POLITIQUE DE DÉNONCIATION ET DE PROTECTION DES LANCEURS D'ALERTE ("POLITIQUE DE SIGNALEMENT")

- CCB -

Décembre 2025

1. INTRODUCTION

« CCB » désigne : La COMPAGNIE DES CIMENTS BELGES (ci-après, « la CCB »), immatriculée à la Banque Carrefour des Entreprises sous le numéro 0419.445.816 et dont le siège social est situé au 260 Grand'Route à 7530 Tournai.

La présente politique de dénonciation et de protection des lanceurs d'alerte (ci-après, la « Politique de Signalement ») est complémentaire au Règlement de Travail de la CCB. En cas de contradiction entre cette politique et le Règlement de Travail, ce dernier prévaut.

Cette Politique de Signalement vise à informer sur les canaux de signalement disponibles ainsi que sur la protection accordée aux lanceurs d'alerte, conformément à la directive 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019, et à la loi belge du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé.

Lorsqu'une personne enfreint une loi ou une politique interne, elle met la CCB, ainsi que ses employés et autres parties prenantes, en danger.

Plus tôt un tel acte répréhensible est stoppé, mieux c'est pour toutes les parties concernées. C'est pourquoi la CCB a mis en place cette Politique de Signalement, avec pour objectifs :

- **Garantir un canal sûr et alternatif** aux voies de communication internes traditionnelles, permettant aux employés, managers, fournisseurs, agents, représentants, distributeurs ou clients de signaler des questions graves ou sensibles. Ces signalements peuvent concerner des violations concernant l'éthique ou de toute législation applicable.
- **Agir comme un système d'alerte précoce**, en permettant à la direction générale de la CCB d'être informée de ces problèmes le plus rapidement possible, afin de (i) les évaluer et les investiguer, et (ii) si nécessaire, de prendre des mesures appropriées pour limiter les conséquences d'une infraction, d'un danger ou d'un autre risque grave.

Pour éviter toute ambiguïté, les signalements effectués dans le cadre de cette Politique de Signalement doivent être réalisés sur une base volontaire.

Toute personne ayant connaissance, dans un contexte professionnel, d'une situation qui viole ou semble violer les lois et règlements peut ainsi la signaler en toute sécurité. La CCB s'engage à garantir la confidentialité des signalements et à protéger les lanceurs d'alerte contre toute forme de représailles ou de discrimination.

2. ***CHAMP D'APPLICATION DU SIGNALEMENT***

2.1. PERSONNE À L'INITIATIVE DU SIGNALEMENT

La personne à l'initiative du signalement est le « ***lanceur d'alerte*** », c'est-à-dire toute personne qui - **dans un contexte professionnel** - a obtenu des informations sur des violations (effectives ou potentielles), à propos desquelles elle a des motifs raisonnables de croire qu'elles sont véridiques et qui en fait le signalement.

Les personnes suivantes ont ainsi la possibilité d'effectuer un signalement :

- Les actuels ou anciens travailleurs ;
- Les indépendants ;
- Les actionnaires ;
- Les membres de l'organe d'administration, de direction ou de surveillance ;
- Les fournisseurs ;
- Les sous-traitants ;
- Les fournisseurs ;
- Les clients ;
- Les candidats à un emploi ;
- Les stagiaires ;
- Les bénévoles.

Par exception, la présente procédure est également applicable aux personnes qui signalent - **en dehors d'un contexte professionnel** - une violation en matière de services, produits et marchés financiers ainsi qu'en matière de la Lutte contre le blanchiment d'argent.

2.2. OBJET DU SIGNALEMENT

Le lanceur d'alerte peut effectuer un signalement portant sur :

- **Des violations constatées** ;
- **Des soupçons raisonnables** de violations réelles ou potentielles qui ont eu lieu ou sont très susceptibles de se produire ;
- **Des tentatives de dissimulation** de ces violations.

Les signalements doivent concerner des violations des lois et règlements dans les domaines suivants :

- Marchés publics ;
- Services, produits et marchés financiers, prévention du blanchiment d'argent et du financement du terrorisme ;
- Sécurité et conformité des produits ;
- Sécurité des transports ;

- Protection de l'environnement ;
- Radioprotection et sûreté nucléaire ;
- Sécurité alimentaire, santé et bien-être des animaux ;
- Santé publique ;
- Protection des consommateurs ;
- Protection de la vie privée et des données personnelles, sécurité des réseaux et des systèmes d'information ;
- Lutte contre la fraude fiscale et sociale.
- Fraude (fraude financière, fraude documentaire, détournement de fonds) ;
- Défauts graves ou erreurs délibérées dans les rapports financiers ou contrôles internes ;
- Violations du droit de la concurrence (fixation des prix, ententes illégales) ;
- Non-respect des droits de l'homme ;
- Corruption ou pots-de-vin ;
- Infractions graves en matière de sécurité, environnement ou discrimination.

Exemples spécifiques :

1. **Sécurité des produits :** Distribution de produits ne respectant pas les normes légales.
2. **Sécurité des transports :** Non-respect des temps de conduite obligatoires par des prestataires.
3. **Protection des données :**
    - Transmission illégale de données personnelles à des tiers ;
    - Non-conformité avec les règles de cybersécurité.
4. **Concurrence :** Participation à des accords illégaux sur les prix.
5. **Infractions financières :** Fraude, blanchiment d'argent, financement du terrorisme, corruption, détournements.
6. **Discrimination et harcèlement :** Harcèlement sexuel ou autre forme grave d'intimidation.
7. **Marchés publics :** Favoritisme ou contacts illégaux avec des fonctionnaires.

En cas de doute sur l'application de la présente politique ou sur la qualification d'un acte comme violation, le lanceur d'alerte est encouragé à demander des informations complémentaires auprès de son supérieur hiérarchique ou du Service Juridique de la CCB.

2.3. EXCLUSIONS DE LA PRÉSENTE POLITIQUE

La Politique de Signalement est uniquement destinée à signaler des abus ou des irrégularités (suspectés ou avérés) qui relèvent du champ d'application défini par cette politique.

Pour toute autre problématique, il est recommandé de suivre les procédures internes appropriées ou de contacter les départements concernés. Cette politique ne remplace pas les canaux de communication internes existants au sein de la CCB, mais les complète en offrant une option supplémentaire de signalement en toute confiance et sans crainte de représailles.

La Politique de Signalement n'est pas destinée à :

- **Plaintes ordinaires concernant la CCB** : Pour ces cas, vous pouvez utiliser la procédure de réclamations interne.
- **Réclamations liées aux clients ou fournisseurs de la CCB** : Ces réclamations doivent être traitées via les processus internes dédiés.
- **Griefs personnels des employés** : La gestion ou le signalement de griefs individuels ne relève pas de la Politique de Signalement.

Bien que la Politique de Signalement vise à offrir un cadre sécurisé pour signaler des violations graves ou des irrégularités, certains types de signalements ne relèvent pas de son champ d'application.

Ces exclusions sont les suivantes :

1. **Situations d'urgence immédiate**

Les signalements portant sur une menace immédiate pour la vie, la santé, la sécurité des personnes ou des biens ne relèvent pas de cette politique. En cas d'urgence, le lanceur d'alerte est invité à contacter immédiatement les autorités locales compétentes ou à appeler le numéro d'urgence local.

2. **Réclamations sur les conditions d'emploi**

Les éventuelles réclamations du lanceur d'alerte concernant ses conditions d'emploi (par exemple, salaire, horaires, congés) ne relèvent pas de cette politique. Ces questions doivent être traitées via les canaux internes existants, tels que les Ressources Humaines.

3. **Litiges personnels sans lien avec une violation**

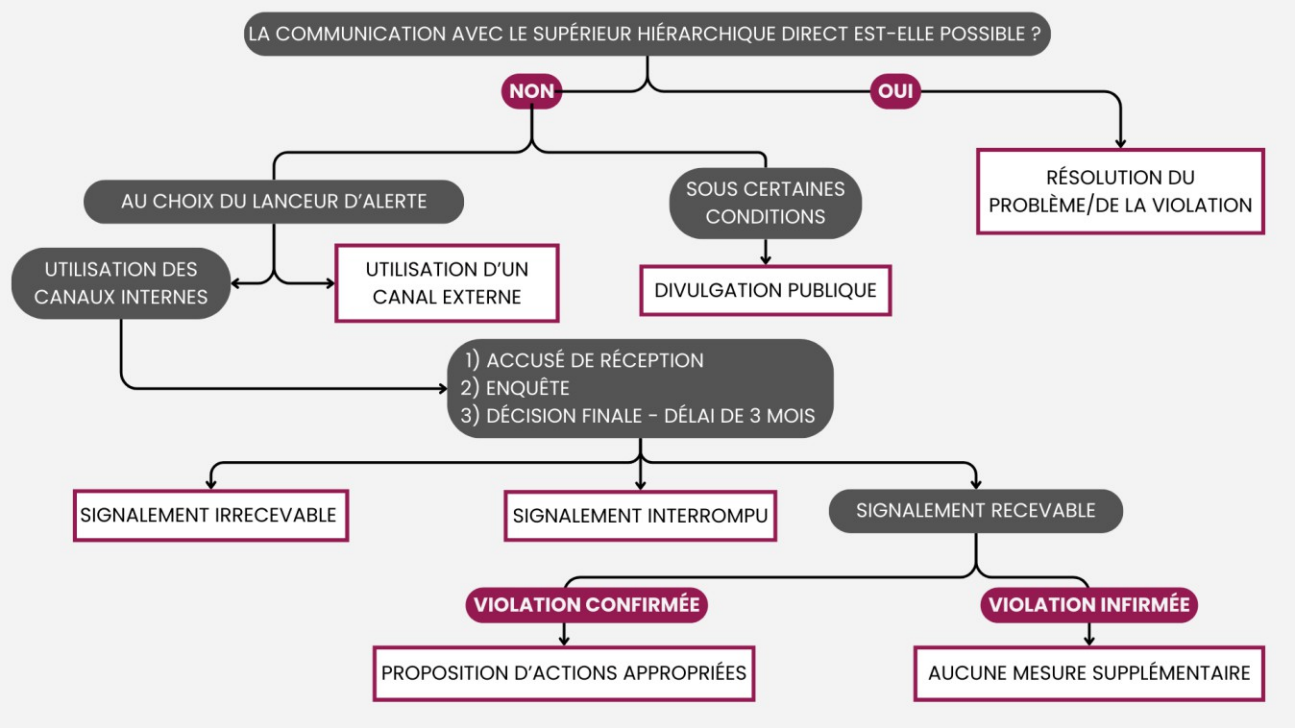
Les litiges personnels ou les différends entre collègues, à moins qu'ils n'impliquent une violation du champ d'application de cette politique, ne sont pas couverts.

3. ***CANAUX DE SIGNALEMENT***

Le lanceur d'alerte a la possibilité de réaliser son signalement via :

- Les canaux de signalement internes, dont la CCB est responsable ;
- Les canaux de signalement externes ;
- La divulgation publique.

3.1. VUE GLOBALE



3.2. CANAUX INTERNES DE SIGNALEMENT

Avant tout signalement conforme à la présente Procédure, le lanceur d'alerte est encouragé à considérer en premier lieu la communication avec son responsable ou supérieur hiérarchique direct.

Si, pour une raison quelconque, le lanceur d'alerte estime qu'il ne peut s'adresser à son supérieur hiérarchique direct ou que la réponse apportée ne peut être considérée comme satisfaisante, il peut alors recourir aux canaux de signalement interne.

a) Fonctionnement des canaux internes de signalement

Si le lanceur d'alerte découvre, prend connaissance ou a des motifs raisonnables de soupçonner une violation à l'un des domaines susmentionnés, il peut en informer la CCB par le biais du gestionnaire de signalement qu'elle a désigné et dont les coordonnées sont reprises ci-dessous.

Chaque signalement doit être détaillé et documenté, incluant les informations suivantes – dans la mesure où elles sont connues – afin que le gestionnaire de signalement puisse vérifier la validité des violations signalées :

- Une description détaillée des événements donnant lieu à la violation et de la manière dont le lanceur d'alerte en a eu connaissance ;
- La date et le lieu de l'événement/des événements ;
- Les noms et fonctions des personnes faisant l'objet du signalement ou les informations permettant de les identifier ;
- Le noms et la fonction de toute autre personne pouvant confirmer les faits rapportés ;
- Toute autre information qui pourrait aider le gestionnaire de signalement à vérifier les faits.

Le lanceur d'alerte peut signaler les violations conformément au GROUP WHISTLEBLOWING MANAGEMENT PROCEDURE par le biais du système de signalement du Groupe Cementir Holding :

La plateforme Cementir complète les dispositifs locaux et est conforme à la législation belge en matière de protection des lanceurs d'alerte, garantissant la confidentialité, l'indépendance et un suivi approprié.

Les signalements d'infractions ou de comportements suspectés peuvent également être effectués via la plateforme d'alerte professionnelle du Groupe Cementir Holding, accessible à l'adresse suivante : https://cementir.integrityline.com.

Cette plateforme sécurisée permet de signaler des préoccupations de manière confidentielle et, si souhaité, de manière anonyme. Elle fournit des informations utiles concernant :

- Ce qui peut être signalé ;
- Le niveau d'anonymat garanti ;
- L'utilisation de la messagerie sécurisée pour assurer un suivi ;
- La politique applicable en matière d'alerte professionnelle ;
- Les droits légaux et les possibilités de signalement auprès d'autorités externes dans l'Union européenne.

Tous les signalements effectués par ce canal sont strictement confidentiels et traités conformément à la législation applicable en matière de protection des données et de lanceurs d'alerte.

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

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

b) Traitement du signalement

Le gestionnaire de signalement accuse réception du signalement dans un délai de 7 jours, par le biais du même moyen de communication.

Le gestionnaire de signalement enquête ensuite rapidement et avec diligence en collaboration avec les services internes concernés. Le gestionnaire de signalement vérifie ainsi la validité des faits signalés, tout en respectant les principes d'impartialité, d'équité et de confidentialité. Ce dernier principe s'applique à toutes les personnes concernées par le signalement, afin d'éviter toute atteinte inutile à leur réputation. Par conséquent, toute personne participant à une enquête ou apprenant l'existence de ladite enquête, doit en préserver la confidentialité.

Le gestionnaire de signalement peut également décider d'impliquer d'autres fonctions, internes ou externes à la CCB, s'il l'estime nécessaire dans le cadre de l'enquête.

Dans l'hypothèse où le signalement concerne le gestionnaire de signalement en lui-même, le

lanceur d'alerte est invité à s'adresser directement au Président du Conseil d'Administration de la CCB, Mr Eddy Fostier par le biais d'un email eddy.fostier@ccb.be.

c) Issue du signalement et décision finale

Suite à l'enquête réalisée par le gestionnaire de signalement, ce dernier est susceptible de prendre les décisions suivantes :

1) Le signalement est considéré comme étant ***irrecevable*** parce qu'il ne relève pas du champ d'application de la présente politique ;

2) Le ***suivi du signalement est interrompu*** :
   - En ce qu'il ne comporte pas suffisamment de preuves vérifiables pour permettre une enquête plus approfondie, un complément d'enquête étant donc nécessaire ;

- En ce que les mêmes faits rapportés ont déjà fait l'objet d'un signalement et d'une enquête ;

3) Le signalement est considéré comme ***recevable mais la violation signalée n'est pas confirmée par l'enquête*** : dans ce cas, la CCB ne prendra aucune mesure supplémentaire.

4) Le signalement est considéré comme ***recevable et valide*** ; des actions appropriées sont par conséquent proposées à la CCB afin de mettre fin à la violation signalée.

Le gestionnaire de signalement communique sa décision finale au lanceur d'alerte dans un délai de 3 mois à compter de l'accusé de réception du signalement.

d) Coopération et bonne foi

Le lanceur d'alerte effectue son signalement en toute bonne foi et ne porte aucune accusation s'il sait sciemment que celles-ci sont fausses. Toute autre personne impliquée dans une enquête doit également coopérer et répondre en toute bonne foi aux questions du gestionnaire de signalement. Le fait de mentir, de retarder, d'entraver ou de refuser de coopérer à une enquête peut donner lieu à des mesures disciplinaires.

Dans tous les cas, la CCB ne permet aucune forme de représailles, de menaces, de punitions ou de discrimination à l'encontre du lanceur d'alerte ou de toute personne ayant coopérée bonne foi à l'enquête.

Toutefois, si un signalement contient des allégations fausses, infondées ou opportunistes, ou s'il est réalisé dans le seul but de discréditer ou de nuire à autrui, le lanceur d'alerte de mauvaise foi s'expose à une peine pouvant aller jusqu'à un an d'emprisonnement et/ou une amende de 8000 €, ainsi qu'à des mesures disciplinaires.

3.3. CANAL EXTERNE DE SIGNALEMENT

Nous recommandons vivement au lanceur d'alerte de privilégier en premier lieu le canal de signalement interne. La CCB a en effet mis en œuvre la présente procédure ainsi que les ressources nécessaires pour traiter les signalements de manière adéquate, rendant ainsi son utilisation efficace.

Néanmoins, le lanceur d'alerte a la possibilité d'effectuer un signalement externe en s'adressant directement à l'une des autorités compétentes s'il estime que son signalement n'a pas abouti à un résultat satisfaisant. Les règles de signalement externe ainsi que l'autorité compétente varient en fonction du domaine de la violation signalée (voir Annexe 1).

3.4. DIVULGATION PUBLIQUE

Le lanceur d'alerte a également la possibilité de rendre public son signalement, notamment en informant la presse ou en publiant en ligne.

Cependant, le lanceur d'alerte qui réalise une divulgation publique bénéficie uniquement de la protection sous deux conditions :

- Le lanceur d'alerte a signalé son problème à l'autorité compétente mais aucune mesure de suivi appropriée n'a été prise (d'un point de vue objectif) ; et

- Le lanceur d'alerte a des motifs raisonnables de croire que le fait signalé peut représenter un danger imminent ou manifeste pour l'intérêt public, notamment en cas d'urgence ou de risque de dommages irréversibles. Par exemple, cela peut être le cas lorsque le lanceur d'alerte estime qu'il existe un risque que les preuves de la violation soient dissimulées ou détruites.

4. DROITS DU LANCEUR D'ALERTE

4.1. CONFIDENTIALITÉ

Le lanceur d'alerte a droit à la confidentialité. Ainsi, son identité ainsi que les détails de son signalement restent confidentiels pendant et après l'enquête.

En revanche, l'identité du lanceur d'alerte est divulguée dans les hypothèses où :

- Le lanceur d'alerte y a consenti ; ou
- Cette divulgation est exigée par la loi, par exemple dans le cadre d'enquêtes menées par des autorités nationales ou dans le cadre de procédures judiciaires. Le cas échéant, la CCB est tenue d'en avertir le lanceur d'alerte, à moins que cela ne risque de compromettre l'enquête ou la procédure (p. ex., s'il y a un risque de destruction des preuves).

La divulgation non autorisée des informations précitées n'est pas acceptée par la CCB et entraîne des mesures disciplinaires, voire le licenciement de la personne ayant divulgué les informations en question. Selon les circonstances, la divulgation non autorisée peut également donner lieu à des poursuites civiles ou pénales.

4.2. PROTECTION CONTRE LES REPRÉSAILLES

Le lanceur d'alerte bénéficie d'une protection contre les représailles si les conditions suivantes sont respectées :

- Le lanceur d'alerte a des motifs raisonnables de croire qu'au moment du signalement, les informations signalées étaient véridiques.
- Le lanceur d'alerte a suivi la procédure telle que prévue par la présente.

Cependant, dans l'hypothèse où l'information est incorrecte mais que le lanceur d'alerte l'a transmise de bonne foi, il bénéficie tout de même de la protection.

Cette protection implique que la CCB ne peut pas prendre de mesures de rétorsion à l'encontre du lanceur d'alerte (voir Annexe 2).

Par conséquent, toute personne travaillant au sein de la CCB qui entreprend des actions pouvant être considérées comme des représailles ou qui encourage d'autres travailleurs à exercer des

représailles à l'encontre du lanceur d'alerte, peut faire l'objet de sanctions ou de poursuites judiciaires (y compris des mesures disciplinaires, un licenciement, des poursuites pénales, etc.).

4.3. VOIES DE RECOURS

Dans l'hypothèse où - malgré l'application de la présente procédure - le lanceur d'alerte est sujet de mesures de représailles, il bénéficie également de certaines voies de recours.

Par exemple, si le lanceur d'alerte a fait l'objet d'un licenciement, le recours approprié à cette mesure serait la réintégration à son travail. Une voie de recours appropriée peut également prendre la forme d'un rétablissement d'un permis ou d'un contrat, si ce dernier a été annulé en conséquence du signalement effectué par le lanceur d'alerte.

4.4. MESURES DE SOUTIEN

En outre, le lanceur d'alerte dispose de mesures de soutien, notamment :

- Des informations et des conseils complets et indépendants ;
- Des conseils techniques à l'égard des autorités ;
- Une assistance juridique conformément aux règles européennes dans le cadre des procédures pénales et civiles transfrontières ;
- Des mesures de soutien (sur le plan technique, psychologique, médiatique et social) ;
- Une assistance financière dans le cadre de procédures judiciaires.

4.5. EXTENSION DE LA PROTECTION DES LANCEURS D'ALERTE

La protection accordées aux lanceurs d'alerte est également étendue aux personnes suivantes :

- Les « ***facilitateurs*** », c'est-à-dire les personnes physiques qui aident le lanceur d'alerte au cours du processus de signalement et dont l'aide devrait être confidentielle ;

- Les tiers qui sont en lien avec les lanceurs d'alerte et qui risquent de faire l'objet de représailles dans un contexte professionnel, tels que des collègues ou des proches des lanceurs d'alerte ;

- Les entités juridiques appartenant aux lanceurs d'alerte ou pour lesquelles ils travaillent, ou encore avec lesquelles ils sont en lien dans un contexte professionnel.

5. DROITS DE LA PERSONNE FAISANT L'OBJET DU SIGNALEMENT

Toute personne faisant l'objet d'un signalement est informée par le gestionnaire de signalement qu'un signalement a été réalisé à son encontre, afin qu'elle puisse y répondre.

Cette information se fait dès que possible, sauf s'il existe des motifs raisonnables de croire que la personne faisant l'objet du signalement est en mesure de détruire les informations, de manipuler des fichiers, de mettre en péril ou de compromettre d'une quelconque manière l'enquête. Dans ce cas, l'information de cette personne n'aura pas lieu ou sera retardée.

Cette personne a la possibilité de contacter le gestionnaire de signalement afin d'exercer son droit d'accès aux informations le concernant, conformément à la législation applicable en matière de protection des données (« ***RGPD*** »).

Toutefois, les restrictions suivantes s'appliquent :

- La personne faisant l'objet du signalement ne peut être informée que des faits signalés la concernant ;
- La personne faisant l'objet du signalement n'est pas informée de l'identité du lanceur d'alerte ;
- Les droits de la personne faisant l'objet du signalement sont limités aux données la concernant.

Les demandes manifestement abusives de la part de la personne faisant l'objet d'un signalement peuvent également être refusées, par exemple en cas de demandes d'accès aux données répétitives.

Si cela est possible et approprié, le gestionnaire de signalement informera la personne faisant l'objet du signalement de sa décision finale.

6. TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Seules les données personnelles strictement nécessaires pour traiter et vérifier la validité du signalement seront collectées et utilisées, et ce, exclusivement dans le cadre des procédures décrites dans cette Politique par la CCB, en tant que responsable du traitement.

CCB déclare que toutes les données personnelles des lanceurs d'alerte et de toute autre personne concernée (y compris les catégories particulières de données dites "sensibles") obtenues dans le cadre des signalements seront traitées en stricte conformité avec les dispositions de la législation applicable en matière de protection des données personnelles et avec sa Politique de Confidentialité.

Catégories de données à caractère personnel traitées

Les données personnelles susceptibles d'être collectées incluent :

1. Lors de la soumission d'un signalement :
    - Données d'identification standard : nom, prénom, société, fonction, adresse et numéro de téléphone (si fournis) ;
    - Informations sur les faits signalés ;
    - Informations relatives aux personnes mentionnées dans le signalement ou impliquées dans son traitement.
    - Toute donnée à caractère personnel transmise par le lanceur d'alerte dans son signalement ;

2. Lors d'une enquête :
    - Données d'identification standard des personnes concernées ;
    - Données nécessaires pour traiter la plainte et enquêter sur les faits signalés.
    - Toute donnée à caractère personnel transmise lors des divers échanges au cours de l'enquête et dans le rapport d'enquête.

3. Documentation générée :
    - Signalement initial, informations collectées durant l'enquête, rapport d'enquête et conclusions.

Finalités et bases légales du traitement des données

Les finalités du traitement des données personnelles, y compris les transferts éventuels au sein de la CCB, sont les suivantes :

a. Promouvoir l'honnêteté, l'intégrité et l'éthique au sein de la CCB ;

b. Permettre le signalement via le système de rapportage interne de l'entreprise ;

c. Gérer les plaintes et traiter les signalements effectués par le biais du système de rapportage interne ;

d. Déterminer si une enquête est nécessaire et conduire/organiser cette enquête ;

e. Analyser les résultats des enquêtes concernant les signalements reçus ;

f. Déterminer les actions correctives à prendre à la suite d'un signalement et/ou d'une enquête connexe et mettre en œuvre les mesures pertinentes.

Nous traitons les données personnelles afin de gérer les signalements des lanceurs d'alerte et d'enquêter sur les allégations. Le traitement de vos données personnelles est dans ce contexte nécessaire pour respecter une obligation légale à laquelle nous sommes soumis.

Nous pouvons divulguer des données personnelles à la police ou aux autorités judiciaires à titre de preuve si des motifs raisonnables laissent présumer qu'un acte illégal ou un crime a été commis par vous dans le cadre de la procédure de signalement.

En outre, le traitement de certaines catégories spécifiques de données personnelles sera effectué uniquement si cela est nécessaire pour établir, exercer ou défendre des droits en justice, ou comme autorisé par la législation applicable en matière de protection des données.

Les suspicions d'infractions pénales seront uniquement traitées dans la mesure nécessaire pour la gestion des litiges propres à la CCB ou comme autrement autorisé par la loi.

Dans certaines circonstances, la CCB peut également traiter des données personnelles collectées via le système de signalement si cela est nécessaire pour se conformer à des obligations légales auxquelles la CCB est soumise.

Aucune décision automatisée, y compris le profilage, n'est réalisée.

Les données personnelles collectées ne seront pas utilisées à des fins de marketing direct.

Conservation et suppression des données

Les données collectées seront conservées uniquement pendant la durée nécessaire et proportionnée, conformément aux obligations légales :

- Suppression immédiate si le signalement est hors du champ d'application ou infondé.
- Suppression après clôture de l'enquête ou des actions engagées, sauf obligation légale contraire.
- Conservation pendant 10 ans correspondant au délai de prescription légale (article 2262bis de l'ancien Code civil).

Sécurité et confidentialité des données

La CCB et ses partenaires utilisent des mesures techniques et organisationnelles adaptées pour garantir la sécurité des données, conformément au RGPD. Les canaux de signalement sont sécurisés, avec un accès limité aux personnes autorisées uniquement.

Droits des personnes concernées

Dans certaines juridictions, comme l'Union européenne et l'Espace économique européen, une personne dont les données sont traitées (la «personne concernée») conformément à cette Politique dispose de plusieurs droits, résumés ci-dessous. Veuillez noter que l'exercice de ces droits est soumis à des exigences et conditions supplémentaires prévues par la législation applicable en matière de protection des données. En résumé, chaque personne dispose des droits suivants:

- Obtenir une confirmation de la CCB indiquant si les données personnelles de la personne concernée sont traitées, et demander l'accès à ces données, leurs finalités de traitement ainsi que les destinataires ou catégories de destinataires concernés.
- Obtenir de la CCB la rectification des données personnelles inexactes ou incomplètes concernant la personne concernée.
- Obtenir de la CCB l'effacement des données personnelles concernant la personne concernée, lorsque cela est légalement applicable.
- Demander à la CCB la limitation du traitement des données personnelles de la personne concernée.
- Recevoir les données personnelles fournies par la personne concernée à la CCB dans un format structuré, couramment utilisé et lisible par machine.

- S’opposer au traitement des données personnelles de la personne concernée par la CCB.

Si une personne concernée souhaite exercer ces droits ou obtenir des informations relatives à ses données, elle peut contacter le Service Juridique de la CCB à l’adresse suivante : stephanie.heyman@ccb.be.

Les personnes soumises à la réglementation européenne sur la protection des données personnelles et souhaitant déposer une plainte concernant le traitement décrit ici peuvent le faire auprès de l’autorité de protection des données compétente, en particulier dans l’État membre de leur résidence habituelle, de leur lieu de travail ou du lieu où une violation présumée des réglementations en matière de protection des données a eu lieu.

Pour de plus amples informations sur le traitement des données et les droits des individus, veuillez consulter la Déclaration de Confidentialité de la CCB.

7. COORDONNÉES DE CONTACT DU GESTIONNAIRE DE SIGNALEMENT

Pour toute question concernant la présente politique, les personnes intéressées peuvent s’adresser directement au gestionnaire de signalement de la CCB via les coordonnées suivantes :

Whistleblowing@cementirholding.it

8. MISES A JOUR

Cette politique sera mise à jour en cas de modification de la législation.

ANNEXE 1. LISTE DES AUTORITÉS BELGES COMPÉTENTES

En Belgique, l'information et le soutien aux lanceurs d'alerte sont fournis par l'intermédiaire de deux organismes :

- Le *Médiateur fédéral*, agissant en tant que coordinateur fédéral des signalements externes. Le Médiateur reçoit les alertes externes, vérifie leur recevabilité et transmet les informations à l'autorité compétente. Dans des cas exceptionnels, le Médiateur enquête également sur le fond et traite les cas de protection.

- *L'Institut fédéral de protection et de promotion des droits de l'homme (IFDH)*, fournissant aux lanceurs d'alerte un soutien professionnel, juridique et psychologique. Cela peut se faire par l'intermédiaire de l'Institut lui-même ou de tiers tels que des cabinets d'avocats ou des psychologues spécialisés dans ce domaine.

À ces deux instruments, s'ajoutent 24 autorités compétentes en fonction du domaine concerné par la violation signalée :

- Le Service public fédéral Economie, PME, Classes Moyennes et Energie
- Le Service public fédéral Finances
- Le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement
- Le Service public fédéral Mobilité et Transports
- Le Service public fédéral Emploi, Travail et Concertation sociale
- Le Service public de programmation Intégration Sociale, Lutte contre la Pauvreté, Economie Sociale et Politique des Grandes Villes
- L'Office National de Sécurité Sociale
- L'Agence fédérale de Contrôle nucléaire
- L'Agence fédérale des médicaments et des produits de santé
- L'Agence fédérale pour la sécurité de la chaîne alimentaire
- L'Autorité belge de la Concurrence
- L'Autorité de protection des données
- L'Autorité des services et marchés financiers
- La Banque nationale de Belgique
- Le Collège de supervision des réviseurs d'entreprises
- Le Service d'Information et de Recherche Sociale
- Les autorités visées à l'article 85 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces
- Le Comité national de sécurité pour la fourniture et la distribution d'eau potable
- L'Institut belge des services postaux et des télécommunications
- L'Institut National d'Assurance Maladie-Invalidité
- L'Institut National d'Assurances Sociales pour Travailleurs Indépendants
- L'Office National de l'Emploi
- Le Service autonome de Coordination Anti-Fraude (CAF)

- Le Contrôle de la Navigation

ANNEXE 2. LISTE NON EXHAUSTIVE DES FORMES DE REPRÉSAILLES INTERDITES (ART. 23 LOI DU 28 NOVEMBRE 2022)

Est interdite toute forme de représailles contre les personnes bénéficiant de la protection des lanceurs d'alerte, en ce compris les menaces de représailles et tentatives de représailles, notamment sous les formes suivantes :

- Suspension, mise à pied, licenciement ou mesures équivalentes ;
- Rétrogradation ou refus de promotion ;
- Transfert de fonctions, changement de lieu de travail, réduction de salaire, modification des horaires de travail ;
- Suspension de la formation ;
- Évaluation de performance ou attestation de travail négative ;
- Mesures disciplinaires imposées ou administrées, réprimande ou autre sanction, y compris une sanction financière ;
- Coercition, intimidation, harcèlement ou ostracisme ;
- Discrimination, traitement désavantageux ou injuste ;
- Non-conversion d'un contrat de travail temporaire en un contrat permanent, lorsque le travailleur pouvait légitimement espérer se voir offrir un emploi permanent ;
- Non-renouvellement ou résiliation anticipée d'un contrat de travail temporaire ;
- Préjudice, y compris les atteintes à la réputation de la personne, en particulier sur les réseaux sociaux, ou pertes financières, y compris la perte d'activité et la perte de revenu ;
- Mise sur liste noire sur la base d'un accord formel ou informel à l'échelle sectorielle ou de la branche d'activité, pouvant impliquer que la personne ne trouvera pas d'emploi à l'avenir au niveau du secteur ou de la branche d'activité ;
- Résiliation anticipée ou annulation d'un contrat relatif à la fourniture de biens ou la prestation de services ;
- Annulation d'une licence ou d'un permis ;
- Orientation vers un traitement psychiatrique ou médical.

WHISTLEBLOWER POLICY AND PROTECTION OF WHISTLEBLOWERS
("WHISTLEBLOWER POLICY")

- CCB -

December 2025

1. INTRODUCTION

"CCB" refers to: COMPAGNIE DES CIMENTS 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**

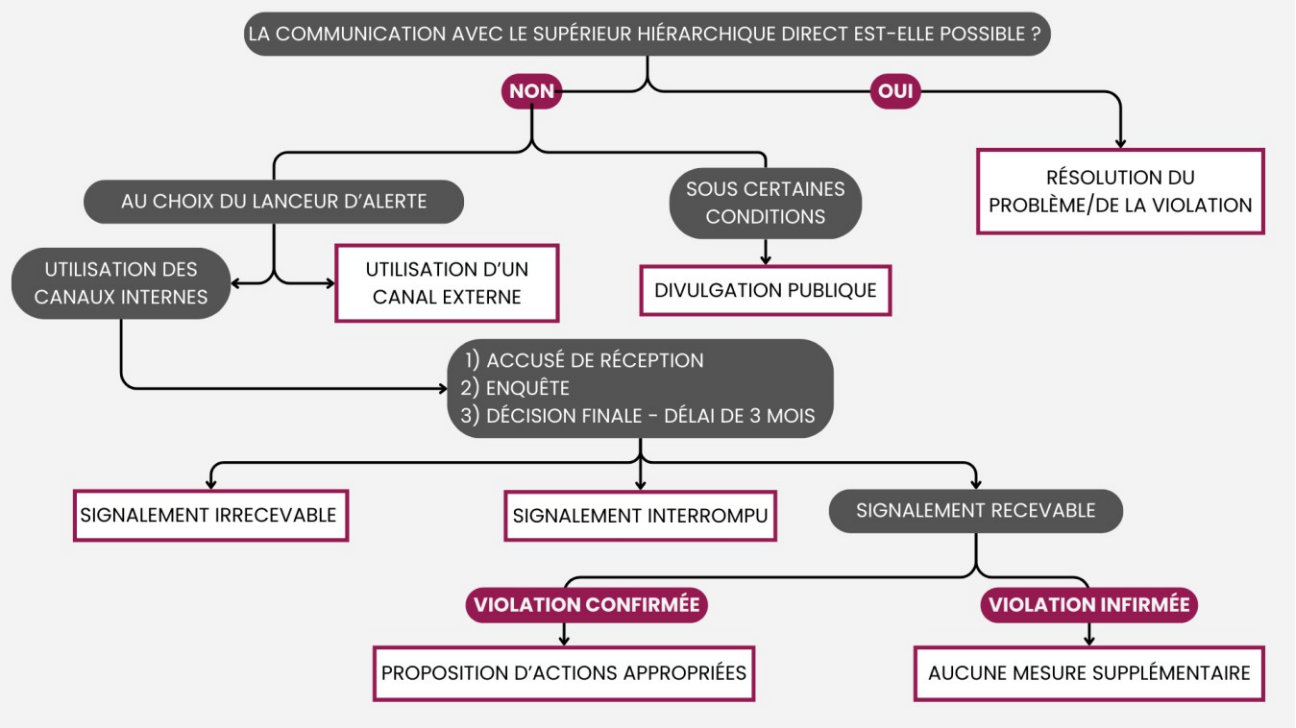
Personal disputes or disagreements between colleagues, unless they involve a violation of the scope of this policy, are not covered.

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 Public Service Finance
- The Federal Public Service for Public Health, Food Chain Safety and the Environment
- The Federal Public Service Mobility and Transport
- The Federal Public Service Employment, Labour and Social Dialogue
- The Public Service for Social Integration, Combating Poverty, Social Economy and Urban Policy
- The National Social Security Office
- The Federal Agency for Nuclear Control
- The Federal Agency for Medicines and Health Products
- The Federal Agency for the Safety of the Food Chain
- The Belgian Competition Authority
- The Data Protection Authority
- The Financial Services and Markets Authority
- The National Bank of Belgium
- The Supervisory Board of Company Auditors
- The Social Information and Research Service
- 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 National Security Committee for the Supply and Distribution of Drinking Water
- The Belgian Institute for Postal Services and Telecommunications
- The National Institute for Health and Disability
- The National Institute for Social Insurance for Self-Employed Persons
- The National Employment Office
- The Independent Anti-Fraud Coordination Service (CAF)

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.