

**BELEID INZAKE KLACHTEN EN BESCHERMING VAN
KLOKKENLUIDERS
("MELDINGSBELEID")**

- CCB -

December 2025

1. INLEIDING

"CCB" verwijst naar: La COMPAGNIE DES CIMENTS BELGES (hierna "CCB" genoemd), geregistreerd bij de Kruispuntbank van Ondernemingen onder nummer 0419.445.816 en met maatschappelijke zetel te 260 Grand'Route, 7530 Doornik.

Dit beleid inzake klokkenluiders en de bescherming van klokkenluiders (hierna "het meldingsbeleid" genoemd) vormt een aanvulling op het arbeidsreglement van CCB. In geval van tegenstrijdigheid tussen dit beleid en het arbeidsreglement prevaleert het arbeidsreglement.

Dit meldingsbeleid heeft tot doel informatie te verstrekken over de beschikbare meldingskanalen en over de bescherming die klokkenluiders wordt geboden, in overeenstemming met Richtlijn 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 en de Belgische wet van 28 november 2022 betreffende de bescherming van personen die schendingen van het recht van de Unie of het nationale recht binnen een juridische entiteit van de privésector melden.

Wanneer iemand een wet of een intern beleid overtreedt, brengt hij CCB, haar werknemers en andere belanghebbenden in gevaar.

Hoe eerder een dergelijke laakbare handeling wordt gestopt, hoe beter het is voor alle betrokken partijen. Daarom heeft CCB dit meldingsbeleid opgesteld, met als doelstellingen:

- **Een veilig alternatief bieden** voor de traditionele interne communicatiekanalen, zodat werknemers, managers, leveranciers, agenten, vertegenwoordigers, distributeurs of klanten ernstige of gevoelige kwesties kunnen melden. Deze meldingen kunnen betrekking hebben op schendingen van de ethiek of van toepasselijke wetgeving.
- **Fungeren als een vroegtijdig waarschuwingssysteem**, waardoor het algemeen management van CCB zo snel mogelijk op de hoogte wordt gebracht van deze problemen, om (i) ze te beoordelen en te onderzoeken, en (ii) indien nodig passende maatregelen te nemen om de gevolgen van een overtreding, een gevaar of een ander ernstig risico te beperken.

Om elke dubbelzinnigheid te vermijden, moeten meldingen in het kader van dit meldingsbeleid op vrijwillige basis gebeuren.

Iedereen die in een professionele context kennis heeft van een situatie die in strijd is of lijkt te zijn met de wet- en regelgeving, kan dit dus in alle veiligheid melden. CCB verbindt zich ertoe de vertrouwelijkheid van de meldingen te waarborgen en klokkenluiders te beschermen tegen elke vorm van vergelding of discriminatie.

2. TOEPASSINGSGEBIED VAN DE MELDING

2.1. PERSOON DIE DE MELDING HEEFT GEDAAN

De persoon die het initiatief neemt tot de melding is de 'klokkenluider', d.w.z. elke persoon die - **in een professionele context** - informatie heeft verkregen over (daadwerkelijke of potentiële) schendingen, waarvan hij/zij redelijke gronden heeft om aan te nemen dat deze waarheidsgetrouw zijn, en die hiervan melding maakt.

De volgende personen hebben dus de mogelijkheid om een melding te doen:

- Huidige of voormalige werknemers;
- Zelfstandigen;
- Aandeelhouders;
- Leden van het bestuurs-, leidinggevend of toezichthoudend orgaan;
- Leveranciers;
- Onderaannemers;
- Leveranciers;
- Klanten;
- Sollicitanten;
- Stagiaires;
- Vrijwilligers.

Bij wijze van uitzondering is deze procedure ook van toepassing op personen die – **buiten een professionele context** – een overtreding melden op het gebied van financiële diensten, producten en markten, alsook op het gebied van de bestrijding van het witwassen van geld.

2.2. DOEL VAN DE MELDING

De klokkenluider kan een melding doen over:

- **Geconstateerde schendingen;**
- **Redelijke vermoedens** van daadwerkelijke of potentiële overtredingen die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden;
- **Pogingen om deze schendingen te verbergen.**

De meldingen moeten betrekking hebben op overtredingen van wetten en voorschriften op de volgende gebieden:

- Overheidsopdrachten;
- Diensten, producten en financiële markten, preventie van witwassen en financiering van terrorisme;
- Productveiligheid en -conformiteit;
- Vervoersveiligheid;

- Milieubescherming;
- Stralingsbescherming en nucleaire veiligheid;
- Voedselveiligheid, gezondheid en welzijn van dieren;
- Volksgezondheid;
- Consumentenbescherming;
- Bescherming van de persoonlijke levenssfeer en persoonsgegevens, veiligheid van netwerken en informatiesystemen;
- Bestrijding van fiscale en sociale fraude.
- Fraude (financiële fraude, documentfraude, verduistering van gelden);
- Ernstige tekortkomingen of opzettelijke fouten in financiële verslagen of interne controles;
- Schendingen van het mededingingsrecht (prijsafspraken, illegale kartels);
- Schending van de mensenrechten;
- Corruptie of omkoping;
- Ernstige overtredingen op het gebied van veiligheid, milieu of discriminatie.

Specifieke voorbeelden:

1. **Productveiligheid:** distributie van producten die niet aan de wettelijke normen voldoen.
2. **Vervoersveiligheid:** niet-naleving van de verplichte rijtijden door dienstverleners.
3. **Gegevensbescherming:**
 - Illegale doorgifte van persoonsgegevens aan derden;
 - Niet-naleving van de regels inzake cyberveiligheid.
4. **Concurrentie:** deelname aan illegale prijsafspraken.
5. **Financiële overtredingen:** fraude, witwassen van geld, financiering van terrorisme, corruptie, verduistering.
6. **Discriminatie en intimidatie:** seksuele intimidatie of andere ernstige vormen van intimidatie.
7. **Overheidsopdrachten:** vriendjespolitiek of illegale contacten met ambtenaren.

Bij twijfel over de toepassing van dit beleid of over de kwalificatie van een handeling als overtreding, wordt de klokkenluider aangemoedigd om aanvullende informatie te vragen aan zijn leidinggevende of aan de juridische dienst van CCB.

2.3. UITSLUITINGEN VAN HET HUIDIGE BELEID

Het meldingsbeleid is uitsluitend bedoeld voor het melden van (vermoedelijk of bewezen) misbruik of onregelmatigheden die binnen het toepassingsgebied van dit beleid vallen.

Voor alle andere kwesties wordt aanbevolen om de juiste interne procedures te volgen of contact op te nemen met de betreffende afdelingen. Dit beleid vervangt niet de bestaande interne communicatiekanalen binnen CCB, maar vult deze aan door een extra mogelijkheid te bieden om in alle vertrouwen en zonder angst voor represailles meldingen te doen.

Het meldingsbeleid is niet bedoeld voor:

- **Gewone klachten over CCB:** voor deze gevallen kunt u gebruikmaken van de interne klachtenprocedure.
- **Klachten met betrekking tot klanten of leveranciers van CCB:** Deze klachten moeten worden behandeld via de daarvoor bestemde interne processen.
- **Persoonlijke klachten van werknemers:** het beheer of de melding van individuele klachten valt niet onder het meldingsbeleid.

Hoewel het meldingsbeleid bedoeld is om een veilig kader te bieden voor het melden van ernstige overtredingen of onregelmatigheden, vallen bepaalde soorten meldingen buiten het toepassingsgebied ervan.

Deze uitsluitingen zijn:

1. Situaties van onmiddellijke noodzaak

Meldingen die betrekking hebben op een onmiddellijke bedreiging voor het leven, de gezondheid, de veiligheid van personen of eigendommen vallen niet onder dit beleid. In geval van nood wordt de klokkenluider verzocht onmiddellijk contact op te nemen met de bevoegde lokale autoriteiten of het lokale noodnummer te bellen.

2. Klachten over arbeidsvoorwaarden

Eventuele klachten van de klokkenluider over zijn arbeidsvoorwaarden (bijvoorbeeld salaris, werktijden, vakantie) vallen niet onder dit beleid. Deze kwesties moeten worden behandeld via de bestaande interne kanalen, zoals Human Resources.

3. Persoonlijke geschillen die geen verband houden met een overtreding

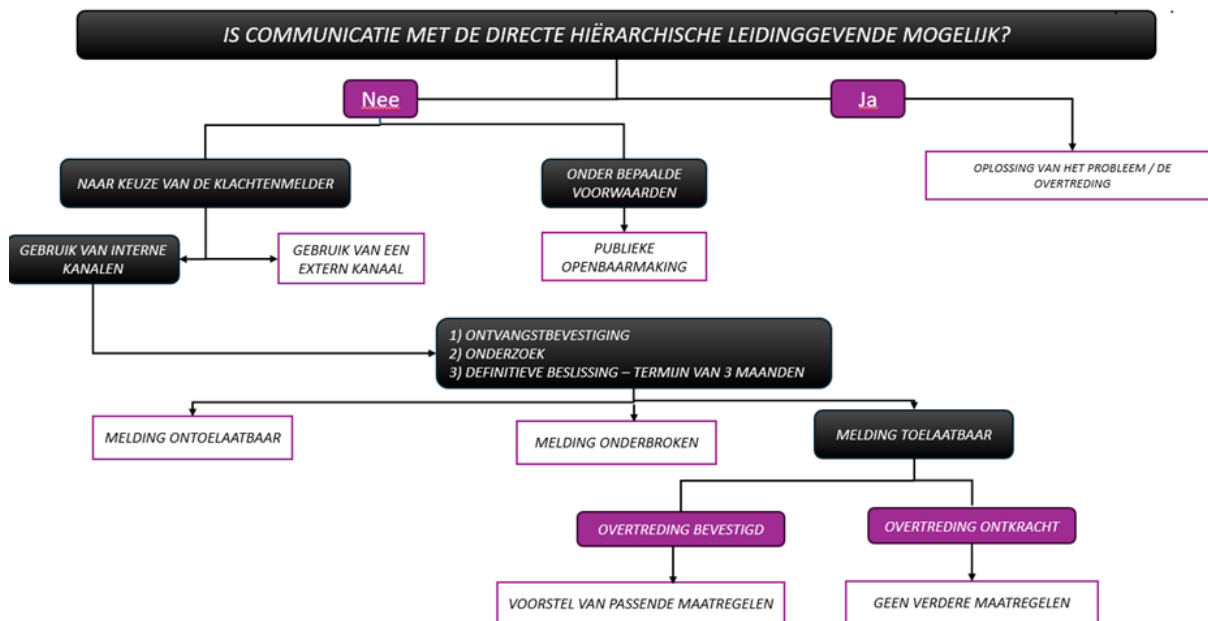
Persoonlijke geschillen of geschillen tussen collega's vallen niet onder dit beleid, tenzij ze een schending van het toepassingsgebied van dit beleid inhouden.

3. MELDINGSKANALEN

De klokkenluider kan zijn melding doen via:

- Interne meldingskanalen, waarvoor CCB verantwoordelijk is;
- Externe meldingskanalen;
- Openbare bekendmaking.

3.1. TOTAALOVERZICHT



3.2. INTERNE MELDKANALEN

Alvorens een melding te doen in overeenstemming met deze procedure, wordt de klokkenluider aangemoedigd om eerst te communiceren met zijn directe leidinggevende of hiërarchische meerdere.

Als de klokkenluider om welke reden dan ook van mening is dat hij zich niet tot zijn directe leidinggevende kan wenden of dat het antwoord niet als bevredigend kan worden beschouwd, kan hij gebruikmaken van de interne meldingskanalen.

a) Werking van de interne meldingskanalen

Als de klokkenluider een schending van een van de bovengenoemde gebieden ontdekt, er kennis van neemt of redelijke gronden heeft om een schending te vermoeden, kan hij/zij CCB hiervan op de hoogte brengen via de door haar aangewezen meldingsbeheerder, waarvan de contactgegevens hieronder zijn vermeld.

Elke melding moet gedetailleerd en gedocumenteerd zijn en de volgende informatie bevatten – voor zover bekend – zodat de meldingsbeheerder de geldigheid van de gemelde schendingen kan controleren:

- Een gedetailleerde beschrijving van de gebeurtenissen die aanleiding hebben gegeven tot de schending en de manier waarop de klokkenluider hiervan op de hoogte is gekomen;
- De datum en plaats van de gebeurtenis/gebeurtenissen;
- De namen en functies van de personen die het voorwerp van de melding uitmaken of informatie waarmee zij kunnen worden geïdentificeerd;
- De namen en functies van andere personen die de gemelde feiten kunnen bevestigen;
- Alle andere informatie die de meldingsbeheerder kan helpen om de feiten te verifiëren.

De klokkenluider kan overtredingen melden in overeenstemming met de GROUP WHISTLEBLOWING MANAGEMENT PROCEDURE via het meldingssysteem van de Cementir Holding Groep:

Het Cementir-platform vormt een aanvulling op de lokale voorzieningen en voldoet aan de Belgische wetgeving inzake de bescherming van klokkenluiders, waardoor vertrouwelijkheid, onafhankelijkheid en een passende opvolging worden gewaarborgd.

Meldingen van overtredingen of verdacht gedrag kunnen ook worden gedaan via het professionele meldingsplatform van de Cementir Holding Groep, dat toegankelijk is op het volgende adres: <https://cementir.integrityline.com>.

Via dit beveiligde platform kunnen zorgen vertrouwelijk en, indien gewenst, anoniem worden gemeld. Het biedt nuttige informatie over:

- Wat er kan worden gemeld;
- Het gegarandeerde niveau van anonimiteit;
- Het gebruik van beveiligde berichten om een follow-up te garanderen;
- Het beleid dat van toepassing is op professionele meldingen;
- De wettelijke rechten en mogelijkheden om meldingen te doen bij externe autoriteiten in de Europese Unie.

Alle meldingen via dit kanaal zijn strikt vertrouwelijk en worden behandeld in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming en klokkenluiders.

E-mail: Whistleblowing@cementirholding.it of ethicscommittee@cementirgroup.com

Post: Cementir Holding Internal Audit Department, Corso di Francia 200, 00191 Rome, Italië

b) Behandeling van de melding

De meldingsbeheerder bevestigt de ontvangst van de melding binnen 7 dagen via hetzelfde communicatiemiddel.

De meldingsbeheerder stelt vervolgens snel en zorgvuldig een onderzoek in, in samenwerking met de betrokken interne diensten. De meldingsbeheerder controleert de geldigheid van de gemelde feiten, met inachtneming van de beginselen van onpartijdigheid, billijkheid en vertrouwelijkheid. Dit laatste beginsel geldt voor alle personen die bij de melding betrokken zijn, om onnodige schade aan hun reputatie te voorkomen. Bijgevolg moet iedereen die aan een onderzoek deelneemt of kennis neemt van het bestaan van een dergelijk onderzoek, de vertrouwelijkheid ervan bewaren.

De meldingsbeheerder kan ook besluiten om andere functies, zowel intern als extern bij CCB, bij het onderzoek te betrekken indien hij dit nodig acht.

Indien de melding betrekking heeft op de meldingsbeheerder zelf, wordt de klokkenluider verzocht zich rechtstreeks te wenden tot de voorzitter van de raad van bestuur van CCB, de heer Eddy Fostier, via e-mail eddy.fostier@ccb.be.

c) Resultaat van de melding en definitieve beslissing

Na het onderzoek door de meldingsbeheerder kan deze de volgende beslissingen nemen:

- 1) De melding wordt als onontvankelijk beschouwd omdat deze niet onder het toepassingsgebied van dit beleid valt;
- 2) De opvolging van de melding wordt stopgezet:
 - Omdat het niet voldoende verifieerbare bewijzen bevat om een grondiger onderzoek mogelijk te maken, waardoor een aanvullend onderzoek noodzakelijk is;
 - Omdat dezelfde feiten al eerder zijn gemeld en onderzocht;
- 3) De melding wordt als ontvankelijk beschouwd, maar de gemelde schending wordt niet bevestigd door het onderzoek: in dit geval zal CCB geen verdere maatregelen nemen.
- 4) De melding wordt als ontvankelijk en geldig beschouwd; er worden daarom passende maatregelen voorgesteld aan CCB om een einde te maken aan de gemelde schending.

De meldingsbeheerder deelt zijn definitieve beslissing binnen drie maanden na ontvangstbevestiging van de melding mee aan de klokkenluider.

d) Samenwerking en goede trouw

De klokkenluider doet zijn melding te goeder trouw en brengt geen beschuldigingen naar voren waarvan hij weet dat ze onjuist zijn. Alle andere personen die bij een onderzoek betrokken zijn, moeten eveneens te goeder trouw meewerken en de vragen van de meldingsbeheerder beantwoorden. Liegen, vertragen, belemmeren of weigeren mee te werken aan een onderzoek kan aanleiding geven tot disciplinaire maatregelen.

In alle gevallen staat CCB geen enkele vorm van vergelding, bedreiging, straf of discriminatie toe tegen de klokkenluider of tegen personen die te goeder trouw aan het onderzoek hebben meegewerkt.

Als een melding echter valse, ongegronde of opportunistische beschuldigingen bevat, of als deze uitsluitend is gedaan om anderen in diskrediet te brengen of schade te berokkenen, kan de klokkenluider te kwader trouw worden gestraft met een gevangenisstraf van maximaal één jaar en/of een boete van € 8000, evenals disciplinaire maatregelen.

3.3. EXTERN MELDKANAAL

Wij raden de klokkenluider ten eerste aan om in eerste instantie gebruik te maken van het interne meldingskanaal. CCB heeft namelijk deze procedure en de nodige middelen

geïmplementeerd om meldingen op adequate wijze te behandelen, waardoor het gebruik ervan doeltreffend is.

De klokkenluider heeft echter de mogelijkheid om een externe melding te doen door zich rechtstreeks tot een van de bevoegde autoriteiten te wenden als hij van mening is dat zijn melding niet tot een bevredigend resultaat heeft geleid. De regels voor externe meldingen en de bevoegde autoriteit variëren naargelang het domein van de gemelde inbreuk (zie bijlage 1).

3.4. OPENBAARMAKING

De klokkenluider heeft ook de mogelijkheid om zijn melding openbaar te maken, met name door de pers te informeren of door deze online te publiceren.

Een klokkenluider die zijn melding openbaar maakt, geniet echter alleen bescherming onder twee voorwaarden:

- De klokkenluider heeft zijn probleem gemeld bij de bevoegde autoriteit, maar er zijn (objectief gezien) geen passende vervolgmaatregelen genomen; en
- De klokkenluider heeft redelijke gronden om aan te nemen dat de gemelde feiten een onmiddellijk of duidelijk gevaar voor het algemeen belang kunnen vormen, met name in geval van noodsituaties of het risico van onomkeerbare schade. Dit kan bijvoorbeeld het geval zijn wanneer de klokkenluider van mening is dat het risico bestaat dat het bewijs van de schending wordt verborgen of vernietigd.

4. RECHTEN VAN DE KLOKKENLUIDER

4.1. VERTROUWELIJKHEID

De klokkenluider heeft recht op vertrouwelijkheid. Zijn identiteit en de details van zijn melding blijven dus vertrouwelijk tijdens en na het onderzoek.

De identiteit van de klokkenluider wordt echter bekendgemaakt in de volgende gevallen:

- de klokkenluider daarmee heeft ingestemd; of
- Deze bekendmaking wettelijk verplicht is, bijvoorbeeld in het kader van onderzoeken door nationale autoriteiten of in het kader van gerechtelijke procedures. In dat geval is CCB verplicht de klokkenluider hiervan op de hoogte te stellen, tenzij dit het onderzoek of de procedure in gevaar zou brengen (bijvoorbeeld als er een risico bestaat dat bewijsmateriaal wordt vernietigd).

Ongeoorloofde openbaarmaking van bovengenoemde informatie wordt door CCB niet getolereerd en leidt tot disciplinaire maatregelen, of zelfs tot ontslag van de persoon die de informatie in kwestie openbaar heeft gemaakt. Afhankelijk van de omstandigheden kan ongeoorloofde openbaarmaking ook aanleiding geven tot civiele of strafrechtelijke vervolging.

4.2. BESCHERMING TEGEN REPRESSAILES

De klokkenluider geniet bescherming tegen represailles als aan de volgende voorwaarden is voldaan:

- De klokkenluider heeft redelijke gronden om aan te nemen dat de gemelde informatie op het moment van de melding waarheidsgetrouw was.
- De klokkenluider heeft de procedure gevolgd zoals hierin beschreven.

Als de informatie echter onjuist blijkt te zijn, maar de klokkenluider deze te goeder trouw heeft doorgegeven, geniet hij toch bescherming.

Deze bescherming houdt in dat CCB geen vergeldingsmaatregelen tegen de klokkenluider mag nemen (zie bijlage 2).

Bijgevolg kan elke persoon die bij CCB werkt en acties onderneemt die als vergeldingsmaatregelen kunnen worden beschouwd, of die andere werknemers aanmoedigt om tegen de klokkenluider, kan worden onderworpen aan sancties of gerechtelijke vervolging (met inbegrip van disciplinaire maatregelen, ontslag, strafrechtelijke vervolging, enz.).

4.3. RECHTSMIDDELEN

Indien de klokkenluider ondanks de toepassing van deze procedure het slachtoffer wordt van represailles, kan hij ook bepaalde rechtsmiddelen aanwenden.

Als de klokkenluider bijvoorbeeld is ontslagen, zou de passende rechtsmiddel tegen deze maatregel zijn herplaatsing in zijn functie zijn. Een passend rechtsmiddel kan ook de herstel van een vergunning of contract zijn, indien deze zijn ingetrokken als gevolg van de melding door de klokkenluider.

4.4. ONDERSTEUNENDE MAATREGELEN

Daarnaast kan de klokkenluider een beroep doen op ondersteunende maatregelen, waaronder:

- Uitgebreide en onafhankelijke informatie en advies;
- Technisch advies aan de autoriteiten;
- Juridische bijstand in overeenstemming met de Europese regels in het kader van grensoverschrijdende strafrechtelijke en civielrechtelijke procedures;
- Ondersteunende maatregelen (op technisch, psychologisch, media- en sociaal vlak);
- Financiële bijstand in het kader van gerechtelijke procedures.

4.5. UITBREIDING VAN DE BESCHERMING VAN KLOKKENLUIDERS

De bescherming die aan klokkenluiders wordt geboden, wordt ook uitgebreid tot de volgende personen:

- De "*facilitators*", d.w.z. natuurlijke personen die de klokkenluider helpen tijdens het meldingsproces en wier hulp vertrouwelijk moet blijven;
- Derden die banden hebben met klokkenluiders en die het risico lopen op represailles in een professionele context, zoals collega's of familieleden van klokkenluiders;
- Rechtspersonen die eigendom zijn van klokkenluiders of waarvoor zij werken, of waarmee zij in een professionele context verbonden zijn.

5. RECHTEN VAN DE PERSOON DIE HET VOORWERP IS VAN DE MELDING

Elke persoon die het voorwerp uitmaakt van een melding wordt door de meldingsbeheerder op de hoogte gebracht dat er een melding tegen hem of haar is gedaan, zodat hij of zij daarop kan reageren.

Deze informatie wordt zo snel mogelijk verstrekt, tenzij er redelijke gronden zijn om aan te nemen dat de persoon op wie de melding betrekking heeft, in staat is om de informatie te vernietigen, bestanden te manipuleren of het onderzoek op enigerlei wijze in gevaar te brengen of te compromitteren. In dat geval zal deze persoon niet of pas later worden geïnformeerd.

De betrokkene heeft de mogelijkheid om contact op te nemen met de meldingsbeheerder om zijn recht op toegang tot de hem betreffende informatie uit te oefenen, in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming ("**AVG**").

De volgende beperkingen zijn echter van toepassing:

- De persoon die het voorwerp uitmaakt van de melding mag alleen worden geïnformeerd over de feiten die hem of haar betreffen;
- De persoon op wie de melding betrekking heeft, wordt niet geïnformeerd over de identiteit van de klokkenluider;
- De rechten van de persoon die het voorwerp uitmaakt van de melding zijn beperkt tot de gegevens die op hem betrekking hebben.

Overduidelijk onredelijke verzoeken van de persoon op wie de melding betrekking heeft, kunnen ook worden geweigerd, bijvoorbeeld in geval van herhaalde verzoeken om toegang tot gegevens.

Indien mogelijk en passend, zal de meldingsbeheerder de persoon op wie de melding betrekking heeft, op de hoogte brengen van zijn definitieve beslissing.

6. VERWERKING VAN PERSOONSGEGEVENS

Alleen persoonsgegevens die strikt noodzakelijk zijn voor de verwerking en verificatie van de geldigheid van de melding worden verzameld en gebruikt, en dit uitsluitend in het kader van de procedures die in dit beleid worden beschreven door CCB, als verantwoordelijke voor de verwerking.

CCB verklaart dat alle persoonsgegevens van klokkenluiders en andere betrokken personen (met inbegrip van bijzondere categorieën van zogenaamde "gevoelige" gegevens) die in het kader van meldingen worden verkregen, zullen worden verwerkt in strikte overeenstemming met de bepalingen van de toepasselijke wetgeving inzake de bescherming van persoonsgegevens en met haar privacybeleid.

Categorieën van verwerkte persoonsgegevens

De persoonsgegevens die kunnen worden verzameld, omvatten:

1. Bij het indienen van een melding:
 - Standaard identificatiegegevens: naam, voornaam, bedrijf, functie, adres en

telefoonnummer (indien verstrekt);

- Informatie over de gemelde feiten;
- Informatie over de personen die in de melding worden genoemd of bij de behandeling ervan betrokken zijn.
- Alle persoonsgegevens die door de klokkenluider in zijn melding worden verstrekt;

2. Bij een onderzoek:

- Standaard identificatiegegevens van de betrokken personen;
- Gegevens die nodig zijn om de klacht te behandelen en de gemelde feiten te onderzoeken.
- Alle persoonsgegevens die tijdens de verschillende uitwisselingen in de loop van het onderzoek en in het onderzoeksrapport worden verstrekt.

3. Gegeneerde documentatie:

- Eerste melding, tijdens het onderzoek verzamelde informatie, onderzoeksrapport en conclusies.

Doeleinden en rechtsgrondslagen voor de verwerking van gegevens

De doeleinden van de verwerking van persoonsgegevens, met inbegrip van eventuele doorgiften binnen CCB, zijn de volgende:

- a. Het bevorderen van eerlijkheid, integriteit en ethiek binnen CCB;
- b. Melding mogelijk maken via het interne meldingssysteem van de onderneming;
- c. Klachten beheren en meldingen via het interne meldingssysteem behandelen;
- d. Bepalen of een onderzoek nodig is en dit onderzoek uitvoeren/organiseren;
- e. De resultaten van onderzoeken naar ontvangen meldingen analyseren;
- f. Bepalen welke corrigerende maatregelen moeten worden genomen naar aanleiding van een melding en/of een daarmee verband houdend onderzoek en de relevante maatregelen uitvoeren.

Wij verwerken persoonsgegevens om meldingen van klokkenluiders te behandelen en beschuldigingen te onderzoeken. De verwerking van uw persoonsgegevens is in dit verband noodzakelijk om te voldoen aan een wettelijke verplichting waaraan wij onderworpen zijn.

We kunnen persoonsgegevens aan de politie of gerechtelijke autoriteiten bekendmaken als bewijs als er redelijke gronden zijn om aan te nemen dat u in het kader van de meldingsprocedure een onwettige handeling of een misdrijf hebt gepleegd.

Bovendien zullen bepaalde specifieke categorieën persoonsgegevens alleen worden verwerkt

indien dit noodzakelijk is voor de vaststelling, uitoefening of verdediging van rechtsvorderingen, of zoals toegestaan door de toepasselijke wetgeving inzake gegevensbescherming.

Vermoedens van strafbare feiten worden alleen verwerkt voor zover dat nodig is voor het beheer van geschillen die specifiek zijn voor CCB of voor zover dat anderszins wettelijk is toegestaan.

In bepaalde omstandigheden kan CCB ook persoonsgegevens verwerken die via het meldingssysteem zijn verzameld, indien dit noodzakelijk is om te voldoen aan wettelijke verplichtingen waaraan CCB is onderworpen.

Er worden geen geautomatiseerde beslissingen genomen, met inbegrip van profilering.

De verzamelde persoonsgegevens worden niet gebruikt voor direct marketingdoeleinden.

Bewaring en verwijdering van gegevens

De verzamelde gegevens worden alleen bewaard gedurende de periode die nodig en proportioneel is, in overeenstemming met de wettelijke verplichtingen:

- Onmiddellijke verwijdering als de melding buiten het toepassingsgebied valt of ongegrond is.
- Verwijdering na afronding van het onderzoek of de ondernomen acties, tenzij wettelijk anders verplicht.
- Bewaring gedurende 10 jaar, overeenkomend met de wettelijke verjaringstermijn (artikel 2262bis van het oude Burgerlijk Wetboek).

Beveiliging en vertrouwelijkheid van gegevens

CCB en haar partners maken gebruik van passende technische en organisatorische maatregelen om de veiligheid van de gegevens te waarborgen, in overeenstemming met de AVG. De meldingskanalen zijn beveiligd en alleen toegankelijk voor bevoegde personen.

Rechten van de betrokkenen

In bepaalde rechtsgebieden, zoals de Europese Unie en de Europese Economische Ruimte, heeft een persoon wiens gegevens worden verwerkt (de "betrokkene") in overeenstemming met dit beleid verschillende rechten, die hieronder worden samengevat. Houd er rekening mee dat de uitoefening van deze rechten onderworpen is aan aanvullende vereisten en voorwaarden die zijn vastgelegd in de toepasselijke wetgeving inzake gegevensbescherming. Samengevat heeft elke persoon de volgende rechten:

- Bevestiging krijgen van CCB of de persoonsgegevens van de betrokkene worden verwerkt, en toegang vragen tot deze gegevens, de doeleinden van de verwerking en de betrokken ontvangers of categorieën van ontvangers.
- Van CCB de rectificatie verkrijgen van onjuiste of onvolledige persoonsgegevens betreffende de betrokkene.
- Van CCB verwijdering van de persoonsgegevens van de betrokkene te verkrijgen, wanneer dit wettelijk van toepassing is.

- CCB verzoeken om de verwerking van de persoonsgegevens van de betrokkene te beperken.
- De persoonsgegevens die de betrokkene aan CCB heeft verstrekt, ontvangen in een gestructureerd, gangbaar en machinaal leesbaar formaat.
- Zich verzetten tegen de verwerking van de persoonsgegevens van de betrokkene door CCB.

Als een betrokkene deze rechten wil uitoefenen of informatie over zijn gegevens wil verkrijgen, kan hij contact opnemen met de juridische dienst van CCB op het volgende adres: stephanie.heyman@ccb.be.

Personen die onder de Europese regelgeving inzake de bescherming van persoonsgegevens vallen en een klacht willen indienen over de hier beschreven verwerking, kunnen dit doen bij de bevoegde gegevensbeschermingsautoriteit, met name in de lidstaat waar zij hun gewone verblijfplaats hebben, waar zij werken of waar een vermeende inbreuk op de gegevensbeschermingsregelgeving heeft plaatsgevonden.

Voor meer informatie over de verwerking van gegevens en de rechten van personen verwijzen wij u naar de privacyverklaring van CCB.

7. CONTACTGEGEVENS VAN DE SIGNALEMENTENBEHEERDER

Voor vragen over dit beleid kunnen geïnteresseerden rechtstreeks contact opnemen met de meldingsbeheerder van CCB via de volgende contactgegevens:

Whistleblowing@cementirholding.it

8. UPDATE

Dit beleid zal worden bijgewerkt in geval van wijzigingen in de wetgeving.

BIJLAGE 1. LIJST VAN BEVOEGDE BELGISCHE AUTORITEITEN

In België worden informatie en ondersteuning aan klokkenluiders verstrekt via twee instanties:

- De *federale ombudsman*, die optreedt als federale coördinator voor externe meldingen. De ombudsman ontvangt externe meldingen, controleert of ze ontvankelijk zijn en stuurt de informatie door naar de bevoegde autoriteit. In uitzonderlijke gevallen onderzoekt de ombudsman ook de inhoud en behandelt hij beschermingszaken.
- *Het Federaal Instituut voor de bescherming en bevordering van de mensenrechten (IFDH)*, dat klokkenluiders professionele, juridische en psychologische ondersteuning biedt. Dit kan gebeuren via het Instituut zelf of via derden, zoals advocatenkantoren of psychologen die gespecialiseerd zijn in dit domein.

Naast deze twee instrumenten zijn er 24 bevoegde autoriteiten, afhankelijk van het domein waarop de gemelde schending betrekking heeft:

- | | | |
|---|---|---|
| ○ De Federale Overheidsdienst Economie, KMO's, Middenstand en Energie | ○ Het Federaal Agentschap voor Nucleaire Controle | ○ De autoriteiten bedoeld in artikel 85 van de wet van 18 september 2017 betreffende de preventie van het witwassen van geld en de financiering van terrorisme en de beperking van het gebruik van contant geld |
| ○ De Federale Overheidsdienst Financiën | ○ Het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten | ○ Het Nationaal Veiligheidscomité voor de levering en distributie van drinkwater |
| ○ De Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu | ○ Het Federaal Agentschap voor de Veiligheid van de Voedselketen | ○ Het Belgisch Instituut voor Postdiensten en Telecommunicatie |
| ○ De Federale Overheidsdienst Mobiliteit en Vervoer | ○ De Belgische Mededingingsautoriteit | ○ Het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering |
| ○ De Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg | ○ De Gegevensbeschermingsautoriteit | ○ Het Rijksinstituut voor Sociale Verzekeringen voor Zelfstandigen |
| ○ De Federale Overheidsdienst Programmering Sociale Integratie, Armoedebestrijding, Sociale Economie en Grootstedelijk Beleid | ○ De Autoriteit voor Financiële Diensten en Markten | ○ De Rijksdienst voor Arbeidsvoorziening |
| ○ De Rijksdienst voor Sociale Zekerheid | ○ De Nationale Bank van België | ○ De Autonome Dienst voor Fraudebestrijding (CAF) |
| | ○ Het College van Toezicht op de Bedrijfsrevisoren | |
| | ○ De Dienst voor Sociale Informatie en Onderzoek | |
| | ○ De Controle van de Scheepvaart | |

BIJLAGE 2. NIET-UITPUTTENDE LIJST VAN VERBODEN VORMEN VAN VERGELDING (ART. 23 WET VAN 28 NOVEMBER 2022)

Elke vorm van represailles tegen personen die onder de bescherming van klokkenluiders vallen, is verboden, met inbegrip van dreigingen met represailles en pogingen tot represailles, met name in de volgende vormen:

- Schorsing, ontslag of gelijkwaardige maatregelen;

- Degradatie of weigering van promotie;
- Overplaatsing, verandering van werkplek, salarisverlaging, wijziging van de werktijden;
- Opschorting van opleiding;
- Negatieve prestatiebeoordeling of negatieve arbeidsverklaring;
- Opgelegde of toegepaste disciplinaire maatregelen, berisping of andere sanctie, met inbegrip van een financiële sanctie;
- Dwang, intimidatie, pesterijen of uitsluiting;
- Discriminatie, benadeling of oneerlijke behandeling;
- Niet-omzetting van een tijdelijk arbeidscontract in een vast contract, terwijl de werknemer redelijkerwijs mocht verwachten dat hij een vaste baan zou krijgen;
- Niet-verlenging of voortijdige beëindiging van een tijdelijke arbeidsovereenkomst;
- Schade, met inbegrip van aantasting van de reputatie van de persoon, met name op sociale netwerken, of financiële verliezen, met inbegrip van verlies van activiteit en verlies van inkomen;
- Op een zwarte lijst worden geplaatst op basis van een formele of informele overeenkomst op sector- of branche-niveau, wat ertoe kan leiden dat de persoon in de toekomst geen werk meer kan vinden in de sector of branche;
- Vervroegde beëindiging of annulering van een contract voor de levering van goederen of diensten;
- Intrekking van een vergunning of licentie;
- Doorverwijzing naar een psychiatrische of medische behandeling.

**WHISTLEBLOWER POLICY AND PROTECTION OF
WHISTLEBLOWERS
(“WHISTLEBLOWER POLICY”)**

- CCB -

December 2025

1. INTRODUCTION

“CCB” refers to: COMPAGNIE DES CEMENTS BELGES (hereinafter “CCB”), registered with the Crossroads Bank for Enterprises under number 0419.445.816 and whose registered office is located at 260 Grand’Route, 7530 Tournai.

This reporting and whistleblower protection policy (hereinafter, the “Whistleblowing Policy”) supplements CCB’s Work Regulations. In the event of any conflict between this policy and the Work Regulations, the latter shall prevail.

This Whistleblowing Policy aims to provide information on the reporting channels available and the protection afforded to whistleblowers, in accordance with Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019, and the Belgian law of 28 November 2022 on the protection of persons who report breaches of Union or national law within a private sector legal entity.

When a person violates a law or internal policy, they put CCB, its employees and other stakeholders at risk.

The sooner such wrongdoing is stopped, the better it is for all parties involved. That is why CCB has implemented this Whistleblowing Policy, with the following objectives:

- **Provide a secure alternative channel** to traditional internal communication channels, enabling employees, managers, suppliers, agents, representatives, distributors or customers to report serious or sensitive issues. These reports may concern violations of ethics or any applicable legislation.
- **Act as an early warning system**, enabling CCB senior management to be informed of these issues as quickly as possible in order to (i) assess and investigate them, and (ii) if necessary, take appropriate measures to limit the consequences of a breach, hazard or other serious risk.

For the avoidance of doubt, reports made under this Whistleblowing Policy must be made on a voluntary basis.

Anyone who becomes aware, in a professional context, of a situation that violates or appears to violate laws and regulations may report it in complete safety. CCB is committed to ensuring the confidentiality of reports and protecting whistleblowers from any form of retaliation or discrimination.

2. SCOPE OF REPORTING

2.1. PERSON INITIATING THE REPORT

The person initiating the report is the "**whistleblower**", i.e. any person who, **in a professional context**, has obtained information about violations (actual or potential) which they have reasonable grounds to believe are true and who reports them.

The following persons are therefore able to make a report:

- Current or former employees;
- Freelancers;
- Shareholders;
- Members of the administrative, management or supervisory body;
- Suppliers;
- Subcontractors;
- Suppliers;
- Customers;
- Job applicants;
- Interns;
- Volunteers.

As an exception, this procedure also applies to persons who report violations relating to financial services, products and markets, as well as anti-money laundering, **outside of a professional context**.

2.2. PURPOSE OF THE REPORT

Whistleblowers may report:

- **Violations observed;**
- **Reasonable suspicions** of actual or potential violations that have occurred or are very likely to occur;
- **Attempts to conceal** these violations.

Reports must concern violations of laws and regulations in the following areas:

- Public procurement;
- Services, products and financial markets, prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Transport safety;

- Environmental protection;
- Radiation protection and nuclear safety;
- Food safety, animal health and welfare;
- Public health;
- Consumer protection;
- Privacy and personal data protection, network and information system security;
- Combating tax and social security fraud.
- Fraud (financial fraud, document fraud, embezzlement);
- Serious defects or deliberate errors in financial reports or internal controls;
- Violations of competition law (price fixing, illegal agreements);
- Failure to respect human rights;
- Corruption or bribery;
- Serious offences relating to safety, the environment or discrimination.

Specific examples:

1. **Product safety:** Distribution of products that do not comply with legal standards.
2. **Transport safety:** Failure by service providers to comply with mandatory driving times.
3. **Data protection:**
 - Illegal transfer of personal data to third parties;
 - Non-compliance with cybersecurity rules.
4. **Competition:** Participation in illegal price-fixing agreements.
5. **Financial offences:** Fraud, money laundering, terrorist financing, corruption, embezzlement.
6. **Discrimination and harassment:** Sexual harassment or other serious forms of intimidation.
7. **Public procurement:** Favouritism or illegal contacts with civil servants.

If there is any doubt about the application of this policy or whether an act constitutes a violation, whistleblowers are encouraged to seek further information from their line manager or CCB Legal Department.

2.3. EXCLUSIONS FROM THIS POLICY

The Whistleblowing Policy is intended solely for reporting abuses or irregularities (suspected or proven) that fall within the scope defined by this policy.

For any other issues, it is recommended that you follow the appropriate internal procedures or contact the relevant departments. This policy does not replace existing internal communication channels within CCB, but complements them by providing an additional option for reporting in confidence and without fear of reprisal.

The Whistleblowing Policy is not intended for:

- **Ordinary complaints about the CWB:** For these cases, you can use the internal complaints procedure.
- **Complaints related to CWB customers or suppliers:** These complaints should be handled through dedicated internal processes.
- **Personal grievances of employees:** The management or reporting of individual grievances is not covered by the Whistleblowing Policy.

Although the Whistleblowing Policy aims to provide a safe framework for reporting serious violations or irregularities, certain types of reports fall outside its scope.

These exclusions are as follows:

1. Immediate emergency situations

Reports concerning an immediate threat to life, health, safety of persons or property are not covered by this policy. In case of emergency, the whistleblower is advised to immediately contact the relevant local authorities or call the local emergency number.

2. Complaints about employment conditions

Any complaints by the whistleblower regarding their employment conditions (e.g. salary, working hours, leave) are not covered by this policy. These issues should be addressed through existing internal channels, such as Human Resources.

3. Personal disputes unrelated to a violation

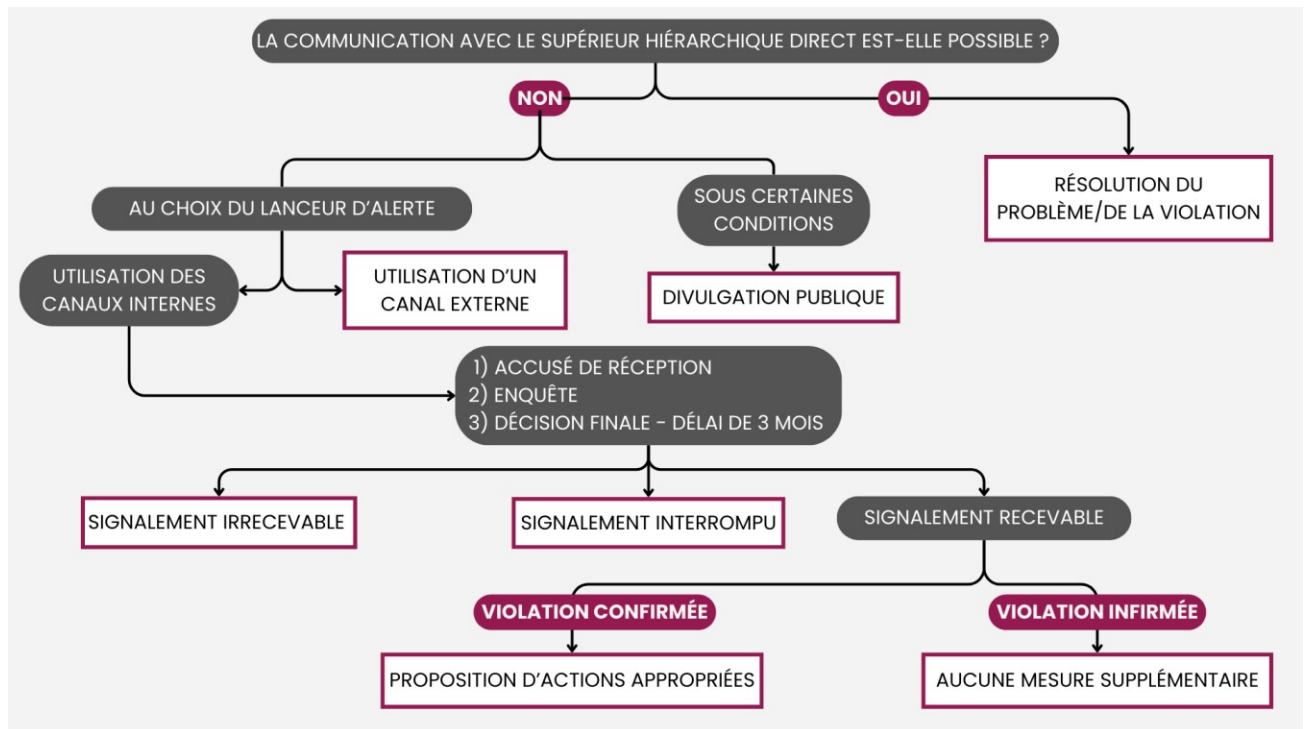
Personal disputes or disagreements between colleagues, unless they involve a violation of the scope of this policy, are not covered.

3. REPORTING CHANNELS

Whistleblowers may submit their reports via:

- Internal reporting channels, for which CCB is responsible;
- External reporting channels;
- Public disclosure.

3.1. OVERVIEW



3.2. INTERNAL REPORTING CHANNELS

Before making any report in accordance with this Procedure, whistleblowers are encouraged to first consider communicating with their line manager or immediate superior.

If, for any reason, the whistleblower feels that they cannot speak to their direct line manager or that the response provided is not satisfactory, they may then use the internal reporting channels.

a) How internal reporting channels work

If the whistleblower discovers, becomes aware of or has reasonable grounds to suspect a violation in any of the above areas, they may report it to CCB through the designated reporting manager, whose contact details are provided below.

Each report must be detailed and documented, including the following information – to the extent known – so that the reporting manager can verify the validity of the reported violations:

- A detailed description of the events giving rise to the violation and how the whistleblower became aware of them;
- The date and location of the event(s);
- The names and positions of the persons subject to the report or information enabling them to be identified;
- The names and positions of any other persons who can confirm the reported facts;
- Any other information that could help the reporting manager verify the facts.

Whistleblowers may report violations in accordance with the GROUP WHISTLEBLOWING MANAGEMENT PROCEDURE through the Cementir Holding Group reporting system:

The Cementir platform complements local mechanisms and complies with Belgian legislation on the protection of whistleblowers, guaranteeing confidentiality, independence and appropriate follow-up.

Reports of suspected violations or behaviour can also be made via the Cementir Holding Group's professional alert platform, accessible at the following address: <https://cementir.integrityline.com>.

This secure platform allows concerns to be reported confidentially and, if desired, anonymously. It provides useful information on:

- What can be reported;
- The level of anonymity guaranteed;
- The use of secure messaging to ensure follow-up;
- The applicable whistleblowing policy;
- Legal rights and options for reporting to external authorities in the European Union.

All reports made through this channel are strictly confidential and treated in accordance with applicable data protection and whistleblower legislation.

Email: Whistleblowing@cementirholding.it or ethicscommittee@cementirgroup.com

Post: Cementir Holding Internal Audit Department, Corso di Francia 200, 00191 Rome, Italy

b) Report processing

The report manager will acknowledge receipt of the report within 7 days, using the same means of communication.

The report manager will then investigate the report promptly and diligently in collaboration with the relevant internal departments. The report manager will verify the validity of the reported facts, while respecting the principles of impartiality, fairness and confidentiality. The latter principle applies to all persons concerned by the report, in order to avoid any unnecessary damage to their reputation. Consequently, any person participating in an investigation or learning of the existence of such an investigation must maintain confidentiality.

The reporting manager may also decide to involve other functions, either internal or external to CCB, if deemed necessary in the context of the investigation.

If the report concerns the reporting manager himself, the whistleblower is invited to contact the Chairman of CCB Board of Directors, Mr Eddy Fostier, directly by email at eddy.fostier@ccb.be.

c) Outcome of the report and final decision

Following the investigation carried out by the reporting manager, the latter may take the following decisions:

- 1) The report is considered **inadmissible** because it does not fall within the scope of this policy;
- 2) **Follow-up on the report is discontinued:**
 - In that it does not contain sufficient verifiable evidence to allow for a more thorough investigation, further investigation is therefore necessary;
 - Where the same facts reported have already been reported and investigated;
- 3) The report is considered **admissible but the reported violation is not confirmed by the investigation**: in this case, CCB will not take any further action.
- 4) The report is considered **admissible and valid**; appropriate actions are therefore proposed to CCB in order to put an end to the reported violation.

The report manager communicates their final decision to the whistleblower within three months of acknowledging receipt of the report.

d) Cooperation and good faith

Whistleblowers must report in good faith and must not make any accusations that they know to be false. Anyone else involved in an investigation must also cooperate and answer the reporting manager's questions in good faith. Lying, delaying, obstructing or refusing to cooperate with an investigation may result in disciplinary action.

In all cases, CCB does not permit any form of retaliation, threats, punishment or discrimination against the whistleblower or any person who has cooperated in good faith with the investigation.

However, if a report contains false, unfounded or opportunistic allegations, or if it is made for the sole purpose of discrediting or harming others, the whistleblower acting in bad faith is liable to a penalty of up to one year's imprisonment and/or a fine of €8,000, as well as disciplinary action.

3.3. EXTERNAL REPORTING CHANNEL

We strongly recommend that whistleblowers use the internal reporting channel as a first resort. CCB has implemented this procedure and the necessary resources to deal with reports appropriately, making it an effective tool.

However, whistleblowers may report externally by contacting one of the competent authorities directly if they believe that their report has not produced a satisfactory outcome. The rules governing external reporting and the competent authority vary depending on the area in which the breach was reported (see Appendix 1).

3.4. PUBLIC DISCLOSURE

Whistleblowers also have the option of making their report public, for example by informing the press or publishing it online.

However, whistleblowers who make a public disclosure are only protected under two conditions:

- The whistleblower has reported the issue to the competent authority but no appropriate follow-up action has been taken (from an objective point of view); and
- The whistleblower has reasonable grounds to believe that the reported matter may pose an imminent or obvious danger to the public interest, particularly in cases of emergency or risk of irreversible damage. For example, this may be the case when the whistleblower believes there is a risk that evidence of the violation will be concealed or destroyed.

4. RIGHTS OF THE WHISTLEBLOWER

4.1. CONFIDENTIALITY

Whistleblowers have the right to confidentiality. Their identity and the details of their report remain confidential during and after the investigation.

However, the whistleblower's identity will be disclosed in the following circumstances:

- The whistleblower has consented to it; or
- Such disclosure is required by law, for example in the context of investigations conducted by national authorities or in the context of legal proceedings. Where applicable, CCB is required to notify the whistleblower, unless this would compromise the investigation or proceedings (e.g. if there is a risk of evidence being destroyed).

Unauthorised disclosure of the above information is not permitted by CCB and will result in disciplinary action, including dismissal of the person who disclosed the information. Depending on the circumstances, unauthorised disclosure may also result in civil or criminal prosecution.

4.2. PROTECTION AGAINST RETALIATION

Whistleblowers are protected against retaliation if the following conditions are met:

- The whistleblower has reasonable grounds to believe that, at the time of reporting, the information reported was truthful.
- The whistleblower has followed the procedure set out herein.

However, if the information is incorrect but the whistleblower reported it in good faith, they are still protected.

This protection means that CCB may not take any retaliatory measures against the whistleblower (see Appendix 2).

Consequently, any person working within CCB who takes actions that could be considered retaliatory or who encourages other workers to take retaliatory action against the whistleblower may be subject to sanctions or legal proceedings (including disciplinary measures, dismissal,

criminal prosecution, etc.).

retaliation against the whistleblower may be subject to sanctions or legal proceedings (including disciplinary measures, dismissal, criminal prosecution, etc.).

4.3. REMEDIES

In the event that, despite the application of this procedure, the whistleblower is subject to retaliatory measures, they also have certain remedies available to them.

For example, if the whistleblower has been dismissed, the appropriate remedy would be reinstatement to their job. An appropriate remedy may also take the form of reinstatement of a licence or contract if it has been cancelled as a result of the whistleblower's report.

4.4. SUPPORT MEASURES

In addition, whistleblowers have access to support measures, including:

- Comprehensive and independent information and advice;
- Technical advice to authorities;
- Legal assistance in accordance with European rules in cross-border criminal and civil proceedings;
- Support measures (technical, psychological, media and social);
- Financial assistance in legal proceedings.

4.5. EXTENSION OF PROTECTION FOR WHISTLEBLOWERS

The protection afforded to whistleblowers is also extended to the following persons:

- 'Facilitators', i.e. natural persons who assist the whistleblower during the reporting process and whose assistance should be confidential;
- Third parties who are connected to whistleblowers and who may be subject to retaliation in a professional context, such as colleagues or relatives of whistleblowers;
- Legal entities owned by whistleblowers or for which they work, or with which they have a professional relationship.

5. RIGHTS OF THE PERSON BEING REPORTED

Any person who is the subject of a report is informed by the report manager that a report has been made against them, so that they can respond.

This information shall be provided as soon as possible, unless there are reasonable grounds to believe that the person subject to the report is in a position to destroy the information, manipulate files, or jeopardise or compromise the investigation in any way. In this case, the person shall not be informed or shall be informed at a later date.

The person concerned may contact the report manager to exercise their right of access to information concerning them, in accordance with applicable data protection legislation (GDPR).

However, the following restrictions apply:

- The person who is the subject of the report may only be informed of the facts reported concerning them;
- The person who is the subject of the report is not informed of the identity of the whistleblower;
- The rights of the person who is the subject of the report are limited to data concerning that person.

Manifestly abusive requests from the person who is the subject of the report may also be refused, for example in the case of repetitive requests for access to data.

Where possible and appropriate, the reporting manager will inform the person subject to the report of their final decision.

6. PROCESSING OF PERSONAL DATA

Only personal data that is strictly necessary for processing and verifying the validity of the report will be collected and used, exclusively within the framework of the procedures described in this Policy by CCB, as the data controller.

CCB declares that all personal data of whistleblowers and any other persons concerned (including special categories of so-called "sensitive" data) obtained in the context of reports will be processed in strict compliance with the provisions of applicable personal data protection legislation and with its Privacy Policy.

Categories of personal data processed

The personal data that may be collected includes:

1. When submitting a report:
 - Standard identification data: surname, first name, company, position, address and telephone number (if provided);
 - Information about the reported facts;
 - Information about the persons mentioned in the report or involved in its processing.
 - Any personal data provided by the whistleblower in their report;
2. During an investigation:
 - Standard identification data of the persons concerned;
 - Data necessary to process the complaint and investigate the reported facts.
 - Any personal data transmitted during the various exchanges during the investigation and in the investigation report.
3. Documentation generated:
 - Initial report, information gathered during the investigation, investigation

report and conclusions.

Purposes and legal basis for data processing

The purposes of personal data processing, including any transfers within CCB, are as follows:

- a. To promote honesty, integrity and ethics within CCB;
- b. Enable reporting via the company's internal reporting system;
- c. Manage complaints and process reports made through the internal reporting system;
- d. To determine whether an investigation is necessary and to conduct/organise that investigation;
- e. Analyse the results of investigations into reports received;
- f. Determine the corrective actions to be taken following a report and/or related investigation and implement the relevant measures.

We process personal data in order to manage whistleblower reports and investigate allegations. The processing of your personal data is necessary in this context to comply with a legal obligation to which we are subject.

We may disclose personal data to the police or judicial authorities as evidence if there are reasonable grounds to believe that an illegal act or crime has been committed by you in connection with the reporting process.

In addition, the processing of certain specific categories of personal data will only be carried out if necessary to establish, exercise or defend legal rights, or as permitted by applicable data protection legislation.

Suspected criminal offences will only be processed to the extent necessary for the management of disputes specific to CCB or as otherwise permitted by law.

In certain circumstances, CCB may also process personal data collected through the reporting system if this is necessary to comply with legal obligations to which CCB is subject.

No automated decisions, including profiling, are made.

The personal data collected will not be used for direct marketing purposes.

Data retention and deletion

The data collected will be retained only for as long as necessary and proportionate, in accordance with legal obligations:

- Immediate deletion if the report is outside the scope of application or unfounded.
- Deletion after the investigation or actions taken have been closed, unless otherwise required by law.
- Retention for 10 years corresponding to the statutory limitation period (Article 2262bis of the former Civil Code).

Data security and confidentiality

CCB and its partners use appropriate technical and organisational measures to ensure data security, in accordance with the GDPR. Reporting channels are secure, with access restricted to authorised persons only.

Rights of data subjects

In certain jurisdictions, such as the European Union and the European Economic Area, a person whose data is processed (the "data subject") in accordance with this Policy has several rights, summarised below. Please note that the exercise of these rights is subject to additional requirements and conditions under applicable data protection legislation. In summary, each person has the following rights:

- To obtain confirmation from CCB as to whether the personal data of the data subject is being processed, and to request access to that data, the purposes of its processing and the recipients or categories of recipients concerned.
- To obtain from CCB the rectification of inaccurate or incomplete personal data concerning the data subject.
- To obtain from CCB the erasure of personal data concerning the data subject, where this is legally applicable.
- Request that CCB restrict the processing of the personal data of the data subject.
- Receive personal data provided by the data subject to CCB in a structured, commonly used and machine-readable format.
- Object to the processing of the data subject's personal data by CCB.

If a data subject wishes to exercise these rights or obtain information about their data, they may contact CCB's Legal Department at the following address: stephanie.heyman@ccb.be.

Individuals subject to European data protection regulations who wish to lodge a complaint regarding the processing described herein may do so with the competent data protection authority, in particular in the Member State of their habitual residence, place of work or place where an alleged breach of data protection regulations has occurred.

For more information on data processing and individual rights, please refer to CCB's Privacy Statement.

7. CONTACT DETAILS OF THE REPORTING MANAGER

For any questions regarding this policy, interested parties may contact the CWB's reporting manager directly using the following contact details:

Whistleblowing@cementirholding.it

8. UPDATES

This policy will be updated in the event of changes to legislation.

APPENDIX 1. LIST OF COMPETENT BELGIAN AUTHORITIES

In Belgium, information and support for whistleblowers is provided through two bodies:

- The *Federal Ombudsman*, acting as the federal coordinator for external reports. The Ombudsman receives external reports, verifies their admissibility and forwards the information to the competent authority. In exceptional cases, the Ombudsman also investigates the substance of the case and deals with protection cases.
- *The Federal Institute for the Protection and Promotion of Human Rights (IFDH)*, which provides whistleblowers with professional, legal and psychological support. This can be done through the Institute itself or through third parties such as law firms or psychologists specialising in this field.

In addition to these two instruments, there are 24 competent authorities depending on the area concerned by the reported violation:

- | | | |
|---|--|---|
| ○ The Federal Public Service Economy, SMEs, Self-Employed and Energy | ○ The Federal Agency for Nuclear Control | ○ The authorities referred to in Article 85 of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash |
| ○ The Federal Public Service Finance | ○ The Federal Agency for Medicines and Health Products | ○ The National Security Committee for the Supply and Distribution of Drinking Water |
| ○ The Federal Public Service for Public Health, Food Chain Safety and the Environment | ○ The Federal Agency for the Safety of the Food Chain | ○ The Belgian Institute for Postal Services and Telecommunications |
| ○ The Federal Public Service Mobility and Transport | ○ The Belgian Competition Authority | ○ The National Institute for Health and Disability |
| ○ The Federal Public Service Employment, Labour and Social Dialogue | ○ The Data Protection Authority | ○ The National Institute for Social Insurance for Self-Employed Persons |
| ○ The Public Service for Social Integration, Combating Poverty, Social Economy and Urban Policy | ○ The Financial Services and Markets Authority | ○ The National Employment Office |
| ○ The National Social Security Office | ○ The National Bank of Belgium | ○ The Independent Anti-Fraud Coordination Service (CAF) |
| | ○ The Supervisory Board of Company Auditors | |
| | ○ The Social Information and Research Service | |

APPENDIX 2. NON-EXHAUSTIVE LIST OF PROHIBITED FORMS OF RETALIATION (ART. 23 LAW OF 28 NOVEMBER 2022)

Any form of retaliation against persons benefiting from whistleblower protection is prohibited, including threats of retaliation and attempts at retaliation, in particular in the following forms:

- Suspension, dismissal, termination of employment or equivalent measures;
- Demotion or refusal of promotion;
- Transfer of duties, change of workplace, reduction in salary, change in working hours;
- Suspension of training;
- Negative performance appraisal or work assessment;
- Disciplinary measures imposed or administered, reprimand or other sanction, including financial penalty;
- Coercion, intimidation, harassment or ostracism;
- Discrimination, disadvantageous or unfair treatment;
- Failure to convert a temporary employment contract into a permanent contract, when the worker could legitimately expect to be offered permanent employment;
- Failure to renew or early termination of a temporary employment contract;
- Damage, including damage to the person's reputation, particularly on social media, or financial loss, including loss of business and loss of income;
- Blacklisting on the basis of a formal or informal agreement at sector or industry level, which may mean that the person will not be able to find employment in the sector or industry in the future;
- Early termination or cancellation of a contract for the supply of goods or services;
- Cancellation of a licence or permit;
- Referral for psychiatric or medical treatment.