

GUIDE DES POLITIQUES

POLITIQUE DU GROUPE SUR LE SIGNALEMENT DES ACTES RÉPRÉHENSIBLES

NUMÉRO: COMP-02GPT | DATE D'ENTRÉE EN VIGUEUR INITIALE: 01/01/2026

TABLE DES MATIÈRES :

- 1.0 Objectif de la Politique du groupe sur le signalement des actes répréhensibles dénonciation
- 2.0 Champ d'application et définitions
- 3.0 Protection des personnes effectuant le signalement
- 4.0 Qu'est-ce qui doit être signalé en vertu de la présente Politique?
- 5.0 À qui et comment dois-je signaler une situation?
- 6.0 Puis-je effectuer un signalement à l'extérieur de GPT?
- 7.0 Contenu des signalements
- 8.0 Confidentialité et anonymat
- 9.0 Évaluation et traitement des signalements
- 10.0 Conservation des signalements
- 11.0 Interdiction des représailles
- 12.0 Traitement des renseignements personnels
- 13.0 Supervision du système de signalement
- 14.0 Signalements aux autorités gouvernementales et réglementaires
- 15.0 Maintien et modification

ANNEXE A : Dispositions supplémentaires spécifiques à chaque pays (par région)

- Autriche
- République tchèque
- Danemark
- Allemagne
- Italie

1.0 OBJET DE LA POLITIQUE DU GROUPE SUR LE SIGNALEMENT DES ACTES RÉPRÉHENSIBLES

Grain & Protein Technologies (« GPT », le « Groupe ») s'engage à respecter les normes les plus élevées en matière d'intégrité, d'éthique et de conformité dans tous les aspects de ses activités. Le Groupe estime que la conduite éthique, la transparence et la responsabilité sont essentielles pour établir une relation de confiance avec ses employés, ses parties prenantes et les communautés au sein desquelles il exerce ses activités.

Conformément à cet engagement, GPT encourage toutes les personnes, tant au sein de GPT que parmi les tiers qui interagissent avec GPT dans un contexte professionnel, à signaler tout acte répréhensible présumé, toute irrégularité, toute violation de la loi ou des politiques internes. Ces signalements sont essentiels pour préserver l'intégrité et la réputation de GPT et pour garantir un milieu de travail sûr, équitable et conforme aux règles.

La présente Politique s'applique à l'échelle mondiale et est conçue pour se conformer aux lois applicables en matière de protection des personnes ayant effectué un signalement dans les juridictions où GPT exerce ses activités. Elle décrit ce qui peut être signalé, la manière dont les signalements sont soumis, les étapes procédurales suivies après la réception d'un signalement et les protections offertes aux personnes qui soulèvent des préoccupations.

En cas de conflit entre la présente Politique et la législation applicable, les dispositions légales prévaudront. La présente Politique s'applique à tous les membres du groupe GPT, mais en raison des différentes exigences légales locales, nous avons créé des annexes ou des politiques locales distinctes pour répondre à des besoins spécifiques et garantir la conformité aux réglementations nationales.

GPT interdit strictement toute mesure de représailles à l'encontre de toute personne qui signale de bonne foi un acte répréhensible ou qui participe à des enquêtes connexes. Ces personnes sont protégées contre la discrimination, le harcèlement ou tout traitement défavorable résultant de leur signalement, comme décrit plus en détail dans la présente Politique.

2.0 CHAMP D'APPLICATION ET DÉFINITIONS

Toute personne, y compris des parties externes, qui a obtenu des informations sur des infractions dans le cadre professionnel peut soumettre un signalement. Cela inclut notamment :

- les employés et dirigeants actuels et anciens de GPT,
- les travailleurs autonomes et les entrepreneurs fournissant des services au Groupe,
- les actionnaires et les membres des organes de GPT, y compris les membres non exécutifs;
- les bénévoles, les personnes en formation rémunérées ou non et les stagiaires;
- les personnes travaillant sous la supervision et la direction de contractants, de sous-traitants de deuxième rang et de fournisseurs;

- les partenaires commerciaux, y compris les clients, les fournisseurs, les conseillers, les mandataires et leurs employés, qui entretiennent ou ont entretenu une relation professionnelle avec GPT.

3.0 PROTECTION DES PERSONNES EFFECTUANT LE SIGNALEMENT

Aux fins de la présente politique, une personne effectuant un signalement est toute personne qui a des motifs raisonnables de soupçonner qu'un acte répréhensible, une situation irrégulière ou une violation de la loi ou d'une politique interne s'est produit en rapport avec GPT (« conduite à signaler ») et qui fait part de ses préoccupations par l'un des canaux de signalement décrits dans la présente Politique.

GPT s'engage à protéger les personnes qui effectuent des signalements de bonne foi et conformément à la présente Politique (« Signalement protégé »). Ces personnes ne doivent subir aucune forme de représailles, de discrimination, de harcèlement ou de désavantage du fait d'un signalement protégé.

L'identité de cette personne, ainsi que toute information permettant de déduire directement ou indirectement son identité, restera strictement confidentielle et ne sera pas divulguée sans son consentement explicite, sauf :

- lorsque la loi applicable l'exige;
- lorsque la divulgation est raisonnablement nécessaire pour enquêter sur le signalement ou pour se conformer à une procédure judiciaire, à condition que la confidentialité soit préservée dans toute la mesure permise par la loi; ou
- lorsque la divulgation est faite aux autorités réglementaires compétentes, aux organismes chargés de l'application de la loi ou à des conseillers professionnels liés par des obligations de confidentialité.

4.0 QU'EST-CE QUI DOIT ÊTRE SIGNALÉ EN VERTU DE LA PRÉSENTE POLITIQUE?

Tout fait qu'une personne estime raisonnablement constituer une violation des politiques, des normes éthiques ou des lois et règlements applicables de GPT doit être signalé conformément à la présente politique.

Voici quelques exemples d'actes à signaler :

- les violations des lois ou des règlements;
- les activités illégales, corrompues, frauduleuses ou irrégulières impliquant l'utilisation des fonds, des actifs ou des biens de GPT;
- les comportements illégaux ou criminels, y compris le vol, la vente ou la consommation de drogues, la violence ou les menaces de violence;
- les violations des politiques et procédures de GPT (y compris, mais sans s'y limiter, le Code de conduite);
- les comportements qui posent un risque important pour la santé publique, la sécurité ou l'environnement;

- les comportements malhonnêtes, contraires à l'éthique ou abusifs en milieu de travail;
- la fraude financière, la mauvaise gestion ou les irrégularités comptables;
- les comportements susceptibles de nuire à la situation financière, à la réputation ou à la confiance des parties prenantes de GPT;
- la négligence grave, la discrimination, le harcèlement ou les comportements abusifs;
- la dissimulation ou la tentative de dissimulation d'une acte répréhensible ou d'une situation irrégulière.

D'autres exemples, lorsque les lois locales en matière de signalement des actes répréhensibles l'exigent, sont détaillés dans les annexes spécifiques à chaque pays de la présente Politique.

Une personne peut également utiliser l'option « *Poser une question* » au lieu de soumettre un rapport officiel. Dans ce cas, GPT évaluera la question et y répondra. Si la situation semble relever des actes à signaler, GPT peut, à sa discrétion, reclasser la question en tant que rapport afin de s'assurer qu'elle soit traitée de manière appropriée conformément à la présente Politique.

Les actes à signaler doivent être distingués des griefs personnels liés au travail. Un grief personnel lié au travail désigne toute question liée à l'emploi actuel ou antérieur d'une personne qui l'affecte personnellement, mais qui n'indique pas de faute professionnelle, de violation de la loi ou des politiques internes.

Voici quelques exemples de griefs personnels liés au travail, sans que cette liste soit exhaustive :

- les conflits ou différends interpersonnels entre employés;
- les décisions relatives aux mutations, aux promotions ou aux évaluations de rendement;
- les mesures disciplinaires, les avertissements ou les décisions de licenciement.

Les signalements alléguant de la discrimination, du harcèlement, des représailles ou d'autres violations des lois sur l'emploi ne sont pas considérés comme des griefs personnels liés au travail et relèvent du champ d'application de la présente Politique. Les griefs personnels liés au travail, tels que décrits ci-dessus, qui n'impliquent pas d'actes à signaler sont généralement mieux traités par l'intermédiaire d'un supérieur hiérarchique direct, d'un responsable ou du service des ressources humaines, qui sont conçus pour traiter les préoccupations liées à l'emploi de manière équitable et rapide.

Si vous n'êtes pas certain qu'une situation relève de la présente politique, vous pouvez communiquer avec le service juridique et de conformité de GPT à l'adresse GPTCompliance@grainproteintech.com pour obtenir des conseils confidentiels sur la meilleure façon de procéder.

5.0 À QUI ET COMMENT DOIS-JE SIGNALER UNE SITUATION?

GPT a mis en place des canaux de signalement sécurisés et confidentiels pour la soumission des rapports.

Lorsque la directive sur la protection des personnes qui signalent des violations du droit de l'Union européenne (UE) 2019/1937 ou d'autres lois fédérales, provinciales ou locales applicables l'exigent, GPT a désigné des personnes responsables, qui sont autorisées à recevoir et à donner suite aux signalements conformément aux exigences légales.

Les employés et autres personnes admissibles qui souhaitent signaler un problème peuvent, au lieu de le faire directement auprès du directeur juridique et responsable de la conformité ou d'autres représentants de la direction, choisir de le signaler de manière confidentielle et, s'ils le souhaitent, de manière anonyme, par l'intermédiaire de GPT AlertLine. Aucune disposition de la présente Politique n'oblige les personnes à signaler un problème en interne avant de le signaler aux autorités gouvernementales ou réglementaires lorsque ce signalement est protégé par la loi applicable.

GPT AlertLine est géré par NAVEX, un service tiers indépendant retenu par GPT pour recevoir et consigner les signalements des employés et des parties externes et pour les transmettre en toute sécurité au personnel interne compétent en vue d'une évaluation et d'un suivi. Elle est exploitée en dehors du site Web et du réseau de l'entreprise afin de garantir la confidentialité et l'indépendance.

GPT AlertLine offre des options de signalement à la fois en ligne et par téléphone. Les liens et numéros de téléphone pertinents sont facilement accessibles sur le site Web de GPT ([GPT Alertline](#)) et sur le site Web de chaque entreprise du groupe GPT, comme indiqué dans les annexes spécifiques à chaque pays de la présente Politique.

Une fois connecté à l'AlertLine, la personne voulant effectuer un signalement peut utiliser les menus dédiés pour sélectionner le pays spécifique de l'entreprise concernée par le signalement avant de le soumettre.

Les canaux de signalement permettent de faire un signalement par écrit ou via GPT AlertLine. Sur demande, une personne souhaitant effectuer un signalement peut également demander à le faire lors d'une rencontre en personne avec la personne désignée. Une telle rencontre sera organisée dans un délai raisonnable après la demande, en conformité avec la loi applicable. Tout enregistrement audio nécessite le consentement explicite de la personne effectuant un signalement; à défaut, un compte rendu écrit ou un résumé est préparé et signé.

Si, pour quelque raison que ce soit et par quelque moyen que ce soit, un signalement relevant du champ d'application de la présente Politique est reçu en dehors des canaux de signalement désignés, la personne qui le reçoit doit immédiatement veiller à préserver la confidentialité de toutes les informations contenues dans le signalement.

Il lui est strictement interdit de divulguer l'identité de la personne qui a effectué le signalement, de la personne visée par celui-ci ou de toute autre personne mentionnée dans le rapport, ainsi que toute information pouvant mener directement ou indirectement à leur identification. Le

destinataire doit également conseiller à la personne qui a effectué le signalement de suivre la procédure de signalement officielle établie par la présente Politique et/ou de transmettre le rapport au service juridique et de conformité de GPT sans délai injustifié et, en tout état de cause, au plus tard sept (7) jours après sa réception. Une fois la confirmation de réception obtenue auprès du responsable du signalement désigné, toutes les copies ou traces du rapport (y compris les courriels ou les notes) doivent être supprimées de manière sécurisée afin de préserver la confidentialité totale et le respect de la protection des données.

6.0 PUIS-JE EFFECTUER UN SIGNALEMENT À L'EXTÉRIEUR DE GPT?

Les personnes souhaitant effectuer un signalement sont avant tout encouragées à utiliser les canaux de signalement internes mis en place par GPT.

Toutefois, dans certaines conditions définies par les lois et règlements applicables, elles peuvent également effectuer un signalement externe directement auprès des autorités compétentes, conformément aux règlements locaux et/ou internationaux pertinents.

Elles doivent se reporter aux annexes spécifiques à chaque pays de la présente Politique pour obtenir plus de détails sur les procédures de signalement externe et les autorités compétentes applicables à leur juridiction.

7.0 CONTENU DES SIGNALEMENTS

Afin de permettre à GPT de réagir et, le cas échéant, d'enquêter efficacement sur une allégation, les signalements doivent être factuels plutôt que spéculatifs et inclure autant d'informations spécifiques que possible. Cela permet à GPT d'évaluer correctement la nature, l'étendue et l'urgence de la situation signalée.

Pour une évaluation et une enquête adéquates, il est recommandé que le signalement comprenne, si possible, les informations suivantes :

- I. le contexte et description du problème, y compris les faits pertinents et les raisons du signalement
- II. le(s) nom(s) de la ou des personnes concernées ou impliquées
- III. le(s) nom(s) de tout témoin
- IV. la date, l'heure et le lieu de l'incident ou des incidents
- V. les détails ou toute copie des preuves ou des documents à l'appui.
- VI. les informations sur les fonds, actifs ou intérêts concernés.
- VII. une indication de la fréquence à laquelle l'incident s'est produit (le cas échéant)

Le mécanisme de signalement ne doit pas être utilisé à mauvais escient. Les signalements effectués de mauvaise foi, y compris ceux qui sont sciemment faux ou faits uniquement dans le but de nuire à une autre personne, sont strictement interdits. Un tel comportement peut entraîner des mesures disciplinaires ou, le cas échéant, des poursuites judiciaires, conformément aux lois de l'État concerné.

Toutefois, aucune mesure ne sera prise à l'encontre d'une personne qui soumet un signalement de bonne foi, même si les faits signalés s'avèrent par la suite incorrects ou non fondés.

GPT s'engage à protéger les personnes qui effectuent un signalement de bonne foi contre les représailles et à veiller à ce que le mécanisme de signalement soit utilisé de manière responsable et éthique.

8.0 CONFIDENTIALITÉ/ANONYMAT

Allégations que la personne a choisi de signaler ouvertement et de manière non anonyme

GPT promeut une culture d'ouverture et de transparence et encourage les personnes à faire part de leurs préoccupations ouvertement dans la mesure du possible. Cela facilite une évaluation, une enquête et un suivi plus efficaces de la situation.

Lorsqu'une personne a choisi de fournir son identité avec son signalement, GPT mettra tout en œuvre pour garantir la confidentialité de l'identité de cette personne, à moins qu'une telle divulgation ne soit requise par la loi, la réglementation ou une procédure judiciaire applicable. Dans tous les cas, les signalements seront traités conformément aux réglementations applicables en matière de protection des données et de signalement.

Allégations pour lesquelles la personne a choisi d'effectuer le signalement de manière anonyme

GPT reconnaît que, dans certaines situations, la personne peut se sentir plus à l'aise de signaler ses préoccupations de manière anonyme. La possibilité de soumettre des signalements anonymes dépend des lois et règlements applicables. Lorsque cela est autorisé, ces signalements seront évalués et, dans la mesure du possible, feront l'objet d'une enquête avec le même soin que les signalements non anonymes.

Les personnes qui signalent initialement de manière anonyme – ou qui, lorsque la loi applicable le permet, font une divulgation publique anonyme – resteront protégés en vertu de la présente Politique si leur identité est révélée ultérieurement, à condition qu'ils satisfassent aux autres conditions énoncées dans la présente Politique.

Toutefois, les personnes qui souhaitent effectuer un signalement anonyme doivent savoir que, dans certains cas, il peut être difficile de mener correctement une enquête approfondie sans connaître leur identité, en particulier lorsque des clarifications, des entrevues ou une vérification des faits sont nécessaires.

9.0 ÉVALUATION ET TRAITEMENT DES SIGNALEMENTS

GPT prend au sérieux tout signalement de violations présumées ou potentielles. Tous les signalements soumis par les canaux désignés seront traités de manière équitable, appropriée et sans retard injustifié. La personne effectuant un signalement recevra un accusé de réception dans les sept (7) jours suivant la date de réception. L'accusé de réception peut être retardé

lorsqu'une action immédiate est nécessaire pour préserver des preuves ou faire face à un risque imminent, conformément à la loi applicable.

GPT s'engage à assurer un suivi rigoureux et impartial de tous les signalements. Les enquêtes sont menées par du personnel qualifié ou, le cas échéant, par des experts et des consultants externes. GPT veille à ce que tous les faits pertinents soient recueillis, documentés et évalués de manière objective, dans le plein respect de ses obligations en matière de confidentialité et de protection des données. Pour cette raison, les exigences de confidentialité, de protection de la vie privée et de conformité aux obligations légales applicables peuvent limiter la mesure dans laquelle des détails spécifiques concernant l'enquête, les mesures prises ou les mesures qui en découlent peuvent être communiqués à la personne qui a fait le signalement. Toute information fournie à celle-ci concernant l'avancement ou le résultat de l'enquête doit être traitée de manière strictement confidentielle.

GPT fournira une réponse à la personne qui a fait le signalement dans un délai raisonnable, et en tout état de cause au plus tard trois (3) mois à compter de :

- la confirmation de réception du signalement
- l'expiration du délai de sept jours prévu pour l'accusé de réception, si aucun accusé de réception n'a été envoyé

GPT ne peut garantir que le résultat de l'enquête correspondra aux attentes ou au résultat souhaité par la personne qui a effectué le signalement. Cependant, elle s'engage pleinement à veiller à ce que toutes les préoccupations légitimes soient traitées de manière équitable, respectueuse et diligente.

Si, au cours de l'évaluation ou de l'enquête, il apparaît que les faits mentionnés dans le signalement pourraient constituer une infraction pénale, le responsable désigné du traitement des signalements, en accord avec les autres fonctions compétentes de l'entreprise et la direction du groupe, évaluera s'il y a lieu, quand et comment renvoyer l'affaire aux autorités judiciaires ou réglementaires compétentes, conformément aux lois et règlements locaux applicables.

10.0 CONSERVATION DES SIGNALEMENTS

Des copies écrites et électroniques de tous les signalements seront conservées de manière sécurisée conformément au calendrier documenté de conservation des données de GPT. Les signalements soumis via GPT AlertLine seront stockés électroniquement sur la plateforme de signalement sécurisée NAVEX.

Tous les dossiers et documents justificatifs ne seront conservés que pendant la durée nécessaire pour se conformer aux exigences légales et réglementaires applicables.

Le cas échéant, GPT anonymisera ou pseudonymisera tout renseignement personnel inclus dans un rapport dans un délai raisonnable à l'issue de l'enquête, conformément à toutes les lois applicables en matière de protection des données, y compris, le cas échéant, le Règlement général sur la protection des données (RGPD).

11.0 INTERDICTION DE REPRÉSAILLES

On entend par « représailles » tout acte ou omission, direct ou indirect, survenant dans un contexte professionnel, qui résulte d'un signalement interne ou externe, ou d'une divulgation publique effectuée en vertu de la présente Politique et qui cause ou est susceptible de causer un préjudice injustifié et inéquitable à la personne ayant fait le signalement.

Aucune personne qui soulève de bonne foi une préoccupation concernant une des situations visées par la présente Politique ne doit subir une forme quelconque de représailles. Toute personne qui se livre à des représailles peut faire l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement, quel que soit son poste ou son ancienneté.

GPT s'engage fermement à protéger les personnes qui font des signalement de bonne foi contre les représailles, le harcèlement ou tout autre traitement défavorable. Toutes les personnes qui effectuent un signalement seront traitées avec respect, dignité et confidentialité tout au long du processus.

Les représailles comprennent, sans s'y limiter, les menaces ou les tentatives de représailles et peuvent prendre la forme de :

- une suspension, une mise à pied, un congédiement ou des mesures équivalentes;
- une rétrogradation ou le refus d'une promotion;
- un transfert de fonctions, un changement de lieu de travail, une réduction de salaire ou une modification des horaires de travail;
- une évaluation de rendement négative ou une référence d'emploi défavorable;
- une mesure disciplinaire, une réprimande ou toute autre sanction, y compris des sanctions financières;
- la coercition, l'intimidation, le harcèlement ou l'ostracisme;
- la discrimination ou d'autres formes de traitement défavorable ou inéquitable;
- le fait de ne pas transformer un contrat de travail à durée déterminée en contrat à durée indéterminée alors qu'il existait une attente légitime;
- le non-renouvellement ou la résiliation anticipée d'un contrat de travail temporaire;
- l'atteinte à la réputation (y compris par le biais des médias sociaux) ou une perte financière, telle que la perte d'activité ou de revenus;
- l'inscription sur une liste noire au sein d'un secteur ou à l'échelle de l'industrie, qu'elle soit officielle ou officieuse;
- la résiliation anticipée ou l'annulation d'un contrat de biens ou de services;
- le retrait ou le refus d'une licence ou d'un permis;
- des orientations injustifiées vers des services psychiatriques ou médicaux.

Les mesures de protection prévues dans la présente Politique s'étendent également, le cas échéant, aux :

- facilitateurs, c'est-à-dire les personnes qui aident une personne dans le processus de signalement dans un contexte professionnel et dont l'aide doit rester confidentielle;

- tiers liés aux personnes ayant effectué le signalement et qui pourraient faire l'objet de représailles dans un contexte professionnel, tels que des collègues ou des proches; et
- personnes morales détenues par le dénonciateur, travaillant pour lui ou liées à lui à titre professionnel.

12.0 TRAITEMENT DES RENSEIGNEMENTS PERSONNELS

Tout traitement de renseignements personnels effectué conformément à la présente Politique, y compris la transmission ou l'échange de renseignements avec les autorités compétentes, doit respecter toutes les lois applicables en matière de protection des données. De même, les signalements impliquant des entités ou des personnes situées dans différentes juridictions peuvent être partagés entre les entités GPT concernées strictement aux personnes qui doivent en prendre connaissance et dans le respect des lois applicables en matière de protection des données et de signalement.

Les renseignements personnels qui ne sont manifestement pas pertinents pour le traitement d'un signalement spécifique ne doivent pas être recueillis ou, s'ils le sont accidentellement, doivent être supprimés sans délai injustifié.

GPT s'assurera que tous les renseignements personnels traités dans le cadre des signalements sont gérés de manière sécurisée, licite et proportionnée, leur accès étant strictement limité aux personnes autorisées à traiter ces renseignements à des fins légitimes.

13.0 SUPERVISION DU SYSTÈME DE SIGNALEMENT

L'efficacité de la présente Politique et le fonctionnement du système de signalement sont examinés périodiquement par le service juridique et de conformité de GPT. La présente Politique peut être mise à jour pour refléter les changements apportés aux lois et règlements applicables, à la structure organisationnelle ou aux normes de pratiques exemplaires.

14.0 SIGNALEMENTS AUX AUTORITÉS GOUVERNEMENTALES ET RÉGLEMENTAIRES

Ces procédures ne visent en aucun cas à limiter le droit des employés de signaler des violations présumées liées à des questions comptables ou d'audit aux autorités gouvernementales et réglementaires compétentes.

15.0 MAINTIEN ET MODIFICATION

Comme pour toute politique ou tout programme d'avantages sociaux, Grain & Protein Technologies se réserve le droit illimité, conformément à la loi, de réviser, réexaminer, interpréter, amender, modifier, suspendre ou mettre fin à tout ou partie de cette politique, de ce plan ou de ce programme à tout moment, avec ou sans préavis. Si une disposition de la présente politique entre en conflit avec une loi ou un règlement applicable ou contrevient à celui-ci, les dispositions de cette loi ou de ce règlement prévaudront. Aucune modification, suspension ou

cessation de la présente politique n'affectera les protections accordées aux personnes qui effectuent un signalement en vertu de la loi applicable.

**TOUTE QUESTION CONCERNANT LE PRÉSENT GUIDE DE POLITIQUE DOIT
ÊTRE ADRESSÉE AU SERVICE JURIDIQUE ET DE CONFORMITÉ.**

Description	Date d'entrée en vigueur	Nom et titre de la personne ayant apporté des modifications
Création de la politique	01/01/2026	Patrick Rykhus, directeur juridique



ANNEXE A : Dispositions supplémentaires spécifiques à certains pays (par région)

La présente annexe considère certains pays dans lesquels GPT exerce ses activités et qui disposent de lois relatives aux signalements pouvant s'appliquer à votre situation en tant que personne effectuant un signalement.

AUTRICHE

1.0 RÉSUMÉ

La présente annexe à la Politique vise à compléter la Politique de signalement des actes répréhensibles existante du groupe GPT en tenant compte des modifications législatives spécifiques qui ont été mises en œuvre en Autriche conformément à la directive sur la protection des personnes qui signalent des violations du droit de l'Union européenne (2019/1937) et à la réglementation locale [loi autrichienne sur la protection des lanceurs d'alerte (*HinweisgeberInnenenschutzgesetz* – « HSchG »)].

La présente annexe traite donc des différences d'application par rapport à la politique mondiale qui s'appliquent à l'entité de GPT située en Autriche, à savoir : **Cimbria Heid GmbH** (la « Société »), et contient des dispositions locales spécifiques concernant les entités autrichiennes et s'appliquant à toutes les personnes mentionnées à la section 2 de la Politique et uniquement dans la mesure où la HSchG est applicable.

2.0 DISPOSITIONS LOCALES SPÉCIFIQUES DÉROGEANT À LA POLITIQUE

2.1 Champ d'application selon la HSchG

La Loi autrichienne sur la protection des lanceurs d'alerte (HSchG) s'applique en cas d'infractions dans les domaines suivants :

- marchés publics;
- services financiers, produits financiers et marchés financiers, ainsi que la prévention du blanchiment d'argent et du financement du terrorisme;
- sécurité et conformité des produits;
- sécurité routière;
- protection de l'environnement;
- radioprotection et sûreté nucléaire;
- Sécurité des denrées alimentaires et aliments pour animaux, santé animale et bien-être des animaux;
- santé publique;
- protection des consommateurs;
- protection de la vie privée et des données personnelles ainsi que sécurité des réseaux et des systèmes d'information;
- prévention et répression des infractions pénales conformément aux articles 302 à 309 du Code criminel (StGB), Journal officiel fédéral I n° 60/1974;
- intérêts financiers de l'Union au sens de l'article 325 du Traité sur le fonctionnement de l'Union européenne (TFUE), par exemple l'utilisation abusive de fonds de l'UE;
- règles du marché intérieur au sens de l'article 26, paragraphe 2, du TFUE et règles de l'Union en matière de concurrence et d'aides d'État.

2.2 RENCONTRE EN PERSONNE

Si un lanceur d'alerte souhaite effectuer un signalement lors d'une rencontre en personne avec la personne désignée, cette rencontre doit avoir lieu dans les quatorze (14) jours civils suivant la demande.

2.3 DÉLAI DE RETOUR D'INFORMATION

GPT fournira un retour d'information au lanceur d'alerte concernant le signalement soumis dans un délai raisonnable, qui ne dépassera pas trois (3) mois à compter de la date de soumission du signalement.

3.0 CANAL DE SIGNALEMENT EXTERNE

Les lanceurs d'alerte sont avant tout encouragés à signaler leurs préoccupations en utilisant le canal interne. Toutefois, si cette option n'est pas possible ou appropriée, s'il n'est pas raisonnable de traiter les informations dans le système interne de signalement des actes répréhensibles ou si celui-ci s'est avéré infructueux ou sans possibilité raisonnable d'aboutir, un lanceur d'alerte peut soumettre un signalement à [l'Office fédéral de prévention et de lutte contre la corruption](#) (*Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung*).

L'article 15 (2) de la HschG désigne les canaux de signalement externes supplémentaires suivants :

- l'Autorité de surveillance des auditeurs (en vertu de la Loi sur la surveillance des auditeurs);
- l'Autorité comptable (en vertu de la Loi sur la comptabilité);
- l'Autorité fédérale de la concurrence (en vertu de la Loi sur la concurrence);
- l'Autorité des marchés financiers (en vertu de la Loi sur l'Autorité des marchés financiers);
- le Bureau de déclaration des opérations suspectes (en vertu de la Loi sur l'Office fédéral de police criminelle);
- les chambres des notaires (en vertu du Code des notaires);
- les Barreaux (en vertu du Statut disciplinaire des avocats et des avocats stagiaires);
- la Chambre des conseillers fiscaux et des auditeurs (en vertu de la Loi sur la profession de comptable public).

3.1 DIVULGATION PUBLIQUE

La divulgation publique n'est autorisée que dans les conditions prévues par la Loi autrichienne sur la protection des lanceurs d'alerte et toute divulgation en dehors de ces conditions peut entraîner la perte des protections.

Les lanceurs d'alerte peuvent effectuer un signalement externe dans les circonstances suivantes :

- Ils ont déjà effectué un signalement par les canaux de signalement internes et externes (ou uniquement à l'autorité compétente) mais aucune mesure appropriée n'a été prise ou n'est prévue dans les
 - I. trois (3) mois après la soumission du signalement par le canal interne prévu à cet effet; ou
 - II. trois (3) mois (ou jusqu'à six (6) mois dans des cas dûment justifiés) après que le signalement a été soumis par un canal de signalement externe.
- Ils ont des motifs raisonnables de croire que :
 - I. l'infraction visée dans le signalement peut entraîner une menace imminente ou évidente pour l'intérêt public, par exemple en cas de situation d'urgence ou de risque de préjudice irréversible; ou
 - II. ils ont des motifs raisonnables de croire que, si le signalement est effectué par l'intermédiaire du système de signalement externe, il existe un risque de représailles ou que le problème a peu de chances d'être traité efficacement. Cela pourrait être dû au fait que des preuves pourraient être dissimulées ou que des éléments pourraient être détruits, ou encore parce que l'autorité concernée n'est pas digne de confiance ou est liée au problème.

4.0 PERSONNES DÉSIGNÉES

La société a désigné les **personnes** suivantes pour gérer le canal de signalement interne; celles-ci ont reçu une formation spécifique et répondent aux exigences d'indépendance et d'impartialité :

- le gestionnaire mondial de la conformité (Global Compliance Manager)
- le gestionnaire juridique, EMEA (Legal Manager, EMEA)

Les personnes désignées agissent de manière autonome et sans conflit d'intérêts, garantissent la confidentialité par défaut et traitent les signalements conformément à la loi applicable et à la présente Politique.

En cas de conflit d'intérêts réel, potentiel ou perçu, la personne désignée s'abstiendra et le dossier sera rapidement réattribué à l'autre personne désignée (ou à un remplaçant dûment désigné) afin de garantir la continuité, la neutralité et un suivi rapide.

5.0 PROTECTION CONTRE LES REPRÉSAILLES ET CONFIDENTIALITÉ

Les représailles à l'encontre d'un lanceur d'alerte qui, de bonne foi, soulève une préoccupation concernant des questions couvertes par la HSchG (voir la section 1.0 ci-dessus) sont juridiquement invalides.

6.0 TRAITEMENT DES DONNÉES PERSONNELLES

Outre les dispositions légales énoncées à la section 11.0 de la Politique, le traitement des données personnelles relatives aux signalements est régi en Autriche par la section 8 de la

HSchG ainsi que par les dispositions de la Loi autrichienne sur la protection des données (*Datenschutzgesetz* – « DSG »).

6.1 DURÉE DE CONSERVATION

Les données personnelles doivent être conservées par GPT pendant cinq (5) ans après la clôture du dossier de signalement et, au-delà, aussi longtemps que nécessaire pour mener à bien les procédures administratives ou judiciaires déjà engagées ou les procédures d'enquête en vertu du Code de procédure pénale (*Strafprozessordnung* – « StPO »).

Les opérations de traitement effectivement réalisées, telles que les modifications, les consultations et les transmissions, doivent être consignées. Les données de journalisation relatives à ces processus doivent être conservées pendant trois (3) ans après l'expiration de l'obligation de conservation de cinq (5) ans.

RÉPUBLIQUE TCHÈQUE

1.0 RÉSUMÉ

La présente annexe à la Politique vise à compléter la politique de signalement des actes répréhensibles existante du groupe GPT en tenant compte des modifications législatives spécifiques qui ont été mises en œuvre en République tchèque conformément à la directive sur la protection des personnes qui signalent des violations du droit de l'Union européenne (2019/1937) et à la réglementation locale. La principale base juridique en matière de signalement des actes répréhensibles en République tchèque est la loi n° 171/2023 Coll. relative à la protection des lanceurs d'alerte (la « Loi tchèque sur la protection des lanceurs d'alerte »).

La présente annexe à la Politique traite donc des différences d'application par rapport à la politique mondiale qui s'appliquent à l'entité de GPT située en République tchèque, à savoir : Cimbria HMD, s.r.o. (la « Société »).

2.0 CHAMP D'APPLICATION ET ENTITÉS COUVERTES

La présente annexe s'applique non seulement à tous les dirigeants, administrateurs, employés et travailleurs temporaires (collectivement, les « collaborateurs ») et à tous les mandataires de la société, y compris, mais sans s'y limiter, les contractants, les consultants et les représentants (collectivement, les « personnes associées »), mais également :

- aux actionnaires et aux détenteurs de droits de vote à l'assemblée générale de la société;
- aux membres de l'organe d'administration, de direction ou de surveillance de la société;
- au personnel externe et occasionnel de la société;
- aux cocontractants de la société et à leurs sous-traitants;
- aux bénévoles ou aux stagiaires;
- aux personnes qui signalent ou divulguent publiquement des informations sur des infractions acquises dans le cadre d'une relation de travail avec la société qui a depuis pris fin; et
- aux personnes dont la relation de travail avec la société n'a pas encore débuté, dans les cas où des informations sur des infractions ont été obtenues au cours du processus de recrutement ou d'autres négociations précontractuelles en République tchèque.

3.0 DÉFINITIONS

Les définitions des termes « lanceur d'alerte », « personne effectuant un signalement » et « d'actes à signaler » au sens de la présente Politique sont étendues en vertu de la loi tchèque comme suit :

- Lanceur d'alerte (divulgateur protégé) : est défini comme « une personne physique qui signale une infraction potentielle qui s'est produite ou est sur le point de se produire et

qui présente les caractéristiques d'une infraction pénale ou d'un délit, ou qui enfreint la loi sur le signalement des actes répréhensibles ou une autre réglementation légale, ou qui porte atteinte aux intérêts financiers de l'Union européenne ou de son marché intérieur »;

- Acte à signaler (comportement inapproprié) : inclut, en plus des définitions de la Politique mondiale, une telle infraction.

La divulgation de faits, d'informations ou de documents susceptibles de menacer la sécurité nationale, liés aux activités des services de renseignement ou dont la notification constituerait une violation de la protection de la confidentialité du clergé dans l'exercice du secret de la confession, est interdite et ne relève pas du champ d'application de la Politique mondiale ni de la présente annexe à la Politique.

4.0 CANAUX DE SIGNALEMENT

Les lanceurs d'alerte peuvent soumettre des signalements par :

- un canal de signalement interne
- un signalement externe au ministère de la Justice de la République tchèque
- la divulgation publique (autorisée uniquement dans des conditions spécifiques prévues par la loi)

4.1 CANAL DE SIGNALEMENT INTERNE

Les lanceurs d'alerte pourront soumettre des rapports internes par les canaux indiqués dans la Politique mondiale, facilement accessible via un lien disponible sur le site Web de la société : [GPT Alertline](#).

Une fois connecté au portail, le lanceur d'alerte peut utiliser les menus prévus à cet effet pour sélectionner le pays de la société du Groupe concernée par le signalement avant de l'envoyer.

Le canal interne permet aux lanceurs d'alerte :

- de soumettre des signalements par tout moyen (écrit ou oral). Si un signalement est fait oralement, il peut se faire par téléphone ou, si le lanceur d'alerte le demande, par vidéoconférence ou lors d'une rencontre en personne organisée dans un délai raisonnable, mais au plus tard quatorze (14) jours après la date de la demande.
- Tout enregistrement audio nécessite le consentement du lanceur d'alerte. À défaut, un procès-verbal écrit est rédigé et signé. La personne désignée doit donner au lanceur d'alerte la possibilité de commenter le compte rendu écrit du signalement ou la transcription de l'enregistrement audio. Les commentaires du lanceur d'alerte doivent être joints à l'enregistrement ou à la transcription.
- de faire un signalement de manière anonyme, s'il le juge nécessaire.

Le lanceur d'alerte sera informé par écrit de la réception du rapport dans les sept (7) jours suivant sa réception. La personne désignée maintiendra la communication avec le lanceur d'alerte et pourra lui demander des renseignements supplémentaires.

La personne désignée est tenue d'évaluer si le signalement est fondé et d'informer le lanceur d'alerte par écrit du résultat de cette évaluation dans les trente (30) jours suivant la date de réception du signalement. Dans les cas complexes sur le plan factuel ou juridique, ce délai peut être prolongé de 30 jours au maximum, mais pas plus de deux fois. La personne désignée est tenue d'informer par écrit le lanceur d'alerte de la prolongation du délai et des motifs de cette prolongation avant l'expiration du délai initial.

Dans le cadre du suivi, la personne désignée doit informer le lanceur d'alerte du résultat de l'examen, qui peut prendre l'une des formes suivantes :

- (I) la confirmation que la soumission ne constitue pas un signalement au sens de la Loi tchèque sur la protection des lanceurs d'alerte; dans ce cas, la personne désignée en informe par écrit le lanceur d'alerte sans délai injustifié;
- (II) la clôture/archivage, lorsque les allégations s'avèrent inexactes ou non fondées, ou lorsque le signalement est devenu sans objet; dans ce cas, la personne désignée doit, sans délai injustifié, informer par écrit le lanceur d'alerte que, sur la base des faits exposés dans le signalement et des circonstances dont elle a connaissance, aucun soupçon de comportement illégal n'a été établi, ou que le signalement s'est avéré fondé sur des informations inexactes et doit la personne désignée également informer le lanceur d'alerte de son droit d'effectuer un signalement auprès d'une autorité publique; ou
- (III) la confirmation que le signalement a été jugé fondé et que des mesures appropriées visant à prévenir ou à remédier à la situation illégale ont été proposées aux organes ou autorités compétents. Les informations relatives aux mesures finalement adoptées seront communiquées par écrit au lanceur sans délai injustifié.

La personne désignée conservera les signalements et les documents connexes, y compris les données personnelles, pendant une période de cinq (5) ans à compter de la date de réception du signalement.

4.2 CANAL DE SIGNALEMENT EXTERNE

Les lanceurs ont le droit d'effectuer un signalement au ministère de la Justice de la République tchèque.

Les informations relatives au signalement au ministère de la Justice de la République tchèque sont disponibles sur le site Web : <https://oznamovatel.justice.cz/>

4.3 DIVULGATION PUBLIQUE

La divulgation publique n'est autorisée que dans les conditions prévues par la Loi tchèque sur la protection des lanceurs d'alerte. Une divulgation publique en dehors des conditions énumérées peut entraîner la perte des protections.

Les lanceurs d'alerte peuvent effectuer un signalement externe dans les circonstances suivantes :

- Ils ont déjà effectué un signalement par le biais du canal interne de signalement et auprès du Ministère, ou uniquement auprès du Ministère, et aucune mesure appropriée n'a été prise dans les délais fixés par la Loi tchèque sur la protection des lanceurs d'alerte. En particulier, la personne désignée n'a pas évalué le bien-fondé du signalement en vertu de l'article 12(3) de la Loi tchèque sur la protection des lanceurs d'alerte, la société n'a pas pris d'autres mesures appropriées pour prévenir ou remédier à la situation illégale en vertu de l'article 12(5) de la Loi tchèque sur la protection des lanceurs d'alerte ou un fonctionnaire en vertu de l'article 13 de la Loi tchèque sur la protection des lanceurs d'alerte n'a pas évalué le signalement en vertu de l'article 17(1) de la Loi tchèque sur la protection des lanceurs d'alerte;
- Ils ont des motifs raisonnables de croire que l'infraction mentionnée dans le signalement peut entraîner une menace imminente ou évidente pour l'ordre ou la sécurité intérieure, la vie ou la santé, l'environnement ou tout autre intérêt public, ou causer un préjudice irréparable.
- Ils ont des motifs raisonnables de croire que, si le signalement est effectué par le biais du système de signalement externe, il existe un risque accru, compte tenu des circonstances de l'affaire, qu'eux-mêmes ou une personne visée à l'article 4(2)(a) à (h) de la Loi tchèque sur la protection des lanceurs d'alerte fassent l'objet de représailles ou que la procédure prévue au Titre III de la Loi tchèque sur la protection des lanceurs d'alerte soit compromise.

5.0 PERSONNES DÉSIGNÉES

La société a désigné les personnes suivantes pour gérer le canal de signalement interne ; celles-ci ont reçu une formation spécifique et répondent aux exigences d'indépendance et d'impartialité :

- le gestionnaire mondial de la conformité (Global Compliance Manager)
- le gestionnaire juridique, EMEA (Legal Manager, EMEA)

Les personnes désignées agissent de manière autonome et sans conflit d'intérêts, garantissent la confidentialité par défaut et traitent les signalements conformément à la loi applicable et à la présente Politique.

En cas de conflit d'intérêts réel, potentiel ou perçu, la personne désignée doit s'abstenir et le dossier sera rapidement réattribué à l'autre personne désignée (ou à un remplaçant dûment désigné) afin de garantir la continuité, la neutralité et un suivi rapide.

6.0 PROTECTION CONTRE LES REPRÉSAILLES ET CONFIDENTIALITÉ

Le principe de non-représailles s'applique non seulement aux collaborateurs, aux personnes associées et aux autres sujets visés à la section 2, qui effectuent un signalement en vertu de la Politique mondiale et de la présente annexe, mais également aux facilitateurs, tels que définis précédemment dans la Politique mondiale, aux tiers liés aux lanceurs d'alerte tels que les collègues, anciens collègues, consultants et membres de la famille, ainsi qu'aux entités juridiques dont le lanceur d'alerte est propriétaire, pour lesquelles il travaille ou auxquelles il est lié dans un contexte professionnel.

La législation de la République tchèque établit une liste exhaustive d'actions ou d'omissions pouvant être considérées comme des mesures de représailles qui comprennent, sans s'y limiter, le licenciement, la mise à pied, les mesures disciplinaires, la réduction de salaire, le transfert de lieu de travail, le refus d'accorder un perfectionnement professionnel, l'exigence d'un rapport médical, tout type de discrimination, une évaluation de rendement négative, le harcèlement, la non-conversion d'un contrat à durée déterminée en contrat à durée indéterminée, etc.

DANEMARK

1.0 RÉSUMÉ

La présente annexe relative à la politique danoise vise à compléter la Politique de signalement des actes répréhensibles existante du groupe GPT et fournit des directives concernant la mise en œuvre de la Loi danoise sur la protection des lanceurs d'alerte (la « Loi ») en ce qui concerne Cimbria A/S (la « Société »).

La présente Politique de signalement du Groupe, ainsi que la présente annexe, fournissent des informations aux lanceurs d'alerte conformément à la Loi.

2.0 CANAUX DE SIGNALEMENT

Les lanceurs d'alerte peuvent soumettre leurs signalements par :

- un canal de signalement interne
- un canal de signalement externe
- la divulgation publique

2.1 CANAL DE SIGNALEMENT INTERNE

Les lanceurs d'alerte pourront soumettre des rapports internes par les canaux indiqués dans la Politique mondiale, facilement accessible via un lien disponible sur le site Web de la Société : [GPT Alertline](#).

Une fois connecté au portail, le lanceur d'alerte peut utiliser les menus dédiés pour sélectionner le pays de la société du Groupe concernée par le signalement avant de le soumettre.

Le canal interne permet aux lanceurs d'alerte :

- de soumettre des signalements par tout moyen (écrit ou oral). Si un signalement est fait oralement, il peut se faire par téléphone ou, à la demande du lanceur d'alerte, par vidéoconférence ou lors d'une rencontre en personne organisée dans un délai raisonnable. Tout enregistrement audio nécessite le consentement du lanceur d'alerte. À défaut, un compte rendu écrit est rédigé et signé.
- de signaler de manière anonyme, s'il le juge nécessaire.

Le lanceur d'alerte sera informé par écrit de la réception du signalement dans les sept (7) jours suivant sa réception. La personne désignée maintiendra la communication avec le lanceur d'alerte et pourra lui demander des renseignements supplémentaires.

La personne désignée fournit une réponse de suivi dans un délai de trois (3) mois à compter de la date d'accusé de réception du signalement ou, en l'absence d'accusé de réception, dans un délai de trois mois à compter de l'expiration du délai de sept jours ouvrables suivant le dépôt du signalement. Dans le cadre de ce suivi, la personne désignée informe le lanceur d'alerte de l'issue du signalement, si possible, à savoir : (i) la clôture/l'archivage (lorsque les allégations s'avèrent inexacts ou non fondées, ou lorsque le signalement est devenu sans objet) ou (ii) la

confirmation que le signalement a été jugé fondé et a été transmis aux organismes/autorités compétents. Toutefois, ces informations doivent être fournies au lanceur d'alerte conformément à la législation danoise, notamment aux obligations légales de confidentialité ainsi qu'à la réglementation sur la protection des données. Si les mesures ou le résultat n'ont pas été déterminés dans le délai de trois (3) mois, le lanceur d'alerte en sera informé et recevra des renseignements sur le retour d'information attendu.

Au cours de la phase d'enquête relative au signalement, des conseillers externes peuvent être impliqués dans le traitement du dossier. Selon la nature du cas, celui-ci peut être transmis à la police pour une enquête plus approfondie.

Si l'identité du lanceur d'alerte a été révélée dans le cadre du signalement et qu'une procédure judiciaire est engagée contre la personne visée par le signalement, le lanceur d'alerte peut être cité à comparaître en tant que témoin dans le cadre de la procédure judiciaire.

2.2 CANAL DE SIGNALEMENT EXTERNE – AUTORITÉ NATIONALE DANOISE

Le signalement peut également être effectué via un canal de signalement externe et indépendant mis en place par l'Autorité danoise de protection des données (« *Datatilsynet* ») pour le traitement des signalements concernant des violations du droit de l'Union européenne, relevant du champ d'application de la directive sur les lanceurs d'alerte et ne concernant donc pas d'autres violations graves de la loi ou d'autres questions graves.

Il est recommandé de soumettre un signalement via le canal interne de la société lorsque la violation peut être traitée efficacement en interne et que le lanceur d'alerte estime qu'il n'y a aucun risque de représailles. Toutefois, il convient de souligner que le signalement via le canal interne ou externe est facultatif, à condition que le signalement concerne les violations susmentionnées du droit de l'Union européenne.

Lien vers le site de signalement externe : <https://whistleblower.dk/indberet>

2.3 DIVULGATION PUBLIQUE

La divulgation publique n'est autorisée que dans les conditions prévues à l'article 5(2) de la Loi (p. ex., recours préalable aux canaux internes et/ou externes sans réponse adéquate ou risque concret de représailles ou de danger pour l'intérêt public). Une divulgation publique en dehors de ces conditions peut entraîner la perte des protections.

3.0 PERSONNES DÉSIGNÉES

La société a désigné les personnes suivantes pour gérer le canal de signalement interne; celles-ci ont reçu une formation spécifique et répondent aux exigences d'indépendance et d'impartialité :

- le gestionnaire mondial de la conformité (Global Compliance Manager)
- le gestionnaire juridique, EMEA (Legal Manager, EMEA)

Les personnes désignées agissent de manière autonome et sans conflit d'intérêts, garantissent la confidentialité par défaut et traitent les signalements conformément à la loi applicable et à la présente Politique.

En cas de conflit d'intérêts réel, potentiel ou perçu, la personne désignée s'abstiendra et le dossier sera rapidement réattribué à l'autre personne désignée (ou à un remplaçant dûment désigné) afin de garantir la continuité, la neutralité et un suivi rapide.

4.0 PROTECTION CONTRE LES REPRÉSAILLES ET CONFIDENTIALITÉ

La protection contre les représailles est assurée conformément aux règles énoncées dans la Loi, plus précisément aux articles 5 à 8. En substance, un lanceur d'alerte ne doit pas faire l'objet de représailles, y compris de menaces ou de tentatives de représailles, du fait d'avoir fait un signalement ou une divulgation publique conformément à la Loi. De plus, on ne doit pas empêcher ou tenter d'empêcher le lanceur d'alerte de faire un signalement.

La protection s'applique aux lanceurs d'alerte qui effectuent des signalements internes et externes ainsi que des divulgations publiques. Toutefois, pour les divulgations publiques, la protection s'applique dans les cas suivants :

- Lorsque le lanceur d'alerte qui procède à la divulgation publique a d'abord effectué un signalement interne et externe ou un signalement externe uniquement, sans que des mesures appropriées aient été prises en réponse au signalement dans le délai applicable.
- Lorsque le lanceur d'alerte qui effectue la divulgation publique a des motifs raisonnables de croire que l'infraction peut présenter un danger imminent ou manifeste pour l'intérêt public
- Lorsque le lanceur d'alerte qui procède à la divulgation publique a des motifs raisonnables de croire que le fait de signaler l'infraction à un mécanisme externe de signalement comporte un risque de représailles ou que, en raison des circonstances particulières de l'affaire, il y a peu de chances que l'infraction soit traitée efficacement.

De plus, la protection ne s'applique que si le lanceur d'alerte a des motifs raisonnables de croire que les renseignements signalés ou divulgués étaient exacts au moment du signalement ou de la divulgation, et que ces renseignements relevaient du champ d'application de la Loi.

En matière de confidentialité, la Loi stipule que les personnes désignées constituant l'entité interne de signalement qui gèrent le canal interne sont tenues à la confidentialité concernant les informations contenues dans les signalements. Cette obligation de confidentialité s'applique de même aux personnes qui, par le biais de la divulgation, ont connaissance de ces informations. Une obligation de confidentialité s'applique également aux employés non autorisés des autorités gérant des mécanismes externes de signalement qui, par inadvertance, ont connaissance de ces informations concernant les signalements.

5.0 CONSERVATION DES DONNÉES PERSONNELLES

Les signalements et les données personnelles connexes concernant les employés seront conservés pendant la durée strictement nécessaire à leur traitement et, en règle générale, pendant cinq (5) ans après la fin de la relation de travail, conformément à l'article 4(1) de la Loi danoise sur la prescription, sauf si des circonstances particulières imposent une période de conservation plus longue, par exemple en raison de procédures judiciaires en cours ou de la perspective de telles procédures.

Les signalements et les données personnelles connexes concernant les clients ou d'autres tiers seront conservés pendant la durée strictement nécessaire à leur traitement et, généralement à des fins de documentation, pendant 3 ans conformément à l'article 3(1) de la Loi danoise sur la prescription, sauf si des circonstances particulières imposent une période de conservation plus longue, par exemple en raison de procédures judiciaires en cours ou de la perspective de telles procédures.

ALLEMAGNE

1.0 RÉSUMÉ

La présente annexe à la Politique vise à compléter la Politique de signalement des actes répréhensibles existante du groupe GPT en tenant compte des modifications législatives spécifiques qui ont été mises en œuvre en Allemagne conformément à la directive sur la protection des personnes qui signalent des violations du droit de l'Union européenne (2019/1937) et à la réglementation locale. En Allemagne, la protection des lanceurs d'alerte est régie par la loi sur la protection des lanceurs d'alerte « *Gesetz zum Schutz von Hinweisgebenden Personen* », également appelée « *Hinweisgeberschutzgesetz* » ou, en abrégé, « *HinSchG* ».

La présente annexe à la Politique traite donc des différences d'application par rapport à la politique mondiale qui s'appliquent à l'entité de GPT située en Allemagne, à savoir GrainProteinTech Climate Control Air Treatment Germany GmbH (la « Société »).

La présente annexe fournit des informations aux lanceurs d'alerte conformément à l'article 5(e) du décret législatif 24/2023. En cas de conflit entre la Politique et la présente annexe, cette dernière prévaut pour l'Allemagne.

2.0 CHAMP D'APPLICATION ET ENTITÉS COUVERTES

La présente annexe à la Politique s'applique non seulement à tous les dirigeants, administrateurs, employés et travailleurs temporaires (collectivement, les « Collaborateurs ») et à tous les mandataires de la société, y compris, mais sans s'y limiter, les contractants, les consultants et les représentants (collectivement, les « Personnes associées »), mais également :

- aux actionnaires et aux détenteurs de droits de vote à l'assemblée générale de la société;
- aux membres de l'organe d'administration, de direction ou de surveillance de la société;
- au personnel externe et occasionnel de la société;
- aux cocontractants de la société et à leurs sous-traitants;
- à ceux qui signalent ou divulguent publiquement des informations sur des violations acquises dans le cadre d'une relation de travail avec la Société qui a depuis pris fin; et
- aux personnes dont la relation de travail avec la société n'a pas encore débuté, dans les cas où des informations sur des infractions ont été obtenues au cours du processus de recrutement ou d'autres négociations précontractuelles en Allemagne.

3.0 DÉFINITIONS

Conformément à la HinSchG, les définitions des termes « lanceurs d'alerte » et « actes à signaler » dans le cadre de la présente Politique sont étendues en vertu du droit allemand comme suit :

- Lanceur d'alerte (divulgateur protégé) : s'entend d'une « personne physique qui a obtenu des informations sur des infractions dans le cadre de ses activités professionnelles et qui divulgue ces informations aux organismes de signalement prévus par la Loi allemande

sur la protection des lanceurs d'alerte ». Les infractions sont des omissions ou des actes illégaux qui relèvent des domaines du droit visés par la directive sur le signalement ou qui constituent un abus parce qu'ils vont à l'encontre de l'objectif ou de la finalité de la directive.

- Les actes à signaler (actes inappropriés) comprennent, outre les définitions figurant dans la Politique mondiale, ces infractions.

La divulgation de faits, d'informations ou de documents provenant des services de renseignement ou susceptibles de nuire à la sécurité nationale ou à des intérêts de sécurité essentiels, ainsi que les divulgations en violation d'une obligation de confidentialité concernant des informations classifiées, le secret des délibérations judiciaires ou le secret professionnel des avocats ou des professionnels de la santé, sont interdites et ne relèvent pas du champ d'application de la Politique mondiale ou de la présente annexe à la Politique.

4.0 CANAUX DE SIGNALEMENT

Les lanceurs d'alerte peuvent soumettre des signalements par le biais :

- d'un canal de signalement interne
- d'un signalement externe auprès d'autorités externes

4.1 CANAL DE SIGNALEMENT INTERNE

Les lanceurs d'alerte pourront soumettre des signalements internes par les canaux indiqués dans la Politique mondiale, facilement accessible via un lien disponible sur le site Web de la Société : [GPT Alertline](#).

Une fois connecté au portail, le lanceur d'alerte peut utiliser les menus dédiés pour sélectionner le pays de la société du Groupe concernée par le signalement avant de le soumettre.

Le canal interne permet aux lanceurs d'alerte :

- de soumettre des signalements par tout moyen (écrit ou oral). Si un signalement est fait oralement, il peut se faire par téléphone ou, à la demande du lanceur d'alerte, par vidéoconférence ou lors d'une rencontre en personne organisée dans un délai raisonnable. Tout enregistrement audio nécessite le consentement du lanceur d'alerte. À défaut, un compte rendu écrit est rédigé et signé;
- de signaler de manière anonyme, s'il le juge nécessaire.

Le lanceur d'alerte sera informé par écrit de la réception du signalement dans les sept (7) jours suivant sa réception. La personne désignée restera en communication avec le lanceur d'alerte et pourra lui demander des renseignements supplémentaires.

La personne désignée fournit une réponse de suivi dans les trois (3) mois suivant la date d'accusé de réception du signalement ou, si aucun accusé de réception n'est reçu, dans les trois mois suivant l'expiration du délai de sept jours ouvrables après le signalement. Dans le cadre du suivi, la personne désignée informera le lanceur d'alerte de l'issue du signalement, à savoir : (i) la clôture/l'archivage (lorsque les allégations s'avèrent inexacts ou non fondées ou lorsque

le signalement est devenu sans objet) ou (ii) la confirmation que le signalement a été jugé fondé et a été transmis aux organismes/autorités compétents.

Les signalements et les données personnelles qui s'y rapportent seront conservés pendant la durée strictement nécessaire à leur traitement et, en tout état de cause, pendant une durée maximale de cinq (5) ans à compter de la communication du résultat de la procédure.

4.2 CANAL DE SIGNALEMENT EXTERNE - AUTORITÉS NATIONALES ALLEMANDES

Les lanceurs d'alerte peuvent effectuer un signalement externe auprès des autorités suivantes :

- Bureau de signalement externe de l'État fédéral auprès de l'Office fédéral de la justice
[BfJ - Service des lanceurs d'alerte \(bundesjustizamt.de\)](https://www.bundesjustizamt.de)
- *Bundeskartellamt* – pour les infractions relatives au droit de la concurrence et à la Loi sur les marchés numériques
https://www.bundeskartellamt.de/DE/Aufgaben/Kartelle/HinweiseAufKartellverstoesse/hinweiseaufverstoesse_node.html

5.0 PERSONNES DÉSIGNÉES

La Société a désigné les personnes suivantes pour gérer le canal de signalement interne. Celles-ci ont reçu une formation spécifique et répondent aux exigences d'indépendance et d'impartialité :

- le gestionnaire mondial de la conformité (Global Compliance Manager)
- le gestionnaire juridique, EMEA (Legal Manager, EMEA)

Les personnes désignées agissent de manière autonome et sans conflit d'intérêts, garantissent la confidentialité par défaut et traitent les signalements conformément à la loi applicable et à la présente Politique.

En cas de conflit d'intérêts réel, potentiel ou perçu, la personne désignée s'abstiendra et le dossier sera rapidement réattribué à l'autre personne désignée (ou à un remplaçant dûment désigné) afin de garantir la continuité, la neutralité et un suivi rapide.

6.0 PROTECTION CONTRE LES REPRÉSAILLES ET CONFIDENTIALITÉ

Le principe de non-représailles s'applique non seulement aux collaborateurs, aux personnes associées et aux autres personnes visées à la section 2 qui effectuent un signalement en vertu de la Politique mondiale et de la présente annexe, mais également aux facilitateurs, tels que définis précédemment dans la Politique mondiale, aux tiers liés aux lanceurs d'alerte, tels que les collègues, anciens collègues, consultants et membres de la famille, ainsi qu'aux personnes morales dont le lanceur d'alerte est propriétaire, pour lesquelles il travaille ou avec lesquelles il entretient des liens dans un contexte professionnel.



Les représailles peuvent inclure, sans s'y limiter, le licenciement, la mise à pied, des mesures disciplinaires, une réduction de salaire, un transfert de lieu de travail, toute forme de discrimination, une évaluation de rendement négative, du harcèlement, la non-conversion d'un contrat à durée déterminée en contrat à durée indéterminée, etc.

ITALIE

1.0 RÉSUMÉ

La présente annexe à la Politique vise à compléter la politique de signalement des actes répréhensibles existante du groupe GPT en tenant compte des modifications législatives spécifiques qui ont été mises en œuvre en Italie conformément à la directive sur la protection des personnes qui signalent des violations du droit de l'Union européenne (2019/1937) et à la réglementation locale (décret législatif n° 24 du 10 mars 2023, transposant la directive sur le signalement en Italie, et les lignes directrices de l'Autorité nationale anticorruption).

La présente annexe à la Politique traite donc des différences d'application par rapport à la politique mondiale qui s'appliquent aux entités de GPT situées en Italie, à savoir : Cimbria S.r.l., GrainProteinTech Climate Control Air Treatment S.p.A., Tecno Poultry Equipment S.p.A. (chacune étant la « Société »).

La présente annexe fournit des informations aux lanceurs d'alerte conformément à l'article 5(e) du décret législatif 24/2023. En cas de conflit entre la Politique et la présente annexe, cette dernière prévaut pour l'Italie.

2.0 CHAMP D'APPLICATION ET ENTITÉS COUVERTES

La présente annexe à la Politique s'applique non seulement à tous les dirigeants, administrateurs, employés et travailleurs temporaires (collectivement, les « Collaborateurs ») et à tous les mandataires de la société, y compris, sans s'y limiter, les contractants, les consultants et les représentants (collectivement, les « Personnes associées »), mais également :

- aux actionnaires et aux détenteurs de droits de vote à l'assemblée générale de la société;
- aux membres de l'organe d'administration, de direction ou de surveillance de la société;
- au personnel externe et occasionnel de la société;
- aux cocontractants de la société et à leurs sous-traitants;
- aux bénévoles et aux stagiaires (rémunérés ou non);
- aux personnes qui signalent ou divulguent publiquement des informations sur des infractions dont elles ont eu connaissance dans le cadre d'une relation de travail avec la société pendant la période d'essai;
- aux personnes qui signalent ou divulguent publiquement des informations sur des infractions acquises dans le cadre d'une relation de travail avec la Société qui a depuis pris fin; et
- aux personnes dont la relation de travail avec la société n'a pas encore débuté, dans les cas où des informations sur des infractions ont été obtenues au cours du processus de recrutement ou d'autres négociations précontractuelles avec la société.

3.0 DÉFINITIONS

Conformément au décret législatif n° 24/2023, les définitions de « lanceur d'alerte » et de « acte à signaler » au titre de la présente Politique sont étendues en vertu de la loi italienne comme suit :

- Lanceur d'alerte (divulgateur protégé) : est défini comme « une personne physique qui signale des comportements, des actes ou des omissions entraînant des violations (ou des soupçons fondés de violations) des lois et règlements italiens et de l'Union européenne, tels que constatés par le lanceur d'alerte dans le cadre de son emploi, affectant l'intérêt public ou l'intégrité de l'administration publique ou d'une entité privée et constituant des infractions administratives, comptables, civiles ou criminelles ou des comportements illégaux significatifs ».
- Les actes à signaler (actes inappropriés) comprennent, en plus des définitions figurant dans la Politique mondiale :
 1. les infractions civiles, pénales, administratives ou comptables;
 2. les comportements illicites visés par le décret législatif 231/2001;
 3. le cas échéant, les violations des modèles d'organisation et de gestion adoptés conformément au décret législatif 231/2001 (« MOG 231 »);
 4. les violations du droit de l'Union européenne dans des secteurs tels que les marchés publics, les services, produits et marchés financiers, la prévention du blanchiment d'argent et du financement du terrorisme, la sécurité des produits, la sécurité des transports, la protection de l'environnement, etc.;
 5. les actes ou les omissions portant atteinte aux intérêts financiers de l'UE;
 6. les actes ou les omissions affectant le marché intérieur de l'UE (entravant la libre circulation des biens, des services, des personnes ou des capitaux);
 7. les violations des mesures restrictives de l'Union européenne (sanctions de l'UE), y compris les violations des dispositions nationales de mise en œuvre, les infractions pénales ou les infractions administratives liées aux régimes de sanctions de l'UE, lorsque ces violations sont identifiées dans un contexte professionnel.

La divulgation de faits, d'informations ou de documents relatifs à un intérêt personnel de la personne qui effectue le signalement et qui se rapporte exclusivement à son emploi individuel, de violations déjà réglementées de manière contraignante par d'autres règlements de l'UE ou italiens, de violations de la sécurité nationale, d'informations classifiées, du secret professionnel médico-légal et médical, de délibérations judiciaires et de la divulgation de faits, d'informations ou de documents recueillis illégalement est interdite et ne relèvera pas du champ d'application de la Politique globale ou de la présente annexe à la Politique.

4.0 CANAUX DE SIGNALEMENT

Les lanceurs d'alerte peuvent soumettre leurs signalements par :

- le canal de signalement interne;
- un signalement externe à l'Autorité nationale anticorruption italienne (ANAC) via sa plateforme en ligne;

- la divulgation publique (autorisée uniquement dans les conditions spécifiques prévues à l'article 15 du décret législatif 24/2023).

4.1 CANAL DE SIGNALEMENT INTERNE

Les lanceurs d'alerte pourront soumettre des signalements internes par les canaux indiqués dans la Politique mondiale, facilement accessible via un lien disponible sur le site Web de la Société : [GPT Alertline](#).

Une fois connecté au portail, le lanceur d'alerte peut utiliser les menus dédiés pour sélectionner le pays de la société du Groupe concernée par le signalement avant de le soumettre.

Le canal interne permet aux lanceurs d'alerte :

- de soumettre des signalements par tout moyen (écrit ou oral). Si un signalement est fait oralement, il peut se faire par téléphone ou, à la demande du lanceur d'alerte, par vidéoconférence ou lors d'une rencontre en personne organisée dans un délai raisonnable. Tout enregistrement audio nécessite le consentement du lanceur d'alerte. À défaut, un compte rendu écrit est rédigé et signé;
- de signaler de manière anonyme, s'il le juge nécessaire.

Le lanceur d'alerte sera informé par écrit de la réception du signalement dans les sept (7) jours suivant sa réception. La personne désignée maintiendra la communication avec le lanceur d'alerte et pourra lui demander des renseignements supplémentaires.

La personne désignée fournit une réponse de suivi dans les trois (3) mois suivant la date d'accusé de réception du signalement ou, si aucun accusé de réception n'est reçu, dans les trois mois suivant l'expiration du délai de sept jours ouvrables après le signalement. Dans le cadre du suivi, la personne désignée informera le lanceur d'alerte de l'issue du signalement, à savoir : (i) la clôture/l'archivage (lorsque les allégations s'avèrent inexactes ou non fondées ou lorsque le signalement est devenu sans objet) ou (ii) la confirmation que le signalement a été jugé fondé et a été transmis aux organismes/autorités compétents.

Les signalements et les données personnelles qui s'y rapportent seront conservés pendant la durée strictement nécessaire à leur traitement et, en tout état de cause, pendant une durée maximale de cinq (5) ans à compter de la communication du résultat de la procédure.

4.2 CANAL DE SIGNALEMENT EXTERNE - AUTORITÉ NATIONALE ANTICORRUPTION ITALIENNE (« ANAC »)

Les lanceurs d'alerte peuvent effectuer un signalement externe dans les circonstances suivantes prévues par le décret législatif :

- Un canal de signalement interne n'a pas été mis en place ou ne respecte pas les normes requises.
- Ils ont déjà effectué un signalement interne qui n'a pas donné lieu à un suivi ou a abouti à un résultat négatif.

- Ils ont des motifs raisonnables de croire qu'un signalement interne ne ferait pas l'objet d'un suivi ou pourrait entraîner des représailles (par exemple, dans les cas de conflit d'intérêts où la personne chargée du signalement est la même que le lanceur d'alerte, la personne visée par le signalement ou toute autre personne impliquée ou concernée par le signalement).
- Ils ont des motifs raisonnables de croire que la violation peut constituer un danger imminent ou manifeste pour le public.

En Italie, l'ANAC est une autorité administrative indépendante dotée de pouvoirs de réglementation, d'enquête et de sanction dans le domaine du signalement d'actes répréhensibles.

Les lanceurs d'alerte peuvent soumettre des signalements externes à l'ANAC oralement ou par écrit via sa plateforme informatique. Si un signalement est fait oralement, il peut être effectué par téléphone ou par tout autre système de messagerie vocale. Si le dénonciateur le demande, il peut opter pour une vidéoconférence ou une rencontre en personne dans un délai raisonnable

L'ANAC est tenue d'accuser réception du signalement dans les 7 jours suivant sa réception, sauf si le lanceur d'alerte demande de ne pas le faire ou si cela compromettrait la confidentialité du signalement. L'ANAC doit assurer un suivi rigoureux des signalements, mener les enquêtes nécessaires et répondre au lanceur d'alerte dans un délai de trois (3) mois (ou de six (6) mois s'il existe des motifs justifiés de retard) à compter de l'accusé de réception, ou, en l'absence d'accusé de réception, dans un délai de trois (3) ou six (6) mois à compter de l'expiration du délai de sept (7) jours ouvrables suivant le dépôt du signalement. Dans sa réponse, l'ANAC informera le lanceur d'alerte du résultat de l'enquête, qui peut également consister en la clôture du signalement, sa transmission à d'autres autorités compétentes, une recommandation ou l'imposition d'amendes administratives.

Pour plus d'informations sur la procédure de signalement via l'ANAC, veuillez consulter les liens ci-dessous :

<https://www.anticorruzione.it/-/anac-national-anti-corruption-authority-en-brochure-2023>
<https://www.anticorruzione.it/-/whistleblowing#p.%203>

4.3 DIVULGATION PUBLIQUE

La divulgation publique n'est autorisée que dans les conditions prévues à l'article 15 du décret législatif (par exemple, recours préalable aux voies internes et/ou externes sans réponse adéquate, ou risque concret de représailles ou de danger pour l'intérêt public). Une divulgation publique en dehors de ces conditions peut entraîner la perte des protections.

5.0 PERSONNES DÉSIGNÉES

La société a désigné les personnes suivantes pour gérer le canal de signalement interne. Celles-ci ont reçu une formation spécifique et répondent aux exigences d'indépendance et d'impartialité :

- le gestionnaire mondial de la conformité (Global Compliance Manager)
- le gestionnaire juridique, EMEA (Legal Manager, EMEA)

Les personnes désignées agissent de manière autonome et sans conflit d'intérêts, garantissent la confidentialité par défaut et traitent les signalements conformément à la législation applicable et à la présente politique.

En cas de conflit d'intérêts réel, potentiel ou perçu, la personne désignée doit s'abstenir et le dossier sera rapidement réattribué à l'autre personne désignée (ou à un remplaçant dûment désigné) afin de garantir la continuité, la neutralité et un suivi rapide.

6.0 PROTECTION CONTRE LES REPRÉSAILLES ET CONFIDENTIALITÉ

Le principe de non-représailles s'applique non seulement aux collaborateurs, aux personnes associées et aux autres sujets visés à la section 2, qui effectuent un signalement en vertu de la Politique mondiale et de la présente annexe, mais également aux facilitateurs, tels que définis précédemment dans la Politique mondiale, aux tiers liés aux lanceurs d'alerte, tels que les collègues, anciens collègues, consultants et membres de la famille, ainsi qu'aux entités juridiques dont le lanceur d'alerte est propriétaire, pour lesquelles il travaille ou auxquelles il est lié dans un contexte professionnel.

La loi italienne établit une liste exhaustive d'actes et d'omissions, même s'il ne s'agit que de tentatives ou de menaces, pouvant être considérés comme des mesures de représailles, notamment, mais sans s'y limiter : le licenciement, la mise à pied, les mesures disciplinaires (y compris les sanctions financières et la suspension), la réduction de salaire, le déclassement ou la non-promotion, le changement de fonctions, le transfert de lieu de travail, tout type de discrimination, les notes de mérite négatives, les références négatives, le harcèlement, l'ostracisme, la non-conversion d'un contrat à durée déterminée en contrat à durée indéterminée, l'atteinte à la réputation, l'annulation de contrats de fourniture, la demande de se soumettre à un examen psychiatrique ou médical.