity, ter attentie van Mevr. Corinne Merla Vorstlaan 36/8, 1170 Brussel.
Telefoonnummer	+32 2 880 77 88
"back up" kanaal wanneer het prioriteitskanaal niet bevoegd is om te op te treden (zie artikel 4, laatste alinea van de procedure)	
E-mail	els.de.jaeger@wtwco.com
Adres	Willis Towers Watson Consulting BV, ter attentie van Mevr. Els De Jaeger, Da Vincilaan 5, Gebouw Caprese, 1930 Zaventem.
Telefoonnummer	+32 2 678 15 78

[4] Wij herinneren u eraan dat de verzender meestal de mogelijkheid heeft om de optie "privé" in zijn e-mail te activeren.
[5] Gelieve op de envelop "Vertrouwelijk" te vermelden.

Bijlage 3: Historiek van het beleid

Datum van wijziging	Versie	Wijziging	Goedkeuringsdatum
N/A	1.0	Eerste versie	29 December 2020
9 November 2021	1.1	- Ondertekende versie	9 November 2021
17 Maart 2023	1.2	- wijzigingen naar aanleiding van de Belgische klokkenluiderswet van 28 november 2022	17 Maart 2023