POLICY GUIDE

GROUP WHISTLEBLOWING POLICY

NUMBER: COMP-02GPT | ORIGINAL EFFECTIVE DATE: 01/01/2026

TABLE OF CONTENTS:

1.0 PURPOSE OF THE GROUP WHISTLEBLOWING POLICY

Grain & Protein Technologies ("GPT", the "Group") is committed to maintaining the highest standards of integrity, ethics and compliance throughout all aspects of its business. It believes that ethical conduct, transparency, and accountability are fundamental to building trust with its employees, stakeholders, and the communities in which it operates.

In line with this commitment, GPT encourages all individuals, both within GPT and among third parties who interact with GPT in a work-related context to report any suspected misconduct, irregularities, breaches of laws, or internal policies. Such reports are essential for safeguarding GPT's integrity and reputation, and for ensuring a safe, fair and compliant workplace.

This Global Policy applies globally and is designed to comply with applicable whistleblower protection laws in the jurisdictions where GPT operates. It outlines what can be reported, how reports are submitted, the procedural steps followed after a report is received, and the protections offered to those raising concerns.

In the event of any conflict between this Policy and applicable legislation, the legal provisions shall prevail. This Policy applies to all members of the GPT Group, but due to different local legal requirements, we have created annexes or separate local policies to address specific needs and ensure compliance with national regulations.

GPT strictly prohibits retaliation against anyone who reports misconduct in good faith or participates in related investigations. Individuals are protected from discrimination, harassment, or any adverse treatment resulting from their report as further described in this Policy.

2.0 SCOPE AND DEFINITIONS

Any individual, including external parties, who has acquired information on breaches in the work-related context may submit a report. This includes especially:

- current and former employees and officers of GPT;
- self-employed individuals and contractors providing services to the Group;
- shareholders and members of GPT's bodies, including non-executive members;
- volunteers, paid or unpaid trainees and interns;
- persons working under the supervision and direction of contractors, subcontractors and suppliers;
- business partners, including customers, suppliers, advisers, agents and their employees, who have or had a professional relationship with GPT.

3.0 WHISTLEBLOWER PROTECTION

For the purposes of this Policy, a Whistleblower is any individual who has reasonable grounds to suspect that misconduct, an improper situation, or a breach of law or internal policy has

occurred in relation to GPT ("Reportable Conduct") and who discloses such concerns through one of the reporting channels described in this Policy.
GPT is committed to protecting individuals who make reports in good faith and in accordance with this Policy ("Protected Disclosure"). Whistleblowers must not suffer any form of retaliation, reprisal, discrimination, harassment, or disadvantage as a result of making a Protected Disclosure.

The identity of the Whistleblower, and any information from which that identity might be directly or indirectly inferred, will be kept strictly confidential and will not be disclosed without the Whistleblower's explicit consent, except:

- Where required by applicable law;
- Where disclosure is reasonably necessary to investigate the report or to comply with legal proceedings, provided confidentiality is preserved to the fullest extent permitted by law; or
- Where the disclosure is made to competent regulatory authorities, law enforcement agencies, or professional advisers who are bound by confidentiality obligations.

4.0 WHAT SHOULD BE REPORTED UNDER THIS POLICY?

Any matter that a person reasonably believes breaches GPT's policies, ethical standards, or applicable laws and regulations should be reported in accordance with this Policy.

Examples of Reportable Conduct may include:

- breaches of laws or regulations;
- unlawful, corrupt, fraudulent or irregular activities involving the use of GPT's funds, assets or property;
- illegal or criminal conduct, including theft, drug sales or use, violence or threatened violence;
- breaches of GPT's policies and procedures (including but not limited to the Code of Conduct);
- conduct that poses a significant risk to public health, safety or the environment;
- dishonest, unethical or abusive behavior in the workplace;
- financial fraud, mismanagement or accounting irregularities;
- conduct likely to damage GPT's financial position, reputation or stakeholders' trust;
- gross negligence, discrimination, harassment or oppressive behavior;
- concealment or attempted concealment of misconduct or an improper state of affairs;

Additional examples, where required by local whistleblowing laws, are further detailed in the country-specific Annexes of this Policy.
A person may also use the "*Ask a Question*" option instead of submitting a formal report. In such case, GPT will assess the question and provide a response. If the matter appears to fall within the scope of Reportable Conduct, GPT may, at its discretion, reclassify the question as a report to ensure that it is handled appropriately under this Policy.

Reportable Conduct must be distinguished from personal work-related grievances. A personal work-related grievance refers to any matter connected to an individual's current or former employment that affects them personally but does not indicate misconduct or a breach of law or internal policies.

Examples of personal work-related grievances include, but are not limited to:

- interpersonal conflicts or disputes between employees;
- decisions relating to transfers, promotions or performance evaluations;
- disciplinary measures, warnings, or employment termination decisions.

Reports alleging discrimination, harassment, retaliation, or other violations of employment laws are not considered personal work-related grievances and fall within the scope of this Policy. Personal work-related grievances, as described above, that do not involve Reportable Conduct are usually best handled through a direct manager, leader or Human Resources channel, which are designed to address employment-related concerns fairly and promptly.

If you are not sure whether a concern falls within this Policy, you may contact the GPT's Legal & Compliance Department at GPTCompliance@grainproteintech.com for confidential guidance on how best to proceed.

5.0 WHO AND HOW SHOULD I REPORT TO?

GPT has established secure and confidential whistleblowing channels for the submission of the reports.

Where required by the EU Whistleblowing Directive (EU) 2019/1937 or other applicable federal, state, or local legislation, GPT has appointed Designated Persons, who are authorized to receive and follow up on whistleblowing reports in compliance with legal requirements.

Employees and other eligible individuals who wish to make a report may, instead of submitting it directly to the General Counsel & Head of Compliance or other management representatives, choose to report confidentially and, if desired, anonymously, through the GPT Alertline. Nothing in this Policy requires individuals to report internally before reporting concerns to governmental or regulatory authorities where such reporting is protected by applicable law.

The GPT Alertline is powered by NAVEX, an independent third-party service engaged by GPT to receive and document reports from employees and external parties, and to transmit them securely to the appropriate internal personnel for assessment and follow-up. It is operated outside the Company's website and corporate network to ensure confidentiality and independence.

The AlertLine provides both web-based and telephone reporting options. The relevant links and telephone numbers can be found easily on GPT's website GPT Alertline and on each GPT group company's website as indicated in the country-specific Annexes of this Policy.

Once logged into the AlertLine, the Whistleblower can use the dedicated menus to select the specific Group company country to which the report relates before submission.

The whistleblowing channels enable reporting in writing or via the GPT Alertline. Upon your request, a whistleblower may also request to make a report through an in-person meeting with the Designated Person. Such a meeting will be arranged within a reasonable timeframe after the request is made, in compliance with the applicable law. Any audio recording requires the Whistleblower's explicit consent; otherwise, a written record or summary is prepared and signed.

If, for any reason and by any means, a report falling under the scope of this Policy is received outside the designated whistleblowing channels, the person who receives it must immediately ensure the confidentiality of all information included in the report.

They are strictly prohibited from disclosing the identity of the Whistleblower, the reported person, or any other individual mentioned in the report, as well as any information that could directly or indirectly lead to their identification. The recipient must also advise the Whistleblower to follow the official reporting procedure established by this Policy and/or forward the report to the GPT Legal and Compliance Department without undue delay and, in any event, no later than seven (7) days of receipt. Once the confirmation of receipt is obtained from the designated reporting handler, any copies or records of the report (including emails or notes), must be securely deleted to ensure full confidentiality and data protection compliance.

6.0 CAN I REPORT CONCERNS OUTSIDE OF GPT?

Whistleblowers are primarily encouraged to use the internal reporting channels established by GPT.

However, under specific conditions defined by applicable laws and regulations, individuals may also make an external report directly to the competent authorities in accordance with the relevant local and/or international regulations.

Reporters should refer to the country-specific Annexes of this Policy for further details on the external reporting procedures and competent authorities applicable to their jurisdictions.

7.0 CONTENT OF REPORTS

To enable GPT to respond and, where appropriate, investigate an allegation effectively, reports should be factual rather than speculative and include as much specific information as

possible. This allows GPT to properly assess the nature, extent and urgency of the matter that is being reported.

For a proper assessment and investigation, it is advisable that the report includes, where available, the following information:

I. Background and description of the concern, including relevant facts and reasons for the report;
II. name(s) of the individual(s) involved or implicated;
III. name(s) of any witnesses;
IV. date, time and place of the incident(s);
V. details or any copies of any supporting evidence or documentation;
VI. information on any funds, assets, or interests affected;
VII. indication of how often the incident has occurred (if applicable).

The Whistleblowing mechanism must not be used improperly. Reports made in bad faith, including those that are knowingly false or made solely to harm another person, are strictly prohibited. Such conduct may result in disciplinary measures or, where applicable, legal actions, in accordance with the laws of the relevant state.

However, no action will be taken against a Whistleblower who submits a report in good faith, even if the facts reported are subsequently found to be incorrect or unsubstantiated.
GPT is committed to protecting good-faith Whistleblowers from retaliation and ensuring that the reporting mechanism is used responsibly and ethically.

8.0 CONFIDENTIALITY/ANONYMITY

Allegations the reporter has chosen to report openly, and not anonymously

GPT promotes an open and transparent culture and encourages individuals to raise any concerns openly whenever possible. Doing so facilitates a more effective assessment, investigation, and follow-up of the matter.

When a Whistleblower has chosen to provide their identification along with their report, GPT will make all reasonable efforts to ensure that the Whistleblower's identity is kept confidential, unless such disclosure is required by applicable law, regulation, or judicial proceedings. In all cases, the reports will be handled in accordance with applicable data protection and whistleblowing regulations.

Allegations where the reporter has chosen to report anonymously

GPT recognizes that, in some situations, the Whistleblower might feel more comfortable reporting their concerns anonymously. The possibility of submitting anonymous reports depends on applicable laws and regulations. Where allowed, such reports will be assessed and, where feasible, investigated with the same care as non-anonymous reports.

Whistleblowers who initially report anonymously – or who, where and when permitted by the applicable law, make an anonymous public disclosure – will remain protected under this Policy if their identity is later revealed, provided they satisfy the other conditions set out in this Policy.

However, Whistleblowers should be aware that, in some cases, it may be difficult to properly conduct a full investigation without knowing the identity of the reporter, particularly when follow-up clarifications, interviews or verification of facts are needed.

9.0 ASSESSMENT AND HANDLING OF REPORTS

GPT takes every report of suspected or potential breaches seriously. All reports submitted through the designated whistleblowing channels will be handled fairly, appropriately and without undue delay. The Whistleblower will receive an acknowledgement of receipt of the report within seven days (7) from the date it was received. Acknowledgment may be delayed where immediate action is required to preserve evidence or address an imminent risk, in compliance with applicable law.

GPT is committed to ensuring thorough and impartial follow-up on all reports. Investigations are carried out by qualified personnel or external experts and consultants where appropriate. GPT ensures that all relevant facts are collected, documented, and assessed objectively with full respect of confidentiality and data protection obligations. For this reason, the need for confidentiality, privacy safeguard, and compliance with applicable legal obligations may limit the extent to which specific details about the investigation, the actions taken or the resulting action could be shared with the Whistleblower. Any information provided to the Whistleblower regarding the progress made or the outcome of the investigation must be treated as strictly confidential.

GPT will provide feedback to the Whistleblower within a reasonable time, and in any event no later than three (3) months from:

- the acknowledgment of the receipt of the report;
- where no acknowledgment is sent, the expiry of the seven-day acknowledgment period.

GPT cannot guarantee the outcome of the investigation will align with the Whistleblower's expectation or desired result. However, it is fully committed to ensure that all genuine concerns are treated fairly, respectfully, and diligently.

If, during the assessment or the investigation, it appears that the facts noted in the report may constitute a criminal offence, the designated reporting handler, in agreement with other competent corporate functions and group management, will assess whether, when, and how to refer the matter to the competent judicial or regulatory authorities, in compliance with applicable local laws and regulations.

10.0 RETENTION OF THE REPORTS

Written and electronic copies of all reports will be securely retained in accordance with GPT's documented data retention schedule. The reports submitted via the GPT Alertline will be stored electronically within the NAVEX secure reporting platform.

All records and supporting documentation shall be retained only for as long as required to comply with applicable legal and regulatory requirements.

Where appropriate, GPT will anonymize or pseudonymize any personal data included in a report, within a reasonable timeframe, following conclusion of the investigation, in compliance with all applicable data protection laws, including, where applicable, the General Data Protection Regulation (GDPR).

11.0 PROHIBITION OF RETALIATION

Retaliation means any direct or indirect act or omission occurring in a work-related context that arises as a consequence of an internal or external report, or a public disclosure made under this Policy, and which causes or may cause unjustified and unfair harm to the Whistleblower.
No Whistleblower who raises a concern in good faith about matters covered by this Policy shall suffer any form of retaliation. Any individual who engages in retaliation may be subject to disciplinary action, up to and including termination, regardless of position or seniority.
GPT is firmly committed to protecting Whistleblowers who make disclosures in good faith from retaliation, harassment, or any other adverse treatment. All Whistleblowers will be treated with respect, dignity, and confidentiality throughout the process.

Retaliation includes, but is not limited to, threats or attempts of retaliation, and may take the form of:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in pay, or alteration of working hours;
- negative performance evaluation or employment reference;
- disciplinary action, reprimand, or other penalty, including financial penalties;
- coercion, intimidation, harassment, or ostracism;
- discrimination or other forms of disadvantageous or unfair treatment;
- failure to convert a fixed-term employment contract into a permanent one where a legitimate expectation existed;
- non-renew or early termination of a temporary employment contract;
- reputational harm (including through social media), or financial loss, such as loss of business or income;
- blacklisting within a sector or industry-wide, whether formal or informal;
- early termination or cancellation of a contract for goods or services;

- withdrawal or refusal of a license or permit;
- unjustified psychiatric or medical referrals.

The protection measures set out in this Policy also extend, where applicable, to:

- Facilitators, meaning individuals who assist a Whistleblower in the reporting process in a work-related context, and whose assistance should be confidential;
- Third persons connected to the Whistleblowers who may face retaliation in a work-related context, such as colleagues or relatives; and
- Legal entities owned by, working for, or otherwise connected to the Whistleblower in a professional capacity.

12.0 PROCESSING OF PERSONAL INFORMATION

Any processing of personal data carried out pursuant to this Policy, including the transmission or exchange of information with competent authorities, shall comply with all applicable data protection laws. Similarly, reports involving entities or individuals located in different jurisdictions may be shared between relevant GPT entities strictly on a need-to-know basis and in compliance with applicable data protection and whistleblowing laws.

Personal data that are manifestly not relevant to the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.
GPT shall ensure that all personal data processed in connection with whistleblowing reports are handled securely, lawfully, and proportionately, with access strictly limited to those persons authorized to process such personal data for legitimate purposes.

13.0 REPORTING SYSTEM OVERSIGHT

The effectiveness of this Policy and the functioning of the whistleblowing system are periodically reviewed by the GPT Legal & Compliance Department. This Policy may be updated to reflect changes in applicable laws and regulations, organizational structure, or best practice standards.

14.0 REPORTS TO GOVERNMENTAL AND REGULATORY AUTHORITIES

These procedures are in no way intended to limit the rights of employees to report alleged violations relating to accounting or auditing matters to proper governmental and regulatory authorities.

15.0 CONTINUATION AND MODIFICATION

As with any policy or benefit program, Grain & Protein Technologies reserves the unrestricted right, consistent with the law, to review, reconsider, interpret, amend, modify, suspend or discontinue all or any portion of such policy, plan or program at any time with or without notice. If any provision of this policy conflicts with or violates any applicable statute or regulation, the provisions of such statute or regulation will control. No modification, suspension, or

discontinuation of this Policy shall affect protections afforded to Whistleblowers under applicable law.

QUESTIONS REGARDING THIS POLICY GUIDE SHOULD BE REFERRED TO THE LEGAL & COMPLIANCE DEPARTMENT.

Description	Effective Date	Change Made By Name and Title
Policy Creation	01/01/2026	Patrick Rykhus, GC

ANNEX A: Additional Country-Specific Provisions (by region)

This Appendix highlights certain countries in which GPT operates that have Whistleblower related laws that may be applicable to your circumstances as a Whistleblower.

AUSTRIA

1.0 SUMMARY

This Policy Annex is intended to supplement the existing GPT Group Whistleblowing Policy by addressing the specific legislative changes that have been implemented in Austria pursuant to EU Directive 2019/1937 on the Protection of Persons Who Report Breaches of Union Law (Whistleblowing Directive) and local regulation [Austrian Whistleblower Protection Act (*HinweisgeberInnenschutzgesetz – "HSchG"*)].

This Policy Annex therefore addresses the differences in application from the Global Policy which apply in GPT's entity located in Austria namely: **Cimbria Heid Gmbh** (the "Company") and contains specific local provisions regarding the Austrian entities and applying to all individuals stated in Section 2 of the Policy and only insofar the HSchG is applicable.

2.0 SPECIFIC LOCAL PROVISIONS DEVIATING FROM THE POLICY

2.1 Scope based on HSchG

The Austrian Whistleblower Protection Act (HSchG) is applicable in case of violations in the following areas:

- Public Procurement;
- Financial services, financial products and financial markets as well as the prevention of money laundering and terrorist financing;
- Product safety and conformity;
- Road safety;
- Environmental protection;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and animal welfare;
- Public Health;
- Consumer protection;

- Protection of privacy and personal data as well as security of network and information systems;
- Prevention and punishment of criminal offenses according to §§ 302 to 309 of the Criminal Code (StGB), Federal Law Gazette I No. 60/1974;
- Financial interests of the Union within the meaning of Art 325 of the Treaty on the Functioning of the European Union (TFEU), e.g. improper use of EU funds;
- Internal market rules within the meaning of Art 26 (2) TFEU and Union rules on competition and state aid.

2.2 IN-PERSON MEETING

In case a Whistleblower wants to make a report by means of an in-person meeting with the Designated Person, such meeting shall take place within fourteen (14) calendar days after the request is made.

2.3 FEEDBACK PERIOD

GPT will give feedback to the Whistleblower regarding the submitted report within a reasonable time, which will be no more than three (3) months after the report was submitted.

3.0 EXTERNAL REPORTING CHANNEL

Whistleblowers are primarily encouraged to report concerns using the internal channel. However, if such an option is not possible or appropriate, if it is not reasonable to handle the information in the internal whistleblower system or if it has proven to be unsuccessful or futile, a Whistleblower can submit a report externally to the Federal Bureau of Anti-Corruption and Prevention of Corruption (Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung).

§ 15 (2) HschG names the following additional External Reporting Channels:

- Auditor supervisory authority (on the basis of the Auditor Supervision Act);
- Accounting authority (on the basis of the Accounting Act);
- Federal Competition Authority (on the basis of the Competition Act);
- Financial Market Authority (on the basis of the Financial Market Authority Act);
- Money Laundering Reporting Office (on the basis of the Federal Criminal Police Office Act);
- Notarial chambers (on the basis of the Notarial Code);
- Bar Associations (on the basis of the Disciplinary Statute for Lawyers and Trainee Lawyers);
- Chamber of Tax Consultants and Auditors (on the basis of the Act on the Public Accounting Profession).

3.1 PUBLIC DISCLOSURE

Public disclosure is permitted only under the conditions set out in the Austrian Whistleblower Protection Act and disclosure outside those conditions may result in the loss of protections.

Whistleblowers may make an external report in the following circumstances:

- They have already made a report through the internal and external whistleblowing channels (or just externally to the competent authority) but no appropriate action was taken or is intended to be taken within:
    I. three (3) months after the report was submitted through the internal whistleblowing channel or
    II. three (3) months (or up to six (6) months in duly justified cases) after the report was submitted through an external whistleblowing channel;
- They have reasonable grounds to believe that:
    I. the infringement referred to in the report may lead to an imminent or obvious threat to the public interest, such as where there is an emergency situation or the risk of irreversible damage; or;
    II. they have reasonable grounds to believe that, if the report is made through the external reporting system, there is a risk of retaliation, or a low chance the issue will be effectively handled. This could be because evidence might be hidden or destroyed, or because the authority involved is not trustworthy or is connected to the problem.

4.0 DESIGNATED PERSONS

The Company has appointed the following **Designated Persons** to manage the internal reporting channel, specifically trained and meeting the requirements of independence and impartiality:

- the Global Compliance Manager; and
- the Legal Manager, EMEA.

The Designated Persons act autonomously and without conflicts of interest, ensure confidentiality by default, and handle reports in accordance with applicable law and this Policy.
In case of any actual, potential, or perceived conflict of interest, the Designated Person shall abstain, and the case will be promptly reassigned to the other Designated Person (or to a duly appointed substitute) to guarantee continuity, neutrality, and timely follow-up.

5.0 PROTECTION AGAINST RETALIATION & CONFIDENTIALITY

Retaliation against a Whistleblower who in good faith raises a concern involving matters covered by the HSchG (see Section 1.0 above) is legally invalid.

6.0 PROCESSING OF PERSONAL INFORMATION

In addition to the legal provisions stated in Section 11.0 of the Policy in Austria processing of personal data with regard to whistleblowing reports is governed by Section 8 of the HSchG as well as the provisions of the Austrian Data Protection Act (*Datenschutzgesetz* – "DSG").

6.1 RETENTION PERIOD

Personal data must be stored by GPT for five (5) years after the report case is closed and beyond that for as long as is necessary to carry out administrative or judicial proceedings that have already been initiated or investigative proceedings under the Code of Criminal Procedure (*Strafprozessordnung* – "StPO").

Processing operations actually carried out, such as changes, queries and transmissions, must be logged. Log data on these processes must be kept three(3) years after the five (5) years retention obligation ceases to apply.

CZECH REPUBLIC

1.0 SUMMARY

This Policy Annex is intended to supplement the existing GPT Group Whistleblowing Policy by addressing the specific legislative changes that have been implemented in the Czech Republic pursuant to EU Directive 2019/1937 on the Protection of Persons Who Report Breaches of Union Law (Whistleblowing Directive) and local regulation. The main legal basis with regard to whistleblowing in the Czech Republic is the Act No. 171/2023 Coll., on the Protection of Whistleblowers (the "Czech Whistleblower Protection Act").

This Policy Annex therefore addresses the differences in application from the Global Policy which apply in GPT's entity located in the Czech Republic, namely: Cimbria HMD, s.r.o. (the "Company").

2.0 SCOPE OF APPLICATION & ENTITIES COVERED

This Policy Annex applies not only to all officers, directors, employees and temporary workers (collectively, "Associates") and to all agents of the Company including but not limited to, contractors, consultants and representatives (collectively "Associated Persons") but also to:

- shareholders and holders of voting rights in the Company's general assembly;

- members of the Company's administrative, management or supervisory body;
- external and occasional staff of the Company;
- co-contractors of the Company and their subcontractors;
- volunteers or interns;
- those who report or publicly disclose information on breaches acquired in a work-based relationship with the Company which has since ended; and
- those whose work-based relationship with the Company is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations in the Czech Republic.

3.0 DEFINITIONS

The definitions of Whistleblower and Reportable Conduct under this Policy are extended under Czech law as follows:

- Whistleblower (Protected Discloser): is defined as "a natural person who notifies of a possible infringement that has occurred or is about to occur and has the characteristics of a criminal offence or misdemeanor or violates whistleblowing law or another legal regulation or financial interest of the European Union or its internal market";
- Reportable Conduct (Improper Conduct) includes, in addition to definitions in the global Policy, such infringement.

The disclosure of facts, information or documents that could threaten national security, relates to activities of the intelligence services or the notification of which would constitute a violation to maintain the confidentiality of the clergy in the exercise of confessional secrecy is prohibited and will not fall within the scope of the Global Policy or this Policy Annex.

4.0 REPORTING CHANNELS

Whistleblowers may submit reports through:

- Internal reporting channel;
- External reporting to the Ministry of Justice of the Czech Republic;
- Public Disclosure (allowed only under specific conditions identified by the Law).

4.1 INTERNAL REPORTING CHANNEL

Whistleblowers will be able to submit internal reports via the channels indicated in the Global Policy, which is easily accessible via a link available on the Company's website: GPT Alertline Once logged into the portal, the Whistleblower can use the dedicated menus to select the specific Group company country to which the report relates before submission.

The internal channel allows Whistleblowers:

- to submit reports by any means (written or oral). If a report is given orally, it can be done by telephone or where requested by the Whistleblower, can choose by a video conference or a physical meeting organized within a reasonable time frame, but no later than fourteen (14) days from the date the request was made.
- Any audio recording requires the Whistleblower's consent; otherwise, a written minute is prepared and signed. The Designated Person shall give the Whistleblower an opportunity to comment on the written record of the report or transcript of the audio recording. The Whistleblower's comments shall be attached to the recording or transcript.
- to report anonymously, if they consider it necessary.

The Whistleblower will be informed in writing of the receipt of the report within seven (7) days of its receipt. The Designated Person will maintain communications with the Whistleblower and may request further information from them.

The Designated Person is obliged to assess whether the report is well-founded and to inform the Whistleblower in writing of the outcome of this assessment within thirty (30) days of the date of receipt of the report. In cases that are factually or legally complex, this time limit may be extended by up to 30 days, but no more than twice. The Designated Person is obliged to inform the Whistleblower in writing of the extension of the time limit and the reasons for such extension before the original time limit expires.

In the follow-up the Designated Person shall inform the Whistleblower of the outcome of the report, namely:

(I) informs that the submission does not constitute a report within the meaning of the Czech Whistleblower Protection Act; in such a case, the Designated Person shall, without undue delay, inform the Whistleblower in writing about that;

(II) closure/archiving, where the allegations are found to be inaccurate or unfounded, or when the report has become irrelevant; in such a case, the Designated Person shall, without undue delay, inform the Whistleblower in writing that, on the basis of the facts set out in the report and the circumstances known to them, no suspicion of unlawful conduct has been established, or that the report has been found to be based on untrue information, and shall also inform the Whistleblower of their right to lodge a report with a public authority; or

(III) confirmation that the report has been found well-founded and that appropriate measures to prevent or remedy the unlawful situation have been proposed to the competent bodies/authorities, and information on the measures ultimately adopted will be communicated to the Whistleblower in writing without undue delay.

The Designated Person will retain the reports and related documents including the personal data for a period of five (5) years from the date of receipt of the report.

4.2 EXTERNAL REPORTING CHANNEL

Whistleblowers have the right to report to the Ministry of Justice of the Czech Republic. Information about reporting to the Ministry of Justice of the Czech Republic is set out on the website: https://oznamovatel.justice.cz/

4.3 PUBLIC DISCLOSURE

Public disclosure is permitted only under the conditions set out in the Czech Whistleblower Protection Act. Public disclosure outside the listed conditions may result in the loss of protections.

Whistleblowers may make an external report in the following circumstances:

- They have already made a report through the internal whistleblowing channel and to the Ministry, or only to the Ministry, and appropriate action has not been taken within the time limits set out in the Czech Whistleblower Protection Act. In particular, the Designated Person has not assessed the reasonableness of the report under section 12(3) of the Czech Whistleblower Protection Act, the Company has not taken other appropriate action to prevent or remedy the unlawful condition under the section 12(5) of the Czech Whistleblower Protection Act, or a civil servant under section 13 of the Czech Whistleblower Protection Act has not assessed the report under the section 17(1) of the Czech Whistleblower Protection Act;
- they have reasonable grounds to believe that the infringement referred to in the report may lead to an imminent or obvious threat to internal order or security, life or health, the environment or other public interest or to irreparable harm; or;
- they have reasonable grounds to believe that, if the report is made through the external reporting system, there is an increased risk, given the circumstances of the case, that they or a person described in section 4(2)(a) through (h) of the Czech Whistleblower Protection Act will be subject to retaliation or that the Title III process of the Czech Whistleblower Protection Act is at risk.

5.0 DESIGNATED PERSONS

The Company has appointed the following Designated Persons to manage the internal reporting channel, specifically trained and meeting the requirements of independence and impartiality:

- the Global Compliance Manager; and
- the Legal Manager, EMEA.

The Designated Persons act autonomously and without conflicts of interest, ensure confidentiality by default, and handle reports in accordance with applicable law and this Policy.

In case of any actual, potential, or perceived conflict of interest, the Designated Person shall abstain, and the case will be promptly reassigned to the other Designated Person (or to a duly appointed substitute) to guarantee continuity, neutrality, and timely follow-up.

6.0 PROTECTION AGAINST RETALIATION & CONFIDENTIALITY

The principle of no retaliation not only applies to Associates, Associated Persons and to the other subjects referred to in Section 2, who make a report under the Global Policy and this Policy Annex but also to facilitators, as previously defined in the Global Policy, third parties connected with the Whistleblowers such as colleagues, ex-colleagues, consultants and family members and legal entities that the Whistleblower owns, works for or is connected within a work-related context.

The Czech Republic law sets out an extensive list of actions or omissions that can be considered as retaliatory measures, which include, but are not limited to employment termination, layoff, disciplinary measures, reduction of salary, transfer of place of work, not allowing professional development, requiring a medical report, any type of discrimination, negative performance review, harassment, non-conversion of fixed-term contract into permanent contract etc.

DENMARK

1.0 SUMMARY

This Danish Policy Annex is intended to supplement the existing GPT Group Whistleblowing Policy by and provides guidance regarding the implementation of the Danish Whistleblower protection Act (the "Act") with respect to Cimbria A/S (the "Company").

This Group Whistleblowing Policy, together with this Policy Annex, provides information to Whistleblowers in accordance with the Act.

2.0 REPORTING CHANNELS

Whistleblowers may submit reports through:

- Internal reporting channel;
- External reporting channel;
- Public Disclosure.

2.1 INTERNAL REPORTING CHANNEL

Whistleblowers will be able to submit internal reports via the channels indicated in the Global Policy, which is easily accessible via a link available on the Company's website: GPT Alertline Once logged into the portal, the Whistleblower can use the dedicated menus to select the specific Group company country to which the report relates before submission.

The internal channel allows Whistleblowers:

- to submit reports by any means (written or oral). If a report is given orally, it can be done by telephone or where requested by the Whistleblower, can choose by a video conference or a physical meeting organized within a reasonable time frame. Any audio recording requires the Whistleblower's consent; otherwise, a written minute is prepared and signed;
- to report anonymously, if they consider it necessary.

The Whistleblower will be informed in writing of the receipt of the report within seven (7) days of its receipt. The Designated Person will maintain communications with the Whistleblower and may request further information from them.

The Designated Person provides a follow-up reply within three (3) months from the date of acknowledgement of receipt of the report or, if no acknowledgement is received, three months from the expiry of the period of seven working days following the report being made. In the follow-up the Designated Person shall inform the Whistleblower of the outcome of the report, if possible, namely: (i) closure/archiving (when the allegations are found to be inaccurate or unfounded, or when the report has become irrelevant), or (ii) confirmation that the report has been found well-founded and has been forwarded to the competent bodies/authorities, however such information shall be provided to the Whistleblower in accordance with Danish legislation, inter alia. statutory confidentiality obligations as well as data protection regulation. If the measures or outcome has not been determined within the three (3) month-period, the Whistleblower will be informed of this as well as information on the expected feedback.

During the investigation phase concerning the report, external advisors may be involved in the handling of the case. Depending on the nature of the case, the case may be forwarded to the police for further investigation.

If the identity of the Whistleblower has been disclosed in connection with the report, and legal proceedings are initiated against the reported person, the Whistleblower may be summoned as a witness in the legal proceedings.

2.2 EXTERNAL REPORTING CHANNEL – DANISH NATIONAL AUTHORITY

Reporting can also be done via an external, independent whistleblowing channel established by the Danish Data Protection Authority ("*Datatilsynet*") for handling of reports concerning breaches of EU law, falling within the scope of the Whistleblower Directive and thus not reports concerning other serious legal violations or other serious matters.

It is encouraged to submit a report via the Company's internal channel where the breach can be effectively addressed internally, and the reporter assesses that there is no risk of retaliation. However, it must be emphasized that reporting under the internal or external channel is optional, provided that the report concerns the aforementioned breaches of EU law.

Link to external reporting site: https://whistleblower.dk/indberet

2.3 PUBLIC DISCLOSURE

Public disclosure is permitted only under the conditions set out in section 5(2) of the Act (e.g., prior use of internal and/or external channels without adequate response, or concrete risk of retaliation or danger to the public interest). Public disclosure outside these conditions may result in the loss of protections.

3.0 DESIGNATED PERSONS

The Company has appointed the following Designated Persons to manage the internal reporting channel, specifically trained and meeting the requirements of independence and impartiality:

- the Global Compliance Manager; and
- the Legal Manager, EMEA.

The Designated Persons act autonomously and without conflicts of interest, ensure confidentiality by default, and handle reports in accordance with applicable law and this Policy.
In case of any actual, potential, or perceived conflict of interest, the Designated Person shall abstain, and the case will be promptly reassigned to the other Designated Person (or to a duly appointed substitute) to guarantee continuity, neutrality, and timely follow-up.

4.0 PROTECTION AGAINST RETALIATION & CONFIDENTIALITY

Protection against retaliation is provided in accordance with the rules set out in the Act, specifically sections 5-8. In essence, a Whistleblower must not be subject to reprisals, including threats or attempts of reprisals, as a result of making a report or a public disclosure in accordance with the Act. Furthermore, the Whistleblower must not be prevented or attempted to be prevented from making a report.

Protection shall apply for Whistleblowers who make internal and external reportings as well as public disclosures. However, for public disclosures the protection applies in the following cases:

- When the Whistleblower making the public disclosure has first made an internal and external report, or directly an external report, without appropriate actions having been made in response to the report within the applicable deadline;

- When the Whistleblower making the public disclosure has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest;
- When the Whistleblower making the public disclosure has reasonable grounds to believe that reporting to an external Whistleblower scheme carries a risk of reprisals or, due to specific circumstances of the case, there is little prospect that the violation will be effectively addressed.

Further, protection shall apply only if the Whistleblower has reasonable grounds to believe that the reported or disclosed information was correct at the time of reporting or disclosure, ad that the information fell within the scope of the Act.

In terms of confidentiality, the Act stipulates that Designated Persons constituting the internal Whistleblower entity who manage the internal channel are bound by confidentiality regarding the information contained in the reports. This confidentiality obligation similarly applies to persons who, through disclosure become aware of such information. A confidentiality obligation also applies to unauthorized employees at authorities operating external Whistleblower schemes who inadvertently become aware of such information concerning the reports.

5.0 RETENTION OF PERSONAL DATA

Reports and related personal data concerning employees will be retained for the time strictly necessary to handle them and generally five (5) years after the employment relationship has ended, with reference to section 4(1) in the Danish limitations act, however unless specific circumstances mandate a longer retention period, for example due to ongoing legal proceedings or the prospect of such.

Reports and related personal data concerning clients or other third parties will be retained for the time strictly necessary to handle them and, generally due to documentation purposes for 3 years with reference to section 3(1) in the Danish limitations act, however unless specific circumstances mandate a longer retention period, for example due to ongoing legal proceedings or the prospect of such.

GERMANY

1.0 SUMMARY

This Policy Annex is intended to supplement the existing GPT Group Whistleblowing Policy by addressing the specific legislative changes that have been implemented in Germany pursuant to EU Directive 2019/1937 on the Protection of Persons Who Report Breaches of Union Law (Whistleblowing Directive) and local regulation. In Germany, the protection of Whistleblowers is regulated in the Law on the Protection of Whistleblowers "Gesetz zum Schutz von hinweisgebenden Personen", also called
"Hinweisgeberschutzgesetz" or in short: "HinSchG".

This Policy Annex therefore addresses the differences in application from the Global Policy which apply in GPT's entity located in Germany, namely GrainProteinTech Climate Control Air Treatment Germany GmbH (the "Company").

This Annex gives information to Whistleblowers pursuant to Article 5(e) of Legislative Decree 24/2023. Where there is any conflict between the Policy and this Annex, this Annex prevails for Italy.

2.0 SCOPE OF APPLICATION & ENTITIES COVERED

This Policy Annex applies not only to all officers, directors, employees and temporary workers (collectively, "Associates") and to all agents of the Company including but not limited to, contractors, consultants and representatives (collectively "Associated Persons") but also to:

- shareholders and holders of voting rights in the Company's general assembly;
- members of the Company's administrative, management or supervisory body;
- external and occasional staff of the Company;
- co-contractors of the Company and their subcontractors;
- those who report or publicly disclose information on breaches acquired in a work-based relationship with the Company which has since ended; and
- those whose work-based relationship with the Company is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations in Germany.

3.0 DEFINITIONS

Pursuant to the HinSchG, the definitions of Whistleblower and Reportable Conduct under this Policy are extended under German law as follows:

- Whistleblower (Protected Discloser): is defined as "a natural person who has obtained information on infringements in connection with their professional activities who discloses such information to the reporting bodies provided for under the German Whistleblower Act". Infringements are acts or omissions that are unlawful and concern the areas of law in the scope of the Whistleblowing Directive or are abusive because they run counter to the aim or purpose of the Directive.

- Reportable Conduct (Improper Conduct) includes, in addition to definitions in the global Policy, such infringements.

The disclosure of facts, information or documents from the intelligence services or that could harm national security or essential security interests and disclosures in breach of a duty of confidentiality on respect of classified information, the secrecy of judicial deliberations, the duty of confidentiality on the part of lawyers or medical professionals, is prohibited and will not fall within the scope of the Global Policy or this Policy Annex.

4.0 REPORTING CHANNELS

Whistleblowers may submit reports through:

- Internal reporting channel;
- External reporting to external authorities.

4.1 INTERNAL REPORTING CHANNEL

Whistleblowers will be able to submit internal reports via the channels indicated in the Global Policy, which is easily accessible via a link available on the Company's website: GPT Alertline Once logged into the portal, the whistleblower can use the dedicated menus to select the specific Group company country to which the report relates before submission.

The internal channel allows Whistleblowers:

- to submit reports by any means (written or oral). If a report is given orally, it can be done by telephone or where requested by the Whistleblower, can choose by a video conference or a physical meeting organized within a reasonable time frame. Any audio recording requires the Whistleblower's consent; otherwise, a written minute is prepared and signed;
- to report anonymously, if they consider it necessary.

The Whistleblower will be informed in writing of the receipt of the report within seven (7) days of its receipt. The Designated Person will maintain communications with the Whistleblower and may request further information from them.

The Designated Person provides a follow-up reply within three (3) months from the date of acknowledgement of receipt of the report or, if no acknowledgement is received, three months from the expiry of the period of seven working days following the report being made. In the follow-up the Designated Person shall inform the Whistleblower of the outcome of the report, namely: (i) closure/archiving (when the allegations are found to be inaccurate or unfounded, or when the report has become irrelevant), or (ii) confirmation that the report has been found well-founded and has been forwarded to the competent bodies/authorities.

Reports and related personal data will be retained for the time strictly necessary to handle them and, in any case, no longer than five (5) years from the communication of the outcome of the procedure.

4.2 EXTERNAL REPORTING CHANNEL - GERMAN NATIONAL AUTHORITIES

Whistleblowers may make an external report to the following authorities:

- Externe Meldestelle des Bundes beim Bundesamt für Justiz
  BfJ - Hinweisgeberstelle (bundesjustizamt.de)

- Bundeskartellamt – for breaches relating to competition law and the Digital Markets Act
  https://www.bundeskartellamt.de/DE/Aufgaben/Kartelle/HinweiseAufKartellverstoesse/hinweiseaufverstoesse_node.html

5.0 DESIGNATED PERSONS

The Company has appointed the following Designated Persons to manage the internal reporting channel, specifically trained and meeting the requirements of independence and impartiality:

- the Global Compliance Manager; and
- the Legal Manager, EMEA.

The Designated Persons act autonomously and without conflicts of interest, ensure confidentiality by default, and handle reports in accordance with applicable law and this Policy.
In case of any actual, potential, or perceived conflict of interest, the Designated Person shall abstain, and the case will be promptly reassigned to the other Designated Person (or to a duly appointed substitute) to guarantee continuity, neutrality, and timely follow-up.

6.0 PROTECTION AGAINST RETALIATION & CONFIDENTIALITY

The principle of no retaliation not only applies to Associates, Associated Persons and to the other subjects referred to in Section 2, who make a report under the Global Policy and this Policy Annex but also to facilitators, as previously defined in the Global Policy, third parties connected with the Whistleblowers such as colleagues, ex-colleagues, consultants and family members and legal entities that the Whistleblower owns, works for or is connected within a work-related context.

Retaliation may include, but is not limited to employment termination, layoff, disciplinary measures, reduction of salary, transfer of place of work, any type of discrimination, negative performance review, harassment, non-conversion of fixed-term contract into permanent contract etc.

ITALY

1.0 SUMMARY

This Policy Annex is intended to supplement the existing GPT Group Whistleblowing Policy by addressing the specific legislative changes that have been implemented in Italy pursuant to EU Directive 2019/1937 on the Protection of Persons Who Report Breaches of Union Law (Whistleblowing Directive) and local regulation (Legislative Decree no. 24 of 10 March 2023, implementing the Whistleblowing Directive in Italy and the guidance of National Anti-Corruption Authority).

This Policy Annex therefore addresses the differences in application from the Global Policy which apply in GPT's entities located in Italy, namely: Cimbria S.r.l.; GrainProteinTech Climate Control Air Treatment S.p.A.; Tecno Poultry Equipment S.r.l. (each the "Company").

This Annex gives information to Whistleblowers pursuant to Article 5(e) of Legislative Decree 24/2023. Where there is any conflict between the Policy and this Annex, this Annex prevails for Italy.

2.0 SCOPE OF APPLICATION & ENTITIES COVERED

This Policy Annex applies not only to all officers, directors, employees and temporary workers (collectively, "Associates") and to all agents of the Company including but not limited to, contractors, consultants and representatives (collectively "Associated Persons") but also to:

- shareholders and holders of voting rights in the Company's general assembly;
- members of the Company's administrative, management or supervisory body;
- external and occasional staff of the Company;
- co-contractors of the Company and their subcontractors;
- volunteers and trainees (both paid and unpaid);
- those who report or publicly disclose information on breaches acquired in a work-based relationship with the Company during the probationary period;
- those who report or publicly disclose information on breaches acquired in a work-based relationship with the Company which has since ended; and
- those whose work-based relationship with the Company is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations with the Company.

3.0 DEFINITIONS

Pursuant to Legislative Decree No. 24/2023, the definitions of Whistleblower and Reportable Conduct under this Policy are extended under Italian law as follows:

- Whistleblower (Protected Discloser): is defined as "a natural person who reports conduct, acts, omissions resulting in violations (or grounded suspicion of violations) of Italian and EU laws and regulations, as encountered by the Whistleblower within the

employment context, affecting the public interest or the integrity of the public administration or a private entity and consisting of administrative, accounting, civil or criminal offenses or significant illegal conduct".

- Reportable Conduct (Improper Conduct) includes, in addition to definitions in the global Policy:

    1. civil, criminal, administrative or accounting offences;
    2. unlawful conduct relevant under Legislative Decree 231/2001;
    3. if applicable, breaches of the Organization and Management Models adopted pursuant to Legislative Decree 231/2001 ("MOG 231");
    4. breaches of EU law in sectors such as public procurement; financial services, products and markets; prevention of money laundering and terrorist financing; product safety; transport safety; environmental protection; etc.;
    5. acts or omissions harming the EU's financial interests;
    6. acts or omissions affecting the internal market of the EU (hindering free movement of goods, services, persons or capital);
    7. breaches of the European Union restrictive measures (EU sanctions), including the violations of national implementing provisions, criminal offences or administrative breaches relating to EU sanctions regimes, where such violations are identified in a work-related context.

The disclosure of facts, information or documents relating to a personal interest of the reporting person which pertains exclusively to their individual employment, violations already compulsorily regulated by other EU or Italian regulations, breaches of national security, classified information, forensic and medical professional secrecy, judicial deliberations and the disclosure of facts, information or documents unlawfully collected is prohibited and will not fall within the scope of the Global Policy or this Policy Annex.

4.0 REPORTING CHANNELS

Whistleblowers may submit reports through:

- Internal reporting channel;
- External reporting to the Italian National Anti-Corruption Authority (ANAC) via its online platform;
- Public Disclosure (allowed only under specific conditions identified by Article 15 of the Legislative Decree 24/2023).

4.1 INTERNAL REPORTING CHANNEL

Whistleblowers will be able to submit internal reports via the channels indicated in the Global Policy, which is easily accessible via a link available on the Company's website: GPT Alertline Once logged into the portal, the Whistleblower can use the dedicated menus to select the specific Group company country to which the report relates before submission.

The internal channel allows Whistleblowers:

- to submit reports by any means (written or oral). If a report is given orally, it can be done by telephone or where requested by the Whistleblower, can choose by a video conference or a physical meeting organized within a reasonable time frame. Any audio recording requires the Whistleblower's consent; otherwise, a written minute is prepared and signed;
- to report anonymously, if they consider it necessary.

The Whistleblower will be informed in writing of the receipt of the report within seven (7) days of its receipt. The Designated Person will maintain communications with the Whistleblower and may request further information from them.
The Designated Person provides a follow-up reply within three (3) months from the date of acknowledgement of receipt of the report or, if no acknowledgement is received, three months from the expiry of the period of seven working days following the report being made. In the follow-up the Designated Person shall inform the Whistleblower of the outcome of the report, namely: (i) closure/archiving (when the allegations are found to be inaccurate or unfounded, or when the report has become irrelevant), or (ii) confirmation that the report has been found well-founded and has been forwarded to the competent bodies/authorities.

Reports and related personal data will be retained for the time strictly necessary to handle them and, in any case, no longer than five (5) years from the communication of the outcome of the procedure.

4.2 EXTERNAL REPORTING CHANNEL - ITALIAN NATIONAL ANTI-CORRUPTION AUTHORITY ("ANAC")

Whistleblowers may make an external report in the following circumstances provided by the Legislative Decree:

- an internal reporting channel has not been established or does not comply with the required standards;
- they have already made an internal report that has not been followed up or had a negative outcome;
- they have reasonable grounds to believe that an internal report would not be followed up or could lead to retaliation (e.g., conflict of interest cases in which the handler of the report coincides with the reporter, the reported person or otherwise is a person involved or affected by the report);
- they have reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public.

In Italy ANAC is an independent administrative authority with regulatory, investigation and sanctioning powers in the area of whistleblowing.

Whistleblowers may submit external reports to ANAC orally or in writing via its IT platform. If a report is given orally, it can be done by telephone or any other voice mail system or where requested by the Whistleblower, can choose by a videoconference or a physical meeting within a reasonable time frame

ANAC is required to acknowledge the report within 7 days of its receipt unless requested by the reporter not to do so or if doing so would jeopardize the confidentiality of the report. They must diligently follow up on reports, investigate as required and reply to the reporting person within three (3) months (or six (6) months if there are justified reasons for delay) from the acknowledgment, or if no acknowledgement is received, three (3) or six (6) months from the expiry of the period of seven (7) working days following the report being made. With its reply ANAC shall inform the Whistleblower on the investigation outcome, which can also consist in the closing of the report, its transmission to other competent authorities, a recommendation or imposition of administrative fines.
More information on the reporting procedure via ANAC is available via the links below:

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

4.3 PUBLIC DISCLOSURE

Public disclosure is permitted only under the conditions set out in Article 15 of the Legislative Decree (e.g., prior use of internal and/or external channels without adequate response, or concrete risk of retaliation or danger to the public interest). Public disclosure outside these conditions may result in the loss of protections.

5.0 DESIGNATED PERSONS

The Company has appointed the following Designated Persons to manage the internal reporting channel, specifically trained and meeting the requirements of independence and impartiality:

- the Global Compliance Manager; and
- the Legal Manager, EMEA.

The Designated Persons act autonomously and without conflicts of interest, ensure confidentiality by default, and handle reports in accordance with applicable law and this Policy.
In case of any actual, potential, or perceived conflict of interest, the Designated Person shall abstain, and the case will be promptly reassigned to the other Designated Person (or to a duly appointed substitute) to guarantee continuity, neutrality, and timely follow-up.

6.0 PROTECTION AGAINST RETALIATION & CONFIDENTIALITY

The principle of no retaliation not only applies to Associates, Associated Persons and to the other subjects referred to in Section 2, who make a report under the Global Policy and this Policy Annex but also to facilitators, as previously defined in the Global Policy, third parties connected with the Whistleblowers such as colleagues, ex-colleagues, consultants and family members and legal entities that the Whistleblower owns, works for or is connected within a work-related context.

Italian law sets out an extensive list of acts and omissions, even only attempted or threatened, that can be considered as retaliatory measures, which include, but are not limited to: employment termination, layoff, disciplinary measures (including financial sanctions and suspension), reduction of salary, downgrading or non-promotion, change of duties, transfer of place of work, any type of discrimination, negative merit notes, negative references, harassment, ostracism, non-conversion of fixed-term contract into permanent contract, reputational damage, cancellation of supply contracts, request for submission for psychiatric or medical test.