

INTERN MELDINGSBELEID « WHISTLEBLOWING »

CONTASSUR N.V.

CONTASSUR BIJSTAND ADVIES N.V.

Versie: 2025

Validatie Raad van bestuur van Contassur en Contassur Bijstand Advies: december 2025

INHOUDSTAFEL

INLEIDING	2
1. BETROKKEN PERSONEN	3
2. BEOOGDE INBREUKEN	3
3. PROCEDURE	4
4. VERWERKING VAN DE MELDING	5
4.1. Intern meldingskanaal	5
4.2. Extern meldingskanaal	6
4.3. Openbaarmaking	7
5. BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER	7
6. BESCHERMING	7
7. SANCTIES	9
8. OPENBAARHEID VAN DIT BELEID	9
BIJLAGE 1 – CONTACTGEGEVENS VAN DE VOORZITTER VAN DE RAAD VAN BESTUUR	10
BIJLAGE 2 – VERWERKING VAN PERSOONSGEGEVENS IN HET KADER VAN EEN INTERNE MELDING	11

Goedkeuring door de raad van bestuur van Contassur en Contassur Bijstand-Advies: december 2025.

INLEIDING

Onverminderd de toepassing van de bepalingen van de wetgeving inzake de bescherming van de persoonlijke levenssfeer, werd deze interne meldersprocedure ('whistleblowing'-procedure) vastgesteld door de Raden van bestuur van Contassur en Contassur Bijstand Advies (CBA), hierna de onderneming(en) genoemd, met het oog op het beperken van de risico's op financieel verlies en/of reputatieschade als gevolg van niet-naleving van het geldende recht en beleid, de waarden en beginselen die zijn vastgelegd in het integriteitsbeleid.

Het doel van dit beleid is:

- om de procedurele mogelijkheden op te sommen waarmee een potentiële inbreuk binnen Contassur of CBA kan worden gemeld;
en
- om de personen op wie dit beleid van toepassing is te informeren over de bescherming die een melder geniet (ook wel klokkenluider genoemd).

Op deze manier willen Contassur en CBA transparantie bieden over hoe bepaalde problematische situaties kunnen worden aangepakt, zodat ze nader onderzocht kunnen worden en eventueel passende maatregelen genomen kunnen worden.

Dit is een aanvullende en subsidiaire procedure naast de gebruikelijke interne procedures en interne controlemechanismen. Er wordt een beroep op gedaan wanneer de melder van mening is dat hij/zij de normale hiërarchische weg niet kan of niet langer kan volgen.

1. BETROKKEN PERSONEN

De personen die onder dit interne meldingsbeleid vallen, zijn degenen die zich in een professionele context bevinden met Contassur en/of CBA:

- werknemers van de onderneming;
- zelfstandigen, aannemers en onderaannemers en hun personeel of aangestelden waarmee de onderneming samenwerkt;
- aandeelhouders en de leden van de operationele organen (met inbegrip van de leden die niet betrokken zijn bij het dagelijks beheer);
- onderaannemers waarmee de onderneming samenwerkt en hun personeel;
- eventuele bezoldigde of onbezoldigde stagiairs of vrijwilligers;
- eventuele sollicitanten;
- uit dienst getreden werknemers van de onderneming.

Ook alle natuurlijke personen vallen onder dit interne meldingsbeleid, zelfs als zij zich niet in een professionele relatie met de onderneming(en) bevinden, maar een (potentiële) inbreuk willen melden met betrekking tot diensten, producten en financiële markten, of inzake de strijd tegen witwassen van geld en de financiering van terrorisme.

Wat betreft de beschermingsmaatregelen, is dit beleid ook van toepassing op facilitators (personen die een melder vertrouwelijk bijstaan in het meldingsproces), derden die verbonden zijn met de melder en eveneens het risico lopen op represailles (bv. familieleden, collega's enz.) en op rechtspersonen die toebehoren aan de melder, waarvoor de melder werkt of waarmee de melder professioneel verbonden is.

2. BEOOGDE INBREUKEN

De volgende door melders geconstateerde (potentiële) inbreuken kunnen door hen worden gemeld:

- elk onethisch of illegaal gedrag betreffende aspecten die onder de bevoegdheid en controle van Contassur en CBA vallen;
- elke inbreuk (of vermoeden van inbreuk):
 - op de waarden, principes en regels die zijn vastgelegd in hun integriteitsbeleid;
 - op de wetten waarvan de NBB en de FSMA de naleving controleren.¹ Dat zijn in het bijzonder:
 - De WAP (met name de wet van 28 april 2003 betreffende de aanvullende pensioenen en het belastingstelsel van die pensioenen en van sommige aanvullende voordelen inzake sociale zekerheid);
 - De Solvency II-wetgeving (met name de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen);
 - De wet van 4 april 2014 betreffende de verzekeringen;
 - De wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie;
 - De wet van 10 mei 2007 ter bestrijding van discriminatie tussen vrouwen en mannen;

¹ Zie artikel 45 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten.

- De wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden;
- De wet van 5 maart 2002 betreffende het beginsel van non-discriminatie ten gunste van deeltijdwerkers;
- De wet van 5 juni 2002 betreffende het non-discriminatiebeginsel ten voordele van werknemers met een arbeidsovereenkomst voor bepaalde tijd.

Ook worden de inbreuken beoogd die worden opgesomd in de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector, met name:

- Alle mogelijke inbreuken (d.w.z. een handeling of nalatigheid) die betrekking hebben op:
 - overheidsopdrachten;
 - financiële diensten, producten en markten, voorkoming van witwassen van geld en financieren van terrorisme;
 - 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.

Dit beleid is ook van toepassing op inbreuken waardoor de financiële belangen van de Europese Unie worden geschaad en op inbreuken in verband met de interne markt (met inbegrip van inbreuken op de Unieregels inzake mededinging en staatssteun).

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

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

3. PROCEDURE

Elke inbreuk met betrekking tot bovengenoemde gebieden kan naar keuze worden gemeld aan:

- de Compliance Officer van Contassur (meldingsbeheerder) ('intern meldingskanaal'):

Mevrouw Arielle Deltombe
 Contassur nv
 Kunstlaan 47, 1000 Brussel
Arielle.Deltombe@contassur.com
 + 32 2 546 10 00

Indien de melding betrekking heeft op de Compliance Officer, of indien hij/zij zelf een melding doet, wordt hij als meldingsbeheerder vervangen door de voorzitter van de Raad van bestuur van Contassur. (zie contactgegevens in bijlage 1)

- de federale coördinator of aan de bevoegde autoriteiten ('extern meldingskanaal'). Daartoe moet de melder contact opnemen met:
 - de bij koninklijk besluit als bevoegd verklaarde autoriteiten afhankelijk van het betrokken domein.
 - de federale ombudsmannen, die zullen optreden als federaal coördinator voor externe meldingen via www.mediateurfederal.be / www.federaalombudsman.be.
 De federale ombudsmannen hebben de opdracht om:
 - externe meldingen van inbreuken te ontvangen;
 - na te gaan of ze ontvankelijk zijn en of er een redelijk vermoeden is dat de gemelde inbreuken hebben plaatsgevonden;
 - en, indien dit het geval is, het doorsturen van de melding naar de bevoegde autoriteit zodat zij een onderzoek kan starten.

In uitzonderlijke gevallen, zoals wanneer geen enkele instantie bevoegd is, komen de federale ombudsmannen tussenbeide om het onderzoek ten gronde uit te voeren.

Elke aangewezen instantie publiceert de volgende informatie op een afzonderlijke, herkenbare en toegankelijke pagina van haar website:

- de voorwaarden voor de bescherming;
- haar contactgegevens;
- de concrete procedure;
- de regels inzake vertrouwelijkheid;
- de opvolgingsmaatregelen;
- de beroepsmogelijkheden en procedures ter bescherming tegen represailles.

Melders kunnen de melding intern ('intern meldingskanaal') of extern ('extern meldingskanaal') doen. Ze worden echter aangemoedigd om eerst de in dit beleid beschreven interne meldersprocedure te volgen, om mogelijk een interne oplossing voor het gemelde probleem te vinden, alvorens eventueel over te gaan tot een externe melding.

Een interne melding kan schriftelijk gebeuren per brief en/of e-mail, of mondeling via telefoon of andere voicemailsysteem of, op verzoek van de melder, door middel van een persoonlijke ontmoeting binnen een redelijke termijn.

Interne meldingen kunnen anoniem worden gedaan.

De personen die een interne melding doen, worden niettemin aangemoedigd om hun identiteit aan de contactpersoon bekend te maken, met dien verstande dat deze vertrouwelijk zal blijven en alleen bekend zal zijn bij de contactpersoon en niet zal worden bekendgemaakt, tenzij dit wettelijk verplicht is. Het verstrekken van de identiteit stelt de contactpersoon in staat om de melders te informeren over hun rechten en plichten en zo nodig om nadere informatie te vragen

4. VERWERKING VAN DE MELDING

4.1. Intern meldingskanaal

Ongeacht de door de melder gekozen methode om de (potentiële) inbreuk intern te melden (mondeling of schriftelijk), is de vertrouwelijkheid van de identiteit van de melder en van eventuele in de melding genoemde derden altijd gewaarborgd.

Die gegevens zijn alleen toegankelijk voor de Compliance Officer, in zijn hoedanigheid van meldingsbeheerder (of voor de voorzitter van de betrokken Raad van Bestuur in het geval deze de Compliance Officer vervangt). Deze garandeert steeds een neutrale en onafhankelijke opvolging van de melding en de afwezigheid van mogelijke belangenconflicten.

De Compliance Officer (of de voorzitter van de Raad van bestuur indien hij/zij de Compliance Officer vervangt) zal zich steeds professioneel en integer gedragen, waarbij de melding altijd met de nodige discretie wordt behandeld met inachtneming van de bepalingen van de wetgeving inzake de bescherming van de persoonlijke levenssfeer, en een zorgvuldige opvolging en verwerking van de melding zijn gewaarborgd.

De meldingsbeheerder registreert de melding in een daartoe bestemd meldingsregister en informeert de voorzitter van de Raad van bestuur van Contassur of CBA dat er een melding werd gedaan.

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

Binnen 7 dagen na ontvangst van de melding stuurt de meldingsbeheerder de melder een ontvangstbevestiging (tenzij de melding anoniem is).

De meldingsbeheerder voert in alle discretie een onderzoek uit. Daartoe kan hij/zij contact opnemen met elke persoon die hij/zij noodzakelijk acht.

Uiterlijk 3 maanden na de ontvangstbevestiging krijgt de melder feedback over de maatregelen die worden gepland of zijn genomen als opvolging van zijn melding en over de redenen van de opvolging.

De conclusies van dit onderzoek worden opgenomen in een schriftelijk verslag dat in een geanonimiseerde versie wordt overhandigd aan de voorzitter van de betrokken Raad van bestuur (of aan de leden van de betrokken Raad van bestuur in het geval dat de voorzitter als meldingsbeheerder optreedt) en wordt geregistreerd in het meldingsregister.

Indien uit het onderzoek ernstige aanwijzingen voor inbreuken blijken, wordt dit verslag op de agenda geplaatst van de eerstvolgende vergadering van de Raad van bestuur geplaatst, die uiterlijk 3 maanden na ontvangst van het verslag beslist over het vervolg van het dossier.

De melder zal ingelicht worden over het gegeven gevolg aan de procedure die hij/zij ingesteld heeft.

4.2. Extern meldingskanaal²

De melder ontvangt een bevestiging van de melding binnen 7 dagen na ontvangst ervan, tenzij uitdrukkelijk anders verzocht door de melder of tenzij de federale ombudsmannen/de bevoegde autoriteit op redelijke gronden van oordeel zijn/is dat het versturen van een dergelijke bevestiging de identiteit van de melder in gevaar zou brengen.

Binnen een redelijke termijn, en in elk geval uiterlijk binnen 3 maanden na ontvangst van de ontvangstbevestiging van de melding, wordt feedback gegeven aan de melder. In legitieme gevallen

² De onderstaande informatie heeft betrekking op meldprocedures die worden beheerd door externe autoriteiten. Contassur en CBA hebben geen controle over de verwerkingstermijnen, de opvolgingsmodaliteiten of de door deze autoriteiten genomen beslissingen, en kunnen niet aansprakelijk worden gesteld voor eventuele vertragingen, het uitblijven van een antwoord of het seponeren van een melding.

kan worden afgeweken van die termijn van 3 maanden. In dat geval moet uiterlijk binnen 6 maanden feedback worden gegeven aan de melder.

Tot slot moet de bevoegde autoriteit de melder inlichten over het eindresultaat van de onderzoeken die naar aanleiding van de melding werden gevoerd. Ook kunnen de bevoegde autoriteiten van mening zijn dat de gemelde inbreuk duidelijk van geringe betekenis is en dat dus geen verdere opvolging is vereist. De bevoegde autoriteit moet die beslissing echter motiveren.

4.3. Openbaarmaking

Naast de mogelijkheden van interne en/of externe melding moet worden vermeld dat ook kan worden gekozen voor openbaarmaking in de pers of andere openbare media.

De volgende voorwaarden moeten echter in overweging worden genomen:

- De melder heeft eerst een interne en externe melding gedaan of heeft rechtstreeks een externe melding gedaan waarvoor binnen de termijn geen passende maatregelen zijn genomen;
of
- De melder heeft gegronde redenen om aan te nemen dat:
 - de inbreuk een onmiddellijk of reëel gevaar voor het algemeen belang kan vormen, bijvoorbeeld als er sprake is van een noodsituatie of van een risico van onherstelbare schade;
 - er een risico van vergelding is voor externe melding of het onwaarschijnlijk is dat de inbreuk effectief zal worden verholpen, wegens de bijzondere omstandigheden van de zaak (bijvoorbeeld wanneer er een autoriteit bij betrokken is).

5. BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

Het melden gebeurt met respect voor de wetgeving inzake de bescherming van de persoonlijke levenssfeer, met inbegrip van de Algemene Verordening Gegevensbescherming (AVG) en Bijlage 2 betreffende de verwerking van persoonsgegevens in het kader van een interne melding.

Contassur en CBA worden beschouwd als verwerkingsverantwoordelijken voor de persoonsgegevens die worden verwerkt in het kader van de meldingsprocedure.

Persoonsgegevens die duidelijk niet relevant zijn voor de behandeling van een specifieke melding worden niet verzameld of, indien ze per ongeluk worden verzameld, zonder onredelijke vertraging gewist.

De naam, functie en contactgegevens van de melder, alsook van elke persoon op wie de beschermings- en ondersteuningsmaatregelen van toepassing zijn, evenals van de betrokken persoon, met inbegrip van diens ondernemingsnummer indien van toepassing, worden bewaard tot het moment waarop de gemelde inbreuk is verjaard.

6. BESCHERMING

De persoon die te goeder trouw een melding doet, kan gegevens verschaffen die normaal als vertrouwelijk beschouwd worden (behalve in de gevallen die specifiek zijn voorzien in de wet van 28 november 2022). Hij of zij kan in geen geval aansprakelijk gesteld worden voor de bekendmaking van deze gegevens.

De onderneming garandeert dat melders die te goeder trouw handelen, worden beschermd tegen elke rechtstreekse of onrechtstreekse tuchtmaatregel of beslissing van gelijke strekking, zelfs indien de gemelde feiten uiteindelijk ongegrond wordt bevonden.

In het bijzonder mogen zij niet het slachtoffer worden van maatregelen/represailles zoals:

- schorsing, tijdelijke buitendienststelling, ontslag of soortgelijke maatregelen;
- degradatie of weigering van bevordering;
- overdracht van taken, verandering van locatie van de arbeidsplaats, loonsverlaging, verandering van de werktijden;
- schorsing van opleidingen;
- negatieve prestatiebeoordeling of arbeidsreferentie;
- het opleggen of toepassen van een tuchtmaatregel, berisping of andere sanctie, zoals een geldboete;
- dwang, intimidatie, pesterijen of uitsluiting;
- discriminatie, nadelige of ongelijke behandeling;
- niet-omzetting van een tijdelijke arbeidsovereenkomst in een arbeidsovereenkomst voor onbepaalde tijd, in het geval de werknemer redelijkerwijs mocht verwachten 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 omzet- en inkomensverlies;
- plaatsing op een zwarte lijst op basis van een informele of formele overeenkomst voor een hele sector of bedrijfstak, waardoor de betrokkene geen baan meer kan vinden in de sector of de bedrijfstak;
- vroegtijdige beëindiging of beëindiging van een overeenkomst voor de levering van goederen of diensten;
- intrekking van een licentie of vergunning;
- openbaar maken van psychiatrische of medische gegevens.

Melders genieten bescherming tegen mogelijke represailles op voorwaarde dat:

- zij gegronde redenen hadden om aan te nemen dat de gemelde informatie over inbreuken op het moment van de melding juist was; en
- de verstrekte informatie binnen het toepassingsgebied van dit beleid valt;
- zij een interne of externe melding of openbaarmaking hebben gedaan via de in dit beleid vermelde middelen.

Anonieme melders zijn onder bovengenoemde voorwaarden ook beschermd als zij later worden geïdentificeerd en slachtoffer worden van represailles.

Elke beschermde persoon (melder, facilitator, derden of juridische entiteiten die verbonden zijn met de melder) die meent slachtoffer te zijn van of bedreigd te worden met een represaille, kan een gemotiveerde klacht indienen bij de federale coördinator, die een buitengerechtelijke beschermingsprocedure opstart.

Die mogelijkheid doet geen afbreuk aan het recht van de beschermde persoon om zich rechtstreeks tot de hoven en rechtbanken te wenden.

7. SANCTIES

Binnen de grenzen van de wet van 28/11/2022 kunnen natuurlijke rechtspersonen of rechtspersonen die een aangifte verhinderen of trachten te verhinderen of die vergeldingsmaatregelen nemen, die onnodige gerechtelijke of buitengerechtelijke procedures zouden instellen of die de zwijgplicht zouden schenden, worden bestraft in overeenstemming met het Sociaal Strafwetboek. Dit geldt echter niet wanneer de bevoegde autoriteiten uit hoofde van specifieke wettelijke of bestuursrechtelijke bepalingen sancties of administratieve maatregelen opleggen wegens inbreuken op hoofdstuk 3 en artikel 22 van bovengenoemde wet.

Melders worden er echter op gewezen dat zij geen uitdrukkelijke bescherming genieten indien zij bewust valse informatie hebben meegedeeld of bekendgemaakt. In dat geval zullen zij ook de slachtoffers van de daaruit voortvloeiende schade moeten vergoeden.

8. OPENBAARHEID VAN DIT BELEID

Dit beleid wordt meegedeeld aan de leden van de operationele organen, aan de personeelsleden van Contassur en CBA en aan de controlefuncties via een beveiligde toegang tot een SharePoint.

Het wordt ook meegedeeld aan de onderaannemers van Contassur en CBA. Die onderaannemers moeten zich ertoe verbinden dit beleid mee te delen aan al hun personeelsleden die voor de bovenstaande ondernemingen werken.

Ze is beschikbaar op de website www.contassur.eu.

BIJLAGE 1 – CONTACTGEGEVENS VAN DE VOORZITTER VAN DE RAAD VAN BESTUUR

Contassur N.V.

Mevrouw Mireille Van Staeyen

Simon Bolivarlaan nr. 36, 1000 Brussel

Mireille.vanstaeyen@engie.com

+32 476 33 54 84

Contassur Bijstand Advies N.V.

Mevrouw Inès Horwart

Kunstlaan nr. 47, 1000 Brussel

ines.horwart@contassur.com

+32 476 33 04 22

BIJLAGE 2 – VERWERKING VAN PERSOONSGEGEVENS IN HET KADER VAN EEN INTERNE MELDING

Deze bijlage legt uit hoe de persoonsgegevens worden verwerkt van de melder, van een persoon over wie een melding wordt gedaan, of van elke andere derde die in dit kader wordt genoemd. Deze bijlage moet worden gelezen in aanvulling op de privacyverklaring ('privacy notice') van de organisatie.

Wat betreft de melder (artikel 13 van de AVG)		
Doeleinden	De gegevens die aan de onderneming worden doorgegeven, worden gebruikt om een ontvangstbevestiging van de melding naar de melder te sturen, in principe binnen 7 dagen na ontvangst van de melding. De gegevens worden ook verwerkt om de opvolging van de melding te waarborgen, dat wil zeggen: alle maatregelen die worden genomen door de Meldingsbeheerder en het onderzoeksteam, of door een bevoegde autoriteit, om de juistheid van de in de melding geformuleerde beweringen te beoordelen en, indien van toepassing, om de gemelde inbreuk te verhelpen.	
Rechtsgrondslagen	De melder heeft toestemming gegeven voor de verwerking van deze gegevens (artikel 6.1.a AVG). De verwerking van de gegevens is noodzakelijk om de onderneming in staat te stellen te voldoen aan een wettelijke verplichting waaraan zij onderworpen is (de wet van 28 november 2022 betreffende de bescherming van personen die inbreuken op het Unierecht of nationaal recht melden binnen een juridische entiteit uit de privésector) (artikel 6.1.c AVG).	
Gegevenscategorïeën	Het kan gaan om identificatiegegevens (naam), contactgegevens, beroepsgegevens (functie, relatie met de onderneming), informatie over de overtreding (al dan niet strafbaar) en informatie over sancties.	
Duur	Wanneer de melding leidt tot een bewezen overtreding.	Totdat de gemelde inbreuk is verjaard, met inbegrip van tot het einde van de verjaringstermijn voor het instellen van rechtsmiddelen tegen een gerechtelijke, administratieve of andere beslissing. In geval van een strafprocedure: 5jaar voor wanbedrijven; In geval van een vordering op grond van burgerlijke aansprakelijkheid: 5 jaar; In geval van een vordering op grond van contractuele aansprakelijkheid: 10 jaar.
	Wanneer er geen daadwerkelijke inbreuk wordt vastgesteld naar aanleiding van de melding.	Vernietiging of anonimiseren van de gegevens binnen een termijn van 2 maanden vanaf de afsluiting van het onderzoek (d.w.z. vanaf het moment waarop de raad van bestuur zich daarover heeft uitgesproken), behalve de gegevens die nodig zijn om te voldoen aan de verplichting om de meldingen te bewaren gedurende de volledige duur van de arbeidsrelatie met de melder.
Ontvangers	De mededeling van de gegevens van de melder is noodzakelijk voor de personen die door de onderneming gemachtigd en aangewezen zijn en bevoegd zijn om meldingen te ontvangen of op te volgen, evenals, indien van toepassing, voor 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 derden die in de melding worden genoemd, in de gevallen voorzien door de wetgeving inzake melders.	

Wat betreft de persoon die het onderwerp is van de melding of een andere derde die in dit verband wordt genoemd (artikel 14 van de AVG)		
Doeleinden	De aan het bedrijf verstrekte gegevens met betrekking tot de persoon die het onderwerp is van de melding, of een andere derde die in dit verband wordt genoemd, worden gebruikt om te verifiëren of er een overtreding is begaan door de persoon die het onderwerp is van de melding.	
Rechtsgrondslagen	De facilitators en derden die in verband staan met de melders en die het risico lopen om in een professionele context te worden blootgesteld aan represailles, hebben toestemming gegeven voor de verwerking van hun gegevens (artikel 6.1.a van de AVG). De verwerking van de gegevens is noodzakelijk om het bedrijf in staat te stellen te voldoen aan een wettelijke verplichting waaraan het onderworpen is (de wet van 28 november 2022 betreffende de bescherming van personen die inbreuken op het Unierecht of nationaal recht melden die zijn vastgesteld binnen een juridische entiteit in de privésector) (artikel 6.1.c van de AVG).	
Gegevenscategorieën	In de fase waarin de melding wordt gedaan	De verzamelde en verwerkte gegevens zijn die welke het mogelijk maken om de persoon die het onderwerp is van de melding, of een andere derde die in dit verband wordt genoemd, te identificeren. Het kan gaan om identificatiegegevens (zoals hun naam), contactgegevens, professionele gegevens (zoals hun functie en relatie tot het bedrijf), informatie over de inbreuk (ongeacht of het om strafbare feiten gaat), en informatie over eventuele sancties.
	In de fase van de behandeling van de melding	In het geval dat er een onderzoek wordt geopend met als doel de door de melder geuite beschuldigingen te verifiëren, kunnen alle noodzakelijke gegevens die verband houden met het onderzoek en met het nemen van passende maatregelen om de inbreuk te verhelpen worden verzameld, waaronder verslagen van verificatiehandelingen, de opvolging van de melding en de meldingsbrieven.
Duur	Wanneer de melding leidt tot een bevestigde inbreuk	Tot het moment waarop de gemelde inbreuk verjaard is, met inbegrip van het verstrijken van de termijn voor het instellen van rechtsmiddelen tegen een gerechtelijke, administratieve of andere beslissing. In geval van een strafprocedure: 5 jaar voor misdrijven. In geval van een vordering op basis van burgerlijke aansprakelijkheid: 5 jaar. In geval van een vordering op basis van contractuele aansprakelijkheid: 10 jaar.
	Wanneer er geen daadwerkelijke inbreuk wordt vastgesteld naar aanleiding van de melding	Vernietiging of anonimiseren van de gegevens binnen een termijn van 2 maanden vanaf de afsluiting van het onderzoek (dat wil zeggen vanaf het moment waarop de Raad van Bestuur zich hierover heeft uitgesproken), met uitzondering van de gegevens die nodig zijn om te voldoen aan de verplichting om meldingen te bewaren gedurende de volledige duur van de arbeidsrelatie met de melder.
Ontvangers	De communicatie van de gegevens is noodzakelijk voor de personen die door het bedrijf gemachtigd en aangewezen zijn en bevoegd zijn om meldingen te ontvangen of op te volgen, evenals, indien van toepassing, voor de bevoegde autoriteiten. Deze gegevens zullen ook, geheel of gedeeltelijk, worden meegedeeld aan de melder in het kader van terugkoppeling en opvolging van de procedure, mits deze communicatie de vertrouwelijkheid van de persoon die het onderwerp is van de melding niet in gevaar brengt, of behoudens wettelijke uitzonderingen.	