

GUIDA ALLE POLITICHE

POLITICA DI SEGNALAZIONE DEL GRUPPO

NUMERO: COMP-02GPT | DATA DI ENTRATA IN VIGORE ORIGINALE: 01/01/2026

INDICE:

- 1.0 Finalità della politica di segnalazione del gruppo
- 2.0 Ambito di applicazione e definizioni
- 3.0 Tutela degli informatori
- 4.0 Cosa deve essere segnalato ai sensi della presente Politica?
- 5.0 A chi e come devo segnalare?
- 6.0 Posso segnalare le mie preoccupazioni al di fuori di GPT?
- 7.0 Contenuto delle segnalazioni
- 8.0 Riservatezza/Anonimato
- 9.0 Valutazione e gestione delle segnalazioni
- 10.0 Conservazione delle segnalazioni
- 11.0 Divieto di ritorsione
- 12.0 Trattamento dei dati personali
- 13.0 Supervisione del sistema di segnalazione
- 14.0 Segnalazioni alle autorità governative e di regolamentazione
- 15.0 Proroga e modifica

ALLEGATO A: Disposizioni aggiuntive specifiche per Paese (per Regione)

- Austria
- Repubblica Ceca
- Danimarca
- Germania
- Italia

1.0 SCOPO DELLA POLITICA DI SEGNALAZIONE DEL GRUPPO

Grain & Protein Technologies (“GPT”, il “Gruppo”) si impegna a mantenere i più elevati standard di integrità, etica e conformità in tutti gli aspetti della propria attività. Ritiene che la condotta etica, la trasparenza e la responsabilità siano fondamentali per instaurare un rapporto di fiducia con i propri dipendenti, gli stakeholder e le comunità in cui opera.

In linea con questo impegno, GPT incoraggia tutte le persone, sia all’interno dell’azienda che tra i soggetti terzi che interagiscono con GPT in un contesto lavorativo, a segnalare qualsiasi sospetto di comportamento scorretto, irregolarità, violazione delle leggi o delle politiche interne. Tali segnalazioni sono fondamentali per salvaguardare l’integrità e la reputazione di GPT e per garantire un ambiente di lavoro sicuro, equo e conforme alle normative.

La presente Politica Globale si applica a livello mondiale ed è concepita per conformarsi alle leggi applicabili in materia di protezione degli informatori nelle giurisdizioni in cui GPT opera. Essa delinea cosa può essere segnalato, come devono essere presentate le segnalazioni, le fasi procedurali seguite dopo la ricezione di una segnalazione e le tutele offerte a coloro che sollevano preoccupazioni.

In caso di conflitto tra la presente Politica e la legislazione applicabile, prevarranno le disposizioni di legge. La presente Politica si applica a tutti i membri del Gruppo GPT, ma a causa dei diversi requisiti legali locali, abbiamo creato allegati o politiche locali separate per rispondere a esigenze specifiche e garantire la conformità alle normative nazionali.

GPT vieta severamente qualsiasi ritorsione nei confronti di chiunque segnali in buona fede un comportamento scorretto o partecipi alle relative indagini. Le persone sono protette da discriminazioni, molestie o qualsiasi trattamento sfavorevole derivante dalla loro segnalazione, come successivamente descritto nella presente Politica.

2.0 AMBITO DI APPLICAZIONE E DEFINIZIONI

Qualsiasi persona, comprese le parti esterne, che abbia acquisito informazioni su violazioni nel contesto lavorativo può presentare una segnalazione. Ciò include in particolare:

- dipendenti e dirigenti attuali ed ex dipendenti di GPT;
- lavoratori autonomi e appaltatori che forniscono servizi al Gruppo;
- azionisti e membri degli organi di GPT, compresi i membri non esecutivi;
- volontari, tirocinanti e stagisti retribuiti o non retribuiti;
- persone che lavorano sotto la supervisione e la direzione di appaltatori, subappaltatori e fornitori;
- partner commerciali, inclusi clienti, fornitori, consulenti, agenti e i loro dipendenti, che hanno o hanno avuto un rapporto professionale con GPT.

3.0 PROTEZIONE DEGLI INFORMATORI

Ai fini della presente Politica, per "informatore" si intende qualsiasi persona che abbia fondati motivi per sospettare che si sia verificata una condotta scorretta, una situazione impropria o una violazione della legge o delle politiche interne in relazione a GPT ("Condotta segnalabile") e che comunichi tali preoccupazioni attraverso uno dei canali di segnalazione descritti nella presente Politica.

GPT si impegna a proteggere le persone che effettuano segnalazioni in buona fede e in conformità con la presente Politica ("Segnalazione protetta"). Gli informatori non devono subire alcuna forma di ritorsione, rappresaglia, discriminazione, molestia o svantaggio a seguito di una Segnalazione protetta.

L'identità dell'informatore e qualsiasi informazione da cui tale identità possa essere dedotta direttamente o indirettamente saranno mantenute strettamente riservate e non saranno divulgate senza l'esplicito consenso dell'informatore, salvo nei seguenti casi:

- Laddove richiesto dalla legge applicabile;
- Laddove la divulgazione sia ragionevolmente necessaria per indagare sulla segnalazione o per ottemperare a procedimenti legali, a condizione che la riservatezza sia preservata nella misura massima consentita dalla legge; oppure
- Laddove la divulgazione sia effettuata alle autorità di regolamentazione competenti, alle forze dell'ordine o a consulenti professionali vincolati da obblighi di riservatezza.

4.0 COSA DEVE ESSERE SEGNALATO AI SENSI DELLA PRESENTE POLITICA?

Qualsiasi questione che una persona ragionevolmente ritenga violi le politiche, gli standard etici o le leggi e i regolamenti applicabili di GPT deve essere segnalata in conformità con la presente Politica.

Esempi di comportamenti segnalabili possono includere:

- violazioni di leggi o regolamenti;
- attività illegali, corruttive, fraudolente o irregolari che comportano l'uso di fondi, beni o proprietà di GPT;
- comportamenti illegali o criminali, inclusi furto, vendita o uso di sostanze stupefacenti, violenza o minacce di violenza;
- violazioni delle politiche e delle procedure di GPT (incluso, ma non limitato al Codice di Condotta);
- comportamenti che comportano un rischio significativo per la salute pubblica, la sicurezza o l'ambiente;
- comportamenti disonesti, non etici o abusivi sul posto di lavoro;
- frodi finanziarie, cattiva gestione o irregolarità contabili;
- comportamenti che potrebbero danneggiare la posizione finanziaria, la reputazione o la fiducia degli stakeholder di GPT;
- grave negligenza, discriminazione, molestie o comportamenti oppressivi;
- occultamento o tentativo di occultamento di comportamenti scorretti o di situazioni irregolari.

Ulteriori esempi, laddove richiesti dalle leggi locali in materia di segnalazione di irregolarità, sono descritti in dettaglio negli allegati specifici per Paese della presente Politica.

Una persona può anche utilizzare l'opzione "*Fai una domanda*" invece di presentare una segnalazione formale. In tal caso, GPT la valuterà e fornirà una risposta. Se la questione sembra rientrare nell'ambito della Condotta Segnalabile, GPT può, a sua discrezione, riclassificare la domanda come segnalazione per garantire che sia gestita in modo appropriato ai sensi della presente Politica.

La condotta segnalabile deve essere distinta dalle lamentele personali relative al lavoro. Una lamentela personale relativa al lavoro si riferisce a qualsiasi questione connessa all'attuale o precedente impiego di un individuo che lo riguarda personalmente, ma non indica una condotta scorretta o una violazione della legge o delle politiche interne.

Esempi di reclami personali legati al lavoro includono, ma non si limitano a:

- conflitti interpersonali o controversie tra dipendenti;
- decisioni relative a trasferimenti, promozioni o valutazioni delle prestazioni;
- misure disciplinari, ammonimenti o decisioni di licenziamento.

Le segnalazioni relative a presunte discriminazioni, molestie, ritorsioni o altre violazioni delle leggi sul lavoro non sono considerate reclami personali legati al lavoro e rientrano nell'ambito di applicazione della presente Politica. I reclami personali legati al lavoro, come descritti sopra, che non comportano una condotta segnalabile, vengono solitamente gestiti al meglio tramite il proprio responsabile diretto, un leader o il canale delle Risorse Umane, che sono progettati per affrontare le questioni relative al lavoro in modo equo e tempestivo.

Se non siete sicuri che una questione rientri nell'ambito di applicazione della presente Politica, potete contattare il Dipartimento Legale e di Conformità di GPT all'indirizzo GPTCompliance@grainproteintech.com per ricevere una consulenza riservata su come procedere al meglio.

5.0 A CHI E COME DEVO SEGNALARE?

GPT ha istituito canali di segnalazione sicuri e riservati per l'invio delle segnalazioni.

Laddove richiesto dalla Direttiva UE sulla protezione delle persone che segnalano violazioni (UE) 2019/1937 o da altre leggi federali, statali o locali applicabili, GPT ha nominato delle Persone Designate, autorizzate a ricevere e dar seguito alle segnalazioni in conformità con i requisiti legali.

I dipendenti e le altre persone aventi diritto che desiderino effettuare una segnalazione possono, anziché inviarla direttamente al Consulente Legale Generale e Responsabile della Conformità o ad altri rappresentanti della direzione, scegliere di inviarla in modo riservato e, se lo desiderano, in forma anonima, tramite la GPT Alertline. Nessuna disposizione della presente Politica impone

alle persone di effettuare una segnalazione interna prima di segnalare le proprie preoccupazioni alle autorità governative o di regolamentazione, laddove tale segnalazione sia tutelata dalla legge applicabile.

La GPT Alertline è gestita da NAVEX, un servizio di terze parti indipendente incaricato da GPT di ricevere e documentare le segnalazioni da parte di dipendenti e soggetti esterni e di trasmetterle in modo sicuro al personale interno competente per la valutazione e il follow-up. È gestita al di fuori del sito web e della rete aziendale della Società per garantire la riservatezza e l'indipendenza.

L'AlertLine offre opzioni di segnalazione sia via web che telefoniche. I link e i numeri di telefono pertinenti sono facilmente reperibili sul sito web di GPT ([GPT Alertline](#)) e sul sito web di ciascuna società del gruppo GPT, come indicato negli Allegati specifici per Paese della presente Politica.

Una volta effettuato l'accesso all'AlertLine, l'informatore può utilizzare i menu dedicati per selezionare il Paese della società del Gruppo a cui si riferisce la segnalazione prima di inviarla.

I canali di segnalazione consentono di effettuare segnalazioni per iscritto o tramite la GPT Alertline. Su richiesta, un informatore può anche chiedere di effettuare una segnalazione tramite un incontro di persona con la Persona Designata. Tale incontro sarà organizzato entro un lasso di tempo ragionevole dopo la richiesta, nel rispetto della legge applicabile. Qualsiasi registrazione audio richiede il consenso esplicito dell'informatore; in caso contrario, viene redatto e firmato un verbale scritto o una sintesi.

Se, per qualsiasi motivo e con qualsiasi mezzo, una segnalazione che rientra nell'ambito di applicazione della presente Politica viene ricevuta al di fuori dei canali di designati, la persona che la riceve deve immediatamente garantire la riservatezza di tutte le informazioni incluse nella segnalazione.

È severamente vietato divulgare l'identità dell'Informatore, della persona segnalata o di qualsiasi altro individuo menzionato nella segnalazione, nonché qualsiasi informazione che possa portare, direttamente o indirettamente, alla loro identificazione. Il destinatario deve inoltre consigliare all'informatore di seguire la procedura di segnalazione ufficiale stabilita dalla presente Politica e/o inoltrare la segnalazione all'Ufficio Legale e di Conformità di GPT senza indebito ritardo e, in ogni caso, entro e non oltre sette (7) giorni dal ricevimento. Una volta ottenuta la conferma di ricezione dal responsabile della segnalazione designato, qualsiasi copia o registrazione della segnalazione (comprese e-mail o note) deve essere eliminata in modo sicuro per garantire la piena riservatezza e la conformità alla protezione dei dati.

6.0 POSSO SEGNALARE PREOCCUPAZIONI AL DI FUORI DI GPT?

Gli informatori sono invitati in primo luogo a utilizzare i canali di segnalazione interni istituiti da GPT.

Tuttavia, in presenza di condizioni specifiche definite dalle leggi e dai regolamenti applicabili, è possibile effettuare una segnalazione esterna direttamente alle autorità competenti in conformità con le normative locali e/o internazionali pertinenti.

Gli informatori devono fare riferimento agli Allegati specifici per Paese della presente Politica per ulteriori dettagli sulle procedure di segnalazione esterna e sulle autorità competenti applicabili alle loro giurisdizioni.

7.0 CONTENUTO DELLE SEGNALAZIONI

Per consentire a GPT di rispondere e, se del caso, indagare efficacemente su una segnalazione, le segnalazioni devono essere basate sui fatti piuttosto che su speculazioni e includere quante più informazioni specifiche possibili. Ciò consente a GPT di valutare adeguatamente la natura, la portata e l'urgenza della questione oggetto della segnalazione.

Ai fini di una corretta valutazione e indagine, è consigliabile che la segnalazione includa, ove disponibili, le seguenti informazioni:

- I. Contesto e descrizione della questione, compresi i fatti rilevanti e i motivi della segnalazione;
- II. nome/i della/e persona/e coinvolta/e o implicata/e;
- III. nome/i di eventuali testimoni;
- IV. data, ora e luogo dell'incidente o degli incidenti;
- V. dettagli o eventuali copie di prove o documentazione a sostegno;
- VI. informazioni su eventuali fondi, beni o interessi coinvolti;
- VII. indicazione della frequenza con cui si è verificato l'incidente (se applicabile).

Il meccanismo di segnalazione non deve essere utilizzato in modo improprio. Sono severamente vietate le segnalazioni effettuate in malafede, comprese quelle consapevolmente false o effettuate al solo scopo di danneggiare un'altra persona. Tali comportamenti possono comportare misure disciplinari o, ove applicabile, azioni legali, in conformità con le leggi del Paese competente.

Tuttavia, non verrà intrapresa alcuna azione contro un informatore che presenti una segnalazione in buona fede, anche se i fatti segnalati dovessero successivamente rivelarsi errati o infondati.

GPT si impegna a proteggere gli informatori in buona fede da ritorsioni e a garantire che il meccanismo di segnalazione sia utilizzato in modo responsabile ed etico.

8.0 RISERVATEZZA/ANONIMATO

Accuse che l'informatore ha deciso di denunciare apertamente e non in forma anonima

GPT promuove una cultura aperta e trasparente e incoraggia le persone a segnalare apertamente eventuali preoccupazioni, ove possibile. Ciò facilita una valutazione, un'indagine e un seguito più efficaci della questione.

Quando un informatore ha scelto di fornire la propria identità insieme alla segnalazione, GPT farà tutto il possibile per garantire che la sua identità rimanga riservata, a meno che tale divulgazione non sia richiesta dalla legge, dai regolamenti o da procedimenti giudiziari applicabili. In tutti i casi, le segnalazioni saranno gestite in conformità con le normative applicabili in materia di protezione dei dati e di segnalazione di irregolarità.

Denunce in cui l'informatore ha scelto di denunciare in forma anonima

GPT riconosce che, in alcune situazioni, l'informatore potrebbe sentirsi più a suo agio nel segnalare le proprie preoccupazioni in forma anonima. La possibilità di presentare segnalazioni anonime dipende dalle leggi e dai regolamenti applicabili. Laddove consentito, tali segnalazioni saranno valutate e, ove possibile, investigate con la stessa cura delle segnalazioni non anonime.

Gli informatori che inizialmente segnalano in forma anonima – o che, ove e quando consentito dalla legge applicabile, effettuano una divulgazione pubblica anonima – rimarranno protetti ai sensi della presente Politica se la loro identità verrà successivamente rivelata, a condizione che soddisfino le altre condizioni stabilite nella presente Politica.

Tuttavia, gli informatori devono essere consapevoli che, in alcuni casi, potrebbe essere difficile condurre un'indagine completa in modo adeguato senza conoscere l'identità dell'informatore, in particolare quando sono necessari chiarimenti successivi, colloqui o verifiche dei fatti.

9.0 VALUTAZIONE E GESTIONE DELLE SEGNALAZIONI

GPT prende sul serio ogni segnalazione di violazioni sospette o potenziali. Tutte le segnalazioni inviate attraverso i canali di segnalazione designati saranno gestite in modo equo, appropriato e senza indebiti ritardi. L'informatore riceverà una conferma di ricezione della segnalazione entro sette (7) giorni dalla data di recapito. La conferma può essere ritardata qualora sia necessario un intervento immediato per preservare le prove o affrontare un rischio imminente, in conformità con la legge applicabile.

GPT si impegna a garantire un seguito approfondito e imparziale di tutte le segnalazioni. Le indagini vengono condotte da personale qualificato o, ove opportuno, da esperti e consulenti esterni. GPT garantisce che tutti i fatti rilevanti siano raccolti, documentati e valutati in modo obiettivo, nel pieno rispetto degli obblighi di riservatezza e di protezione dei dati. Per questo motivo, la necessità di riservatezza, la tutela della privacy e il rispetto degli obblighi legali applicabili possono limitare la misura in cui dettagli specifici sull'indagine, le azioni intraprese o le azioni risultanti possano essere condivisi con l'informatore. Qualsiasi informazione fornita all'informatore in merito ai progressi compiuti o all'esito dell'indagine deve essere trattata come strettamente riservata.

GPT fornirà un riscontro all'informatore entro un termine ragionevole e, in ogni caso, non oltre tre (3) mesi:

- dalla conferma di ricezione della segnalazione;

- in assenza di conferma, dalla scadenza del periodo di conferma di sette giorni.

GPT non può garantire che l'esito dell'indagine sarà in linea con le aspettative o il risultato desiderato dall'informatore. Tuttavia, si impegna pienamente a garantire che tutte le preoccupazioni fondate siano trattate in modo equo, rispettoso e diligente.

Se, durante la valutazione o l'indagine, dovesse emergere che i fatti riportati nella segnalazione possano costituire un reato penale, il responsabile designato, d'intesa con le altre funzioni aziendali competenti e la direzione del gruppo, valuterà se, quando e come deferire la questione alle autorità giudiziarie o di regolamentazione competenti, in conformità con le leggi e i regolamenti locali applicabili.

10.0 CONSERVAZIONE DELLE SEGNALAZIONI

Le copie cartacee ed elettroniche di tutte le segnalazioni saranno conservate in modo sicuro in conformità con il programma di conservazione dei dati documentato di GPT. Le segnalazioni inviate tramite la GPT Alertline saranno archiviate elettronicamente all'interno della piattaforma di segnalazione sicura NAVEX.

Tutti i registri e la documentazione a supporto saranno conservati solo per il tempo necessario a soddisfare i requisiti legali e normativi applicabili.

Ove opportuno, GPT renderà anonimi o pseudonimizzerà i dati personali inclusi in una segnalazione, entro un lasso di tempo ragionevole, a seguito della conclusione dell'indagine, in conformità con tutte le leggi applicabili in materia di protezione dei dati, incluso, ove applicabile, il Regolamento generale sulla protezione dei dati (GDPR).

11.0 DIVIETO DI RITORSIONE

Per ritorsione si intende qualsiasi atto o omissione, diretto o indiretto, che si verifichi in un contesto lavorativo a seguito di una segnalazione interna o esterna o di una divulgazione pubblica effettuata ai sensi della presente Politica, che causi o possa causare un danno ingiustificato e ingiusto all'informatore.

Nessun informatore che sollevi in buona fede una preoccupazione su questioni contemplate dalla presente Politica subirà alcuna forma di ritorsione. Chiunque si renda responsabile di ritorsioni potrà essere oggetto di azioni disciplinari che possono arrivare fino al licenziamento, indipendentemente dalla posizione ricoperta o dall'anzianità di servizio.

GPT si impegna fermamente a proteggere gli informatori che effettuano segnalazioni in buona fede da ritorsioni, molestie o qualsiasi altro trattamento sfavorevole. Tutti gli informatori saranno trattati con rispetto, dignità e riservatezza durante l'intero processo.

Le ritorsioni includono, ma non si limitano a, minacce o tentativi di ritorsione e possono assumere la forma di:

- sospensione, licenziamento temporaneo, licenziamento o misure equivalenti;
- retrocessione o negazione della promozione;

- trasferimento di mansioni, cambiamento della sede di lavoro, riduzione della retribuzione o modifica dell'orario di lavoro;
- valutazione negativa delle prestazioni o referenze lavorative negative;
- azione disciplinare, richiamo o altra sanzione, comprese le sanzioni pecuniarie;
- coercizione, intimidazione, molestie o emarginazione;
- discriminazione o altre forme di trattamento svantaggioso o ingiusto;
- mancata conversione di un contratto di lavoro a tempo determinato in un contratto a tempo indeterminato laddove sussistesse un legittimo sospetto;
- mancato rinnovo o risoluzione anticipata di un contratto di lavoro temporaneo;
- danno della reputazione (anche attraverso i social media) o perdita finanziaria, come la perdita di affari o di reddito;
- l'inserimento in una lista nera in un campo o in un intero settore, sia essa formale o informale;
- risoluzione anticipata o annullamento di un contratto per beni o servizi;
- revoca o rifiuto di una licenza o di un permesso;
- segnalazioni psichiatriche o mediche ingiustificate.

Le misure di protezione previste dalla presente Politica si estendono, ove applicabile, anche a:

- facilitatori, ovvero persone che assistono un informatore nel processo di segnalazione in un contesto lavorativo e il cui operato deve essere riservato;
- terze persone legate agli informatori che potrebbero subire ritorsioni in un contesto lavorativo, come colleghi o parenti; e
- persone giuridiche di proprietà dell'informatore, che lavorano per lui o che sono altrimenti collegate a lui in ambito professionale.

12.0 TRATTAMENTO DEI DATI PERSONALI

Qualsiasi trattamento dei dati personali effettuato ai sensi della presente Politica, compresa la trasmissione o lo scambio di informazioni con le autorità competenti, dovrà essere conforme a tutte le leggi applicabili in materia di protezione dei dati. Analogamente, le segnalazioni che coinvolgono entità o persone fisiche situate in giurisdizioni diverse potranno essere condivise tra le entità GPT interessate esclusivamente in base alla necessità di conoscere e nel rispetto delle leggi applicabili in materia di protezione dei dati e di segnalazione di irregolarità.

I dati personali che non sono palesemente rilevanti per la gestione di una segnalazione specifica non saranno raccolti o, se raccolti accidentalmente, saranno cancellati senza indebito ritardo. GPT garantirà che tutti i dati personali trattati in relazione alle segnalazioni di whistleblowing siano gestiti in modo sicuro, lecito e proporzionato, con accesso strettamente limitato alle persone autorizzate a trattare tali dati personali per scopi legittimi.

13.0 SUPERVISIONE DEL SISTEMA DI SEGNALEZIONE

L'efficacia della presente Politica e il funzionamento del sistema di segnalazione sono periodicamente esaminati dal Dipartimento Legale e di Conformità di GPT. La presente Politica può essere aggiornata per riflettere le modifiche alle leggi e ai regolamenti applicabili, alla struttura organizzativa o agli standard di best practice.

14.0 SEGNALAZIONI ALLE AUTORITÀ GOVERNATIVE E DI REGOLAMENTAZIONE

Queste procedure non intendono in alcun modo limitare i diritti dei dipendenti di segnalare presunte violazioni relative a questioni contabili o di revisione dei conti alle autorità governative e di regolamentazione competenti.

15.0 CONTINUITÀ E MODIFICA

Come per qualsiasi politica o programma di benefici, Grain & Protein Technologies si riserva il diritto illimitato, in conformità con la legge, di rivedere, riconsiderare, interpretare, emendare, modificare, sospendere o interrompere in tutto o in parte tale politica, piano o programma in qualsiasi momento, con o senza preavviso. Se una qualsiasi disposizione della presente politica è in conflitto con o viola qualsiasi statuto o regolamento applicabile, prevarranno le disposizioni di tale statuto o regolamento. Nessuna modifica, sospensione o interruzione della presente Politica pregiudicherà le tutele garantite agli informatori ai sensi della legge applicabile.

LE DOMANDE RELATIVE ALLA PRESENTE GUIDA ALLA POLITICA DEVONO ESSERE RIVOLTE ALL'UFFICIO LEGALE E DI CONFORMITÀ.

Descrizione	Data di entrata in vigore	Modifica apportata da Nome e titolo
Creazione della politica	01/01/2026	Patrick Rykhus, GC

ALLEGATO A: Disposizioni aggiuntive specifiche per Paese (per Regione)

Il presente allegato evidenzia alcuni Paesi in cui GPT opera e che dispongono di leggi in materia di segnalazione di irregolarità che potrebbero essere applicabili alla vostra situazione in qualità di informatori.

AUSTRIA

1.0 SINTESI

Il presente Allegato alla Politica è inteso a integrare l'attuale Politica di segnalazione del Gruppo GPT affrontando le specifiche modifiche legislative che sono state implementate in Austria ai sensi della Direttiva UE 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione (Direttiva sulla segnalazione di irregolarità) e della normativa locale [Legge austriaca sulla protezione degli informatori (*HinweisgeberInnenenschutzgesetz* – “HSchG”)].

Il presente Allegato alla Politica affronta quindi le differenze di applicazione rispetto alla Politica Globale che si applicano all'entità di GPT situata in Austria, ovvero: **Cimbria Heid GmbH** (la “Società”) e contiene disposizioni locali specifiche relative alle entità austriache e applicabili a tutte le persone indicate nella Sezione 2 della Politica e solo nella misura in cui sia applicabile la legge HSchG.

2.0 DISPOSIZIONI LOCALI SPECIFICHE CHE DIVERGONO DALLA POLITICA

2.1 Ambito di applicazione ai sensi della legge HSchG

La legge austriaca sulla protezione degli informatori (HSchG) si applica in caso di violazioni nei seguenti ambiti:

- Appalti pubblici;
- Servizi finanziari, prodotti finanziari e mercati finanziari, nonché prevenzione del riciclaggio di denaro e del finanziamento del terrorismo;
- Sicurezza e conformità dei prodotti;
- Sicurezza stradale;
- Tutela dell'ambiente;
- Protezione dalle radiazioni e sicurezza nucleare;
- Sicurezza degli alimenti e dei mangimi, salute e benessere degli animali;
- Salute pubblica;
- Tutela dei consumatori;
- Tutela della privacy e dei dati personali, nonché sicurezza delle reti e dei sistemi informativi;
- Prevenzione e punizione dei reati penali ai sensi degli articoli da 302 a 309 del Codice penale (StGB), Gazzetta ufficiale federale I n. 60/1974;
- Interessi finanziari dell'Unione ai sensi dell'articolo 325 del Trattato sul funzionamento dell'Unione Europea (TFUE), ad esempio uso improprio dei fondi dell'UE;
- Norme del mercato interno ai sensi dell'articolo 26, paragrafo 2, del TFUE e norme dell'Unione in materia di concorrenza e aiuti di Stato.

2.2 INCONTRO DI PERSONA

Nel caso in cui un informatore desideri effettuare una segnalazione tramite un incontro di persona con la persona designata, tale incontro avrà luogo entro quattordici (14) giorni di calendario dalla presentazione della richiesta.

2.3 TERMINE PER IL RISPOSTA

GPT fornirà un riscontro all'informatore in merito alla segnalazione presentata entro un termine ragionevole, che non supererà i tre (3) mesi dalla presentazione della segnalazione.

3.0 CANALE DI SEGNALEZIONE ESTERNO

Gli informatori sono incoraggiati in primo luogo a segnalare le loro preoccupazioni utilizzando il canale interno. Tuttavia, se tale opzione non è possibile o appropriata, se non è ragionevole gestire le informazioni nel sistema interno di segnalazione o se si è rivelato infruttuoso o inutile, un informatore può presentare una segnalazione esternamente [all'Ufficio federale per la prevenzione e la lotta alla corruzione](#) (Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung).

Il § 15 (2) HschG indica i seguenti canali di segnalazione esterni aggiuntivi:

- Autorità di vigilanza sui revisori (in base alla legge sulla vigilanza sui revisori);
- Autorità contabile (ai sensi della legge sulla contabilità);
- Autorità federale per la concorrenza (in base alla legge sulla concorrenza);
- Autorità per i mercati finanziari (in base alla legge sull'Autorità per i mercati finanziari);
- Ufficio di segnalazione per il riciclaggio di denaro (in base alla legge sull'Ufficio federale di polizia criminale);
- Ordini dei notai (in base al Codice notarile);
- Ordini degli avvocati (in base allo Statuto disciplinare per avvocati e praticanti);
- Ordine dei consulenti fiscali e dei revisori dei conti (in base alla legge sulla professione di contabile pubblico).

3.1 DIVULGAZIONE AL PUBBLICO

La divulgazione pubblica è consentita solo alle condizioni stabilite dalla legge austriaca sulla protezione degli informatori e la divulgazione al di fuori di tali condizioni può comportare la perdita delle tutele.

Gli informatori possono effettuare una segnalazione esterna nelle seguenti circostanze:

- Hanno già effettuato una segnalazione attraverso i canali di segnalazione interni ed esterni (o solo esternamente all'autorità competente), ma non è stata intrapresa alcuna azione appropriata né si intende intraprenderla entro:
 - I. tre (3) mesi dalla presentazione della segnalazione tramite il canale di segnalazione interno o
 - II. tre (3) mesi (o fino a sei (6) mesi in casi debitamente giustificati) dalla presentazione della segnalazione tramite un canale di segnalazione esterno;

- Hanno motivi ragionevoli per ritenere che:
 - I. la violazione di cui alla segnalazione possa comportare una minaccia imminente o evidente per l'interesse pubblico, ad esempio in caso di situazione di emergenza o di rischio di danno irreversibile; oppure;
 - II. hanno fondati motivi per ritenere che, qualora la segnalazione venga effettuata tramite il sistema di segnalazione esterno, sussista il rischio di ritorsioni o che vi siano scarse probabilità che la questione venga gestita in modo efficace. Ciò potrebbe essere dovuto al fatto che le prove potrebbero essere occultate o distrutte oppure perché l'autorità coinvolta non è affidabile o è collegata al problema.

4.0 PERSONE DESIGNATE

La Società ha nominato le seguenti **Persone Designate** per gestire il canale di segnalazione interna, specificamente formate e in possesso dei requisiti di indipendenza e imparzialità:

- il Responsabile Compliance Globale (Global Compliance Manager); e
- il Responsabile Affari Legali, EMEA (Legal Manager, EMEA).

Le Persone Designate agiscono in modo autonomo e senza conflitti di interesse, garantiscono la riservatezza come standard e gestiscono le segnalazioni in conformità con la legge applicabile e la presente Politica.

In caso di conflitto di interessi effettivo, potenziale o percepito, la Persona Designata si asterrà e il caso sarà prontamente riassegnato all'altra Persona Designata (o a un sostituto debitamente nominato) per garantire continuità, neutralità e un tempestivo follow-up.

5.0 PROTEZIONE CONTRO LE RITORSIONI E RISERVATEZZA

Le ritorsioni nei confronti di un informatore che in buona fede sollevi una preoccupazione riguardante questioni coperte dalla legge HSchG (vedi Sezione 1.0 sopra) sono giuridicamente invalide.

6.0 TRATTAMENTO DEI DATI PERSONALI

Oltre alle disposizioni di legge di cui alla Sezione 11.0 della Politica, in Austria il trattamento dei dati personali relativi alle segnalazioni di whistleblowing è disciplinato dalla Sezione 8 della legge HSchG nonché dalle disposizioni della Legge austriaca sulla protezione dei dati (*Datenschutzgesetz* – “DSG”).

6.1 PERIODO DI CONSERVAZIONE

I dati personali devono essere conservati da GPT per cinque (5) anni dopo la chiusura del caso oggetto della segnalazione e, oltre tale termine, per il tempo necessario a svolgere procedimenti amministrativi o giudiziari già avviati o procedimenti investigativi ai sensi del Codice di procedura penale (*Strafprozessordnung* – “StPO”).



Le operazioni di trattamento effettivamente eseguite, quali modifiche, interrogazioni e trasmissioni, devono essere registrate. I dati di log relativi a tali processi devono essere conservati per tre (3) anni dopo la cessazione dell'obbligo di conservazione di cinque (5) anni.

REPUBBLICA CECA

1.0 SINTESI

Il presente Allegato alla Politica è inteso a integrare l'attuale Politica di segnalazione del Gruppo GPT affrontando le specifiche modifiche legislative che sono state implementate nella Repubblica Ceca ai sensi della Direttiva UE 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione (Direttiva sulla segnalazione di irregolarità) e della normativa locale. La principale base giuridica in materia di segnalazione di irregolarità nella Repubblica Ceca è la Legge n. 171/2023 Coll., sulla protezione degli informatori (la "Legge ceca sulla protezione degli informatori").

Il presente Allegato alla Politica affronta quindi le differenze di applicazione rispetto alla Politica Globale che si applicano all'entità di GPT con sede nella Repubblica Ceca, ovvero: Cimbria HMD, s.r.o. (la "Società").

2.0 AMBITO DI APPLICAZIONE E SOGGETTI INTERESSATI

Il presente Allegato alla Politica si applica non solo a tutti i funzionari, amministratori, dipendenti e lavoratori temporanei (collettivamente, "Collaboratori") e a tutti gli agenti della Società, inclusi, a titolo esemplificativo ma non esaustivo, appaltatori, consulenti e rappresentanti (collettivamente "Persone associate"), ma anche a:

- azionisti e titolari di diritti di voto nell'assemblea generale della Società;
- membri dell'organo amministrativo, direttivo o di vigilanza della Società;
- personale esterno e occasionale della Società;
- co-appaltatori della Società e loro subappaltatori;
- volontari o stagisti;
- coloro che segnalano o rendono pubbliche informazioni su violazioni acquisite nell'ambito di un rapporto di lavoro con la Società che è poi cessato; e
- coloro il cui rapporto di lavoro con la Società deve ancora avere inizio, nei casi in cui le informazioni relative a violazioni siano state acquisite durante il processo di assunzione o altre trattative precontrattuali nella Repubblica Ceca.

3.0 DEFINIZIONI

Le definizioni di informatore e Comportamento segnalabile ai sensi della presente Politica sono estese dalla legge ceca come segue:

- informatore (Segnalante protetto): è definito come “una persona fisica che segnala una possibile violazione che si è verificata o sta per verificarsi e che presenta le caratteristiche di un reato penale o di un illecito amministrativo o che viola la legge sulla segnalazione di irregolarità o un'altra normativa legale o gli interessi finanziari dell'Unione Europea o del suo mercato interno”;
- la condotta segnalabile (condotta impropria) include, oltre alle definizioni contenute nella Politica globale, tale violazione.

La divulgazione di fatti, informazioni o documenti che potrebbero minacciare la sicurezza nazionale, relativi ad attività dei servizi di intelligence o la cui segnalazione costituirebbe una violazione del segreto professionale del clero, è vietata e non rientra nell'ambito di applicazione della Politica Globale o del presente Allegato alla Politica.

4.0 CANALI DI SEGNALEZIONE

Gli informatori possono presentare segnalazioni tramite:

- canale di segnalazione interno;
- segnalazione esterna al Ministero della Giustizia della Repubblica Ceca;
- divulgazione pubblica (consentita solo in specifiche condizioni previste dalla legge).

4.1 CANALE DI SEGNALEZIONE INTERNO

Gli informatori potranno presentare segnalazioni interne tramite i canali indicati nella Politica Globale, facilmente accessibile tramite un link disponibile sul sito web della Società: [GPT Alertline](#).

Una volta effettuato l'accesso al portale, l'informatore può utilizzare i menu dedicati per selezionare il Paese della società del Gruppo a cui si riferisce la segnalazione prima di inviarla.

Il canale interno consente agli informatori:

- di presentare segnalazioni con qualsiasi mezzo (scritto o orale). Se una segnalazione viene fornita oralmente, può essere effettuata per telefono o, su richiesta dell'informatore, tramite videoconferenza o incontro di persona organizzato entro un lasso di tempo ragionevole, ma non oltre quattordici (**14**) giorni dalla data in cui è stata presentata la richiesta;
- qualsiasi registrazione audio richiede il consenso dell'informatore; in caso contrario, viene redatto e firmato un verbale scritto. Il Responsabile designato darà all'informatore l'opportunità di commentare la trascrizione scritta della segnalazione o la trascrizione della registrazione audio. I commenti dell'informatore saranno allegati alla registrazione o alla trascrizione;
- di effettuare la segnalazione in forma anonima, qualora lo ritenga necessario.

L'informatore sarà avvisato per iscritto della ricezione della segnalazione entro sette (**7**) giorni dal suo ricevimento. La Persona Designata manterrà i contatti con l'informatore e potrà richiedere ulteriori informazioni.

La Persona Designata è tenuta a valutare se la segnalazione sia fondata e ad avvisare per iscritto l'informatore dell'esito di tale valutazione entro trenta (**30**) giorni dalla data di ricezione della segnalazione. Nei casi di complessità fattuale o giuridica, tale termine può essere prorogato di altri 30 giorni, ma non più di due volte. La Persona Designata è tenuta ad avvisare per iscritto l'informatore della proroga del termine e dei motivi di tale proroga prima della scadenza del termine originario.

Successivamente, la Persona Designata avviserà l'informatore dell'esito della segnalazione, ovvero:

(I) che la sottomissione non costituisce una segnalazione ai sensi della legge ceca sulla protezione degli informatori; in tal caso, la Persona Designata avviserà per iscritto l'Informatore senza indebito ritardo;

(II) chiusura/archiviazione, qualora le accuse risultino inesatte o infondate o qualora la segnalazione sia diventata irrilevante; in tal caso, la Persona Designata deve, senza indebito ritardo, avvisare per iscritto l'informatore che, sulla base dei fatti esposti nella segnalazione e delle circostanze a sua conoscenza, non è stato accertato alcun sospetto di comportamento illecito o che la segnalazione è risultata basata su informazioni non veritiere e deve inoltre avvisare l'informatore del suo diritto di presentare una segnalazione a un'autorità pubblica; oppure

(III) la conferma che la segnalazione è stata ritenuta fondata e che sono state proposte agli organi/alle autorità competenti misure adeguate a prevenire o porre rimedio alla situazione illecita e le informazioni sulle misure infine adottate saranno comunicate per iscritto all'informatore senza indebito ritardo.

Il Responsabile Designato conserverà le segnalazioni e i relativi documenti, compresi i dati personali, per un periodo di cinque (5) anni dalla data di ricezione della segnalazione.

4.2 CANALE DI SEGNALAZIONE ESTERNO

Gli informatori hanno il diritto di segnalare al Ministero della Giustizia della Repubblica Ceca. Le informazioni relative alla segnalazione al Ministero della Giustizia della Repubblica Ceca sono disponibili sul sito web: <https://oznamovatel.justice.cz/>

4.3 DIVULGAZIONE PUBBLICA

La divulgazione pubblica è consentita solo alle condizioni stabilite dalla legge ceca sulla protezione degli informatori. La divulgazione pubblica al di fuori delle condizioni elencate può comportare la perdita delle tutele.

Gli informatori possono effettuare una segnalazione esterna nelle seguenti circostanze:

- hanno già effettuato una segnalazione attraverso il canale interno di segnalazione e al Ministero, o solo al Ministero, e non sono state intraprese azioni appropriate entro i termini stabiliti dalla legge ceca sulla protezione degli informatori. In particolare, la Persona Designata non ha valutato la ragionevolezza della segnalazione ai sensi della sezione 12(3) della legge ceca sulla protezione degli informatori, la Società non ha adottato altre misure adeguate per prevenire o porre rimedio alla situazione illecita ai sensi dell'articolo 12, paragrafo 5, della legge ceca sulla protezione degli informatori, oppure un funzionario pubblico ai sensi dell'articolo 13 della legge ceca sulla protezione degli informatori non ha valutato la segnalazione ai sensi dell'articolo 17, paragrafo 1, della legge ceca sulla protezione degli informatori;

- abbiano motivi ragionevoli per ritenere che la violazione segnalata possa comportare una minaccia imminente o evidente all'ordine o alla sicurezza interna, alla vita o alla salute, all'ambiente o ad altri interessi pubblici, oppure un danno irreparabile; oppure
- hanno motivi ragionevoli per ritenere che, se la segnalazione viene effettuata tramite il sistema di segnalazione esterno, vi sia un rischio maggiore, date le circostanze del caso, che essi stessi o una persona descritta nella sezione 4(2)(a) - (h) della Legge ceca sulla protezione degli informatori siano oggetto di ritorsioni o che il processo di cui al Titolo III della Legge ceca sulla protezione degli informatori sia a rischio.

5.0 PERSONE DESIGNATE

La Società ha nominato le seguenti Persone Designate per gestire il canale di segnalazione interno, specificamente formate e in possesso dei requisiti di indipendenza e imparzialità:

- il Responsabile Compliance Globale (Global Compliance Manager); e
- il Responsabile Affari Legali, EMEA (Legal Manager, EMEA).

Le Persone Designate agiscono in modo autonomo e senza conflitti di interesse, garantiscono la riservatezza come standard e gestiscono le segnalazioni in conformità con la legge applicabile e la presente Politica.

In caso di conflitto di interessi effettivo, potenziale o percepito, la Persona Designata dovrà astenersi e il caso sarà prontamente riassegnato all'altra Persona Designata (o a un sostituto debitamente nominato) per garantire continuità, neutralità e un tempestivo follow-up.

6.0 PROTEZIONE CONTRO LE RITORSIONI E RISERVATEZZA

Il principio di non ritorsione si applica non solo ai Collaboratori, alle Persone associate o agli altri soggetti di cui alla Sezione 2 che effettuano una segnalazione ai sensi della Politica Globale e del presente Allegato alla Politica, ma anche ai facilitatori, come precedentemente definiti nella Politica Globale, a terzi collegati agli informatori quali colleghi, ex colleghi, consulenti e familiari, nonché alle persone giuridiche di cui l'informatore è proprietario, per le quali lavora o alle quali è collegato in un contesto lavorativo.

La legge della Repubblica Ceca stabilisce un elenco esaustivo di azioni o omissioni che possono essere considerate misure di ritorsione tra cui, a titolo esemplificativo ma non esaustivo, la cessazione del rapporto di lavoro, il licenziamento, le misure disciplinari, la riduzione dello stipendio, il trasferimento della sede di lavoro, il diniego di opportunità di sviluppo professionale, la richiesta di un certificato medico, qualsiasi tipo di discriminazione, la valutazione negativa delle prestazioni, le molestie, la mancata conversione del contratto a tempo determinato in contratto a tempo indeterminato, ecc.

DANIMARCA

1.0 SINTESI

Il presente Allegato alla Politica danese è inteso a integrare l'attuale Politica sul whistleblowing del Gruppo GPT e fornisce indicazioni relative all'attuazione della Legge danese sulla protezione degli informatori (la "Legge") in relazione a Cimbria A/S (la "Società").

La presente Politica di segnalazione del Gruppo, insieme al presente Allegato alla Politica, fornisce indicazioni agli informatori in conformità con la Legge.

2.0 CANALI DI SEGNALEZIONE

Gli informatori possono presentare segnalazioni tramite:

- canale di segnalazione interno;
- canale di segnalazione esterno;
- divulgazione pubblica.

2.1 CANALE DI SEGNALEZIONE INTERNO

Gli informatori potranno inviare segnalazioni interne tramite i canali indicati nella Politica Globale, facilmente accessibile tramite un link disponibile sul sito web della Società: [GPT Alertline](#).

Una volta effettuato l'accesso al portale, l'informatore può utilizzare i menu dedicati per selezionare il Paese della società del Gruppo a cui si riferisce la segnalazione prima di inviarla.

Il canale interno consente agli informatori:

- di presentare segnalazioni con qualsiasi mezzo (scritto o orale). Se una segnalazione viene fornita oralmente, può essere effettuata per telefono o, su richiesta dell'informatore, tramite videoconferenza o incontro di persona organizzato entro un lasso di tempo ragionevole. Qualsiasi registrazione audio richiede il consenso dell'informatore; in caso contrario, viene redatto e firmato un verbale scritto;
- di effettuare segnalazioni in forma anonima, qualora lo ritenga necessario.

L'informatore sarà avvisato per iscritto della ricezione della segnalazione entro sette (7) giorni dal suo ricevimento. La Persona Designata manterrà i contatti con l'informatore e potrà richiedere ulteriori informazioni.

La Persona Designata fornisce una risposta di follow-up entro tre (3) mesi dalla data di conferma di ricezione della segnalazione o, in mancanza di tale conferma, entro tre mesi dalla scadenza del termine di sette giorni lavorativi successivo alla presentazione della segnalazione. Nel follow-up, la Persona Designata avvisa l'informatore dell'esito della segnalazione, se possibile, ovvero: (i) chiusura/archiviazione (quando le accuse risultano inesatte o infondate o quando la segnalazione è diventata irrilevante), oppure (ii) conferma che la segnalazione è stata ritenuta fondata ed è stata inoltrata agli organismi/alle autorità competenti; tuttavia, tali avvisi devono

essere forniti all'informatore in conformità con la legislazione danese, considerando gli obblighi di riservatezza previsti dalla legge e la normativa sulla protezione dei dati. Se le misure o l'esito non sono stati determinati entro il periodo di tre (3) mesi, l'informatore sarà avvisato e riceverà notizie sul feedback previsto.

Durante la fase di indagine relativa alla segnalazione, potrebbero essere coinvolti consulenti esterni nella gestione del caso. A seconda della sua natura, questo potrebbe essere trasmesso alla polizia per ulteriori indagini.

Se l'identità dell'informatore è stata rivelata in relazione alla segnalazione e vengono avviati procedimenti legali contro la persona segnalata, l'informatore potrebbe essere chiamato a testimoniare nel corso del procedimento.

2.2 CANALE DI SEGNALAZIONE ESTERNO – AUTORITÀ NAZIONALE DANESE

La segnalazione può essere effettuata anche tramite un canale di segnalazione esterno e indipendente istituito dall'Autorità danese per la protezione dei dati ("Datatilsynet") per la gestione delle segnalazioni relative a violazioni del diritto dell'UE che rientrano nell'ambito di applicazione della Direttiva sugli informatori e quindi non segnalazioni relative ad altre gravi violazioni legali o altre questioni gravi.

Si incoraggia a presentare una segnalazione tramite il canale interno della Società, laddove la violazione possa essere efficacemente affrontata internamente e l'informatore ritenga che non vi sia alcun rischio di ritorsione. Tuttavia, è necessario sottolineare che la segnalazione tramite il canale interno o esterno è facoltativa, a condizione che la segnalazione riguardi le suddette violazioni del diritto dell'Unione Europea.

Link al sito di segnalazione esterno: <https://whistleblower.dk/indberet>

2.3 DIVULGAZIONE PUBBLICA

La divulgazione pubblica è consentita solo alle condizioni stabilite nella sezione 5(2) della Legge (ad esempio, precedente utilizzo di canali interni e/o esterni senza una risposta adeguata, rischio concreto di ritorsioni o pericolo per l'interesse pubblico). La divulgazione pubblica al di fuori di queste condizioni può comportare la perdita delle tutele.

3.0 PERSONE DESIGNATE

La Società ha nominato le seguenti Persone Designate per gestire il canale di segnalazione interna, specificamente formate e in possesso dei requisiti di indipendenza e imparzialità:

- il Responsabile Compliance Globale (Global Compliance Manager); e
- il Responsabile Affari Legali, EMEA (Legal Manager, EMEA).

Le Persone Designate agiscono in modo autonomo e senza conflitti di interesse, garantiscono la riservatezza di default e gestiscono le segnalazioni in conformità con la legge applicabile e la presente Politica.

In caso di conflitto di interessi effettivo, potenziale o percepito, la Persona Designata si asterrà e il caso sarà prontamente riassegnato all'altra Persona Designata (o a un sostituto debitamente nominato) per garantire continuità, neutralità e un tempestivo follow-up.

4.0 PROTEZIONE CONTRO LE RITORSIONI E RISERVATEZZA

La protezione contro le ritorsioni è garantita in conformità con le norme stabilite nella Legge, in particolare nelle sezioni 5-8. In sostanza, un informatore non deve essere soggetto a ritorsioni, incluse minacce o tentativi di ritorsione a seguito di una segnalazione o di una divulgazione pubblica in conformità con la Legge. Inoltre, all'informatore non deve essere impedito o tentato di impedirgli di effettuare una segnalazione.

La protezione si applica agli informatori che effettuano segnalazioni interne ed esterne, nonché divulgazioni pubbliche. Tuttavia, per le divulgazioni pubbliche la protezione si applica nei seguenti casi:

- quando l'informatore che effettua la divulgazione pubblica ha prima presentato una segnalazione interna ed esterna, o direttamente una segnalazione esterna, senza che siano state intraprese azioni appropriate in risposta alla segnalazione entro il termine applicabile;
- quando l'informatore che effettua la segnalazione pubblica ha fondati motivi per ritenere che la violazione possa rappresentare un pericolo imminente o evidente per l'interesse pubblico;
- quando l'informatore che effettua la segnalazione pubblica ha motivi ragionevoli per ritenere che la segnalazione a un sistema esterno comporti un rischio di ritorsioni o, a causa delle circostanze specifiche del caso, vi siano scarse possibilità che la violazione venga efficacemente affrontata.

Inoltre, la protezione si applica solo se l'informatore ha motivi ragionevoli per ritenere che le informazioni segnalate o divulgate fossero corrette al momento della segnalazione o della divulgazione e che le informazioni rientrassero nell'ambito di applicazione della legge.

In termini di riservatezza, la legge stabilisce che le Persone Designate che costituiscono l'ente interno di segnalazione e che gestiscono il canale interno, siano tenute al segreto professionale per quanto riguarda le informazioni contenute nelle segnalazioni. Tale obbligo di riservatezza si applica analogamente alle persone che, attraverso la divulgazione, vengono a conoscenza di tali informazioni. L'obbligo di riservatezza si applica anche ai dipendenti non autorizzati delle autorità che gestiscono sistemi di segnalazione esterni che vengono inavvertitamente a conoscenza di tali informazioni relative alle segnalazioni.

5.0 CONSERVAZIONE DEI DATI PERSONALI

Le segnalazioni e i relativi dati personali riguardanti i dipendenti saranno conservati per il tempo strettamente necessario al loro trattamento e, in generale, per cinque (5) anni dopo la cessazione del rapporto di lavoro, con riferimento all'articolo 4, paragrafo 1, della legge danese

sulla prescrizione, a meno che circostanze specifiche non impongano un periodo di conservazione più lungo, ad esempio a causa di procedimenti legali in corso o della prospettiva di tali procedimenti.

Le segnalazioni e i relativi dati personali riguardanti i clienti o altre terze parti saranno conservati per il tempo strettamente necessario al loro trattamento e, in generale, a fini di documentazione, per 3 anni con riferimento alla sezione 3(1) della legge danese sulla prescrizione, a meno che circostanze specifiche non impongano un periodo di conservazione più lungo, ad esempio a causa di procedimenti legali in corso o della prospettiva di tali procedimenti.

GERMANIA

1.0 SINTESI

Il presente Allegato alla Politica è inteso a integrare l'attuale Politica di segnalazione del Gruppo GPT affrontando le specifiche modifiche legislative che sono state implementate in Germania ai sensi della Direttiva UE 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione (Direttiva sulla segnalazione di irregolarità) e della normativa locale. In Germania, la protezione degli informatori è disciplinata dalla legge sulla protezione degli informatori "Gesetz zum Schutz von hinweisgebenden Personen", detta anche "Hinweisgeberschutzgesetz" o, in breve: "HinSchG".

Il presente Allegato alla Politica affronta quindi le differenze di applicazione rispetto alla Politica Globale che si applicano all'entità di GPT con sede in Germania, ovvero GrainProteinTech Climate Control Air Treatment Germany GmbH (la "Società").

Il presente Allegato fornisce avvisi agli informatori ai sensi dell'articolo 5(e) del Decreto Legislativo 24/2023. In caso di conflitto tra la Politica e il presente Allegato, per la Germania prevale il presente Allegato.

2.0 AMBITO DI APPLICAZIONE E SOGGETTI INTERESSATI

Il presente Allegato alla Politica si applica non solo a tutti i funzionari, amministratori, dipendenti e lavoratori temporanei (collettivamente, "Collaboratori") e a tutti gli agenti della Società, inclusi, a titolo esemplificativo ma non esaustivo, appaltatori, consulenti e rappresentanti (collettivamente "Persone Associate"), ma anche a:

- azionisti e titolari di diritti di voto nell'assemblea generale della Società;
- membri dell'organo amministrativo, direttivo o di vigilanza della Società;
- personale esterno e occasionale della Società;
- i co-appaltatori della Società e i loro subappaltatori;
- coloro che segnalano o divulgano pubblicamente informazioni su violazioni acquisite nell'ambito di un rapporto di lavoro con la Società che è poi cessato; e
- coloro il cui rapporto di lavoro con la Società deve ancora avere inizio, nei casi in cui le informazioni relative a violazioni siano state acquisite durante il processo di assunzione o altre trattative precontrattuali in Germania.

3.0 DEFINIZIONI

Ai sensi dell'HinSchG, le definizioni di "Informatore" e di "Comportamento segnalabile" ai sensi della presente Politica sono estese dalla legge tedesca come segue:

- informatore (denunciante protetto): è definito come «una persona fisica che abbia ottenuto informazioni su violazioni nell'ambito delle proprie attività professionali e che comunichi tali informazioni agli organismi di segnalazione previsti dalla legge tedesca sulla tutela degli informatori». Le violazioni sono atti o omissioni illegali che riguardano gli

ambiti giuridici contemplati dalla direttiva sulla segnalazione di irregolarità o che costituiscono abuso in quanto contrari all'obiettivo o allo scopo della direttiva;

- la condotta segnalabile (condotta impropria) include, oltre alle definizioni contenute nella Politica globale, tali violazioni.

È vietata la divulgazione di fatti, informazioni o documenti provenienti dai servizi di intelligence o che potrebbero danneggiare la sicurezza nazionale o interessi essenziali di sicurezza, nonché le divulgazioni in violazione di un obbligo di riservatezza in relazione a informazioni classificate, al segreto delle deliberazioni giudiziarie, all'obbligo di riservatezza da parte di avvocati operatori sanitari; tali casi non rientrano nell'ambito di applicazione della Politica Globale o del presente Allegato alla Politica.

4.0 CANALI DI SEGNALAZIONE

Gli informatori possono presentare segnalazioni tramite:

- canale di segnalazione interno;
- segnalazione esterna alle autorità esterne.

4.1 CANALE DI SEGNALAZIONE INTERNO

Gli informatori potranno inviare segnalazioni interne tramite i canali indicati nella Politica Globale, facilmente accessibile tramite un link disponibile sul sito web della Società: [GPT Alertline](#).

Una volta effettuato l'accesso al portale, l'informatore può utilizzare i menu dedicati per selezionare il Paese specifico della società del Gruppo a cui si riferisce la segnalazione prima di inviarla.

Il canale interno consente agli informatori:

- di presentare segnalazioni con qualsiasi mezzo (scritto o orale). Se una segnalazione viene fornita oralmente, può essere effettuata per telefono o, su richiesta dell'informatore, tramite videoconferenza o incontro di persona organizzato entro un lasso di tempo ragionevole. Qualsiasi registrazione audio richiede il consenso dell'informatore; in caso contrario, viene redatto e firmato un verbale scritto;
- di effettuare segnalazioni in forma anonima, qualora lo ritenga necessario.

L'informatore sarà avvisato per iscritto della ricezione della segnalazione entro sette (7) giorni dal suo ricevimento. La Persona Designata manterrà i contatti con l'informatore e potrà richiedere ulteriori informazioni.

La Persona Designata fornisce una risposta di follow-up entro tre (3) mesi dalla data di conferma di ricezione della segnalazione o, in mancanza di conferma, entro tre mesi dalla scadenza del periodo di sette giorni lavorativi successivi alla presentazione della segnalazione. Successivamente, la Persona Designata informerà l'informatore dell'esito della segnalazione, ovvero: (i) chiusura/archiviazione (quando le accuse risultano inesatte o infondate o quando la

segnalazione è diventata irrilevante), oppure (ii) conferma che la segnalazione è stata ritenuta fondata ed è stata inoltrata agli organismi/alle autorità competenti.

Le segnalazioni e i relativi dati personali saranno conservati per il tempo strettamente necessario al loro trattamento e, in ogni caso, non oltre cinque (5) anni dalla comunicazione dell'esito della procedura.

4.2 CANALE DI SEGNALAZIONE ESTERNO - AUTORITÀ NAZIONALI TEDESCHE

Gli informatori possono effettuare una segnalazione esterna alle seguenti autorità:

- Externe Meldestelle des Bundes beim Bundesamt für Justiz
[BfJ - Hinweisgeberstelle \(bundesjustizamt.de\)](https://www.bundesjustizamt.de/BfJ-Hinweisgeberstelle)
- Bundeskartellamt – per violazioni relative al diritto della concorrenza e al Digital Markets Act
https://www.bundeskartellamt.de/DE/Aufgaben/Kartelle/HinweiseAufKartellverstoesse/hinweiseaufverstoesse_node.html

5.0 PERSONE DESIGNATE

La Società ha nominato le seguenti Persone Designate per gestire il canale di segnalazione interno, specificamente formate e in possesso dei requisiti di indipendenza e imparzialità:

- il Responsabile Compliance Globale (Global Compliance Manager); e
- il Responsabile Affari Legali, EMEA (Legal Manager, EMEA).

Le Persone Designate agiscono in modo autonomo e senza conflitti di interesse, garantiscono la riservatezza come standard e gestiscono le segnalazioni in conformità con la legge applicabile e la presente Politica.

In caso di conflitto di interessi effettivo, potenziale o percepito, la Persona Designata si asterrà e il caso sarà prontamente riassegnato all'altra Persona Designata (o a un sostituto debitamente nominato) per garantire continuità, neutralità e un tempestivo follow-up.

6.0 PROTEZIONE CONTRO LE RITORSIONI E RISERVATEZZA

Il principio di non ritorsione si applica non solo ai Dipendenti, alle Persone collegate e agli altri soggetti di cui alla Sezione 2, che effettuano una segnalazione ai sensi della Politica Globale e del presente Allegato alla Politica, ma anche ai facilitatori, come precedentemente definiti nella Politica Globale, a terzi collegati agli informatori quali colleghi, ex colleghi, consulenti e familiari, nonché alle persone giuridiche di cui l'informatore è titolare, per le quali lavora o alle quali è collegato in un contesto lavorativo.

La ritorsione può includere, a titolo esemplificativo ma non esaustivo, la cessazione del rapporto di lavoro, la sospensione dal servizio, misure disciplinari, la riduzione dello stipendio, il trasferimento della sede di lavoro, qualsiasi tipo di discriminazione, una valutazione negativa



delle prestazioni, molestie, la mancata conversione del contratto a tempo determinato in contratto a tempo indeterminato, ecc.

ITALIA

1.0 SINTESI

Il presente Allegato alla Politica è inteso a integrare l'attuale Politica di segnalazione del Gruppo GPT affrontando le specifiche modifiche legislative che sono state implementate in Italia ai sensi della Direttiva UE 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione (Direttiva sulla segnalazione di irregolarità) e della normativa locale (Decreto Legislativo n. 24 del 10 marzo 2023, che attua la Direttiva sulla segnalazione di irregolarità in Italia e le linee guida dell'Autorità Nazionale Anticorruzione).

Il presente Allegato alla Politica affronta quindi le differenze di applicazione rispetto alla Politica Globale che si applicano alle entità di GPT situate in Italia, ovvero: Cimbria S.r.l.; GrainProteinTech Climate Control Air Treatment S.p.A.; Tecno Poultry Equipment S.p.A. (ciascuna la "Società").

Il presente Allegato fornisce notizie agli informatori ai sensi dell'articolo 5, lettera e), del Decreto Legislativo 24/2023. In caso di conflitto tra la Politica e il presente Allegato, per l'Italia prevale il presente Allegato.

2.0 AMBITO DI APPLICAZIONE E SOGGETTI INTERESSATI

Il presente Allegato alla Politica si applica non solo a tutti i funzionari, amministratori, dipendenti e lavoratori temporanei (collettivamente, "Collaboratori") e a tutti gli agenti della Società, inclusi, a titolo esemplificativo ma non esaustivo, appaltatori, consulenti e rappresentanti (collettivamente "Persone Associate"), ma anche a:

- azionisti e titolari di diritti di voto nell'assemblea generale della Società;
- membri dell'organo amministrativo, direttivo o di vigilanza della Società;
- personale esterno e occasionale della Società;
- co-appaltatori della Società e loro subappaltatori;
- volontari e tirocinanti (sia retribuiti che non retribuiti);
- coloro che segnalano o rendono pubbliche informazioni su violazioni acquisite nell'ambito di un rapporto di lavoro con la Società durante il periodo di prova;
- coloro che segnalano o rendono pubbliche informazioni relative a violazioni acquisite nell'ambito di un rapporto di lavoro con la Società che si è nel frattempo concluso; e
- coloro il cui rapporto di lavoro con la Società deve ancora avere inizio, nei casi in cui le informazioni relative alle violazioni siano state acquisite durante il processo di selezione o altre trattative precontrattuali con la Società.

3.0 DEFINIZIONI

Ai sensi del Decreto Legislativo n. 24/2023, le definizioni di Informatore e Comportamento Segnalabile ai sensi della presente Politica sono estese dalla legge italiana come segue:

- informatore (Segnalante protetto): è definito come "una persona fisica che segnala comportamenti, atti, omissioni che comportino violazioni (o fondato sospetto di violazioni) delle leggi e dei regolamenti italiani e dell'UE, riscontrati dall'informatore nell'ambito del rapporto di lavoro, che ledono l'interesse pubblico o l'integrità della pubblica amministrazione o di un soggetto privato e consistono in illeciti amministrativi, contabili, civili o penali o in comportamenti illeciti rilevanti".
- I comportamenti segnalabili (comportamenti scorretti) includono, oltre alle definizioni contenute nella Politica globale:
 1. reati civili, penali, amministrativi o contabili;
 2. comportamenti illeciti rilevanti ai sensi del Decreto Legislativo 231/2001;
 3. se applicabile, violazioni dei Modelli di Organizzazione e Gestione adottati ai sensi del Decreto Legislativo 231/2001 ("MOG 231");
 4. violazioni del diritto dell'Unione Europea in settori quali gli appalti pubblici; i servizi, i prodotti e i mercati finanziari; la prevenzione del riciclaggio di denaro e del finanziamento del terrorismo; la sicurezza dei prodotti; la sicurezza dei trasporti; la tutela dell'ambiente; ecc.;
 5. atti o omissioni che ledono gli interessi finanziari dell'UE;
 6. atti od omissioni che incidono sul mercato interno dell'UE (ostacolando la libera circolazione di beni, servizi, persone o capitali);
 7. violazioni delle misure restrittive dell'Unione Europea (sanzioni UE), incluse le violazioni delle disposizioni nazionali di attuazione, i reati penali o le violazioni amministrative relative ai regimi sanzionatori dell'UE, qualora tali violazioni siano individuate in un contesto lavorativo.

È vietata la divulgazione di fatti, informazioni o documenti relativi a un interesse personale dell'informatore che riguardi esclusivamente il suo rapporto di lavoro individuale, violazioni già disciplinate in modo vincolante da altre normative dell'UE o italiane, violazioni della sicurezza nazionale, informazioni classificate, segreto professionale forense e medico, deliberazioni giudiziarie e la divulgazione di fatti, informazioni o documenti raccolti illegalmente, che non rientreranno nell'ambito di applicazione della Politica Globale o del presente Allegato alla Politica.

4.0 CANALI DI SEGNALEZIONE

Gli informatori possono presentare segnalazioni tramite:

- Canale di segnalazione interno;
- Segnalazione esterna all'Autorità Nazionale Anticorruzione (ANAC) tramite la sua piattaforma online;
- Divulgazione pubblica (consentita solo alle condizioni specificate dall'articolo 15 del Decreto Legislativo 24/2023).

4.1 CANALE DI SEGNALEZIONE INTERNA

Gli informatori potranno inviare segnalazioni interne tramite i canali indicati nella Politica Globale, facilmente accessibile tramite un link disponibile sul sito web della Società: [GPT Alertline](#).

Una volta effettuato l'accesso al portale, l'informatore può utilizzare i menu dedicati per selezionare il Paese della specifica società del Gruppo a cui si riferisce la segnalazione prima di inviarla.

Il canale interno consente agli informatori:

- di presentare segnalazioni con qualsiasi mezzo (scritto o orale). Se una segnalazione viene fornita oralmente, può essere effettuata per telefono o, su richiesta dell'informatore, tramite videoconferenza o incontro di persona organizzato entro un lasso di tempo ragionevole. Qualsiasi registrazione audio richiede il consenso dell'informatore; in caso contrario, viene redatto e firmato un verbale scritto;
- di effettuare segnalazioni in forma anonima, qualora lo ritenga necessario.

L'informatore sarà avvisato per iscritto della ricezione della segnalazione entro sette (7) giorni dal suo ricevimento. Il Responsabile designato manterrà i contatti con l'informatore e potrà richiedere ulteriori informazioni.

La Persona Designata fornisce una risposta di follow-up entro tre (3) mesi dalla data di conferma di ricezione della segnalazione o, in mancanza di conferma, entro tre mesi dalla scadenza del periodo di sette giorni lavorativi successivi alla presentazione della segnalazione. Nel seguito, la Persona Designata informerà l'informatore dell'esito della segnalazione, ovvero: (i) chiusura/archiviazione (quando le accuse risultano inesatte o infondate o quando la segnalazione è diventata irrilevante), oppure (ii) conferma che la segnalazione è stata ritenuta fondata ed è stata inoltrata agli organismi/alle autorità competenti.

Le segnalazioni e i relativi dati personali saranno conservati per il tempo strettamente necessario al loro trattamento e, in ogni caso, non oltre cinque (5) anni dalla comunicazione dell'esito del procedimento.

4.2 CANALE DI SEGNALEZIONE ESTERNO - AUTORITÀ NAZIONALE ANTICORRUZIONE ("ANAC")

Gli informatori possono effettuare una segnalazione esterna nelle seguenti circostanze previste dal Decreto Legislativo:

- se non sia stato istituito un canale di segnalazione interno o questo non sia conforme agli standard richiesti;
- se abbiano già effettuato una segnalazione interna che non ha avuto seguito o ha avuto esito negativo;
- se hanno ragionevoli motivi per ritenere che una segnalazione interna non avrebbe seguito o potrebbe comportare ritorsioni (ad esempio, casi di conflitto di interessi in cui il responsabile della segnalazione coincide con l'informatore, la persona segnalata o è comunque una persona coinvolta o interessata dalla segnalazione);
- se abbiano ragionevoli motivi per ritenere che la violazione possa costituire un pericolo imminente o manifesto per il pubblico.

In Italia l'ANAC è un'autorità amministrativa indipendente con poteri di regolamentazione, indagine e sanzione in materia di segnalazione di irregolarità.

Gli informatori possono presentare segnalazioni esterne all'ANAC oralmente o per iscritto tramite la sua piattaforma informatica. Se una segnalazione viene effettuata oralmente, può avvenire per telefono o tramite qualsiasi altro sistema di segreteria telefonica oppure, su richiesta dell'informatore, tramite videoconferenza o incontro di persona entro un lasso di tempo ragionevole

L'ANAC è tenuta a confermare la ricezione della segnalazione entro sette (7) giorni dal ricevimento, a meno che l'informatore non ne faccia richiesta in senso contrario o qualora ciò possa compromettere la riservatezza della segnalazione. L'ANAC deve dare seguito alle segnalazioni con diligenza, svolgere le indagini necessarie e rispondere all'informatore entro tre (3) mesi (o sei (6) mesi in caso di giustificati motivi di ritardo) dalla conferma di ricezione, oppure, in assenza di tale conferma, entro tre (3) o sei (6) mesi dalla scadenza del termine di sette (7) giorni lavorativi successivi alla presentazione della segnalazione. Con la sua risposta, l'ANAC informerà l'informatore sull'esito dell'indagine, che può consistere anche nella chiusura della segnalazione, nella sua trasmissione ad altre autorità competenti, in una raccomandazione o nell'imposizione di sanzioni amministrative.

Maggiori informazioni sulla procedura di segnalazione tramite l'ANAC sono disponibili ai link sottostanti:

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

4.3 DIVULGAZIONE AL PUBBLICO

La divulgazione al pubblico è consentita solo alle condizioni di cui all'articolo 15 del Decreto Legislativo (ad esempio, previo ricorso a canali interni e/o esterni senza adeguata risposta, o concreto rischio di ritorsioni o pericolo per l'interesse pubblico). La divulgazione al pubblico al di fuori di tali condizioni può comportare la perdita delle tutele.

5.0 PERSONE DESIGNATE

La Società ha nominato le seguenti Persone Designate per la gestione del canale di segnalazione interna, specificamente formate e in possesso dei requisiti di indipendenza e imparzialità:

- il Responsabile Compliance Globale (Global Compliance Manager); e
- il Responsabile Affari Legali, EMEA (Legal Manager, EMEA).

Le Persone Designate agiscono in modo autonomo e senza conflitti di interesse, garantiscono la riservatezza di default e gestiscono le segnalazioni in conformità con la legge applicabile e la presente Politica.

In caso di conflitto di interessi effettivo, potenziale o percepito, la Persona Designata dovrà astenersi e il caso sarà prontamente riassegnato all'altra Persona Designata (o a un sostituto debitamente nominato) per garantire continuità, neutralità e un tempestivo follow-up.

6.0 PROTEZIONE CONTRO LE RITORSIONI E RISERVATEZZA

Il principio di non ritorsione si applica non solo ai Collaboratori, alle Persone associate e agli altri soggetti di cui alla Sezione 2, che effettuano una segnalazione ai sensi della Politica Globale e del presente Allegato alla Politica, ma anche ai facilitatori, come precedentemente definiti nella Politica Globale, a terzi collegati agli Informatori quali colleghi, ex colleghi, consulenti e familiari, nonché alle persone giuridiche di cui l'informatore è proprietario, per cui lavora o alle quali è collegato in un contesto lavorativo.

La legge italiana stabilisce un elenco esaustivo di atti e omissioni, anche solo tentati o minacciati, che possono essere considerati misure di ritorsione, tra cui, a titolo esemplificativo ma non esaustivo: licenziamento, cassa integrazione, provvedimenti disciplinari (comprese sanzioni pecuniarie e sospensione), riduzione dello stipendio, declassamento o mancata promozione, modifica delle mansioni, trasferimento della sede di lavoro, qualsiasi tipo di discriminazione, note di merito negative, referenze negative, molestie, emarginazione, mancata conversione del contratto a tempo determinato in contratto a tempo indeterminato, danno alla reputazione, annullamento di contratti di fornitura, richiesta di sottoporsi a visite psichiatriche o mediche.