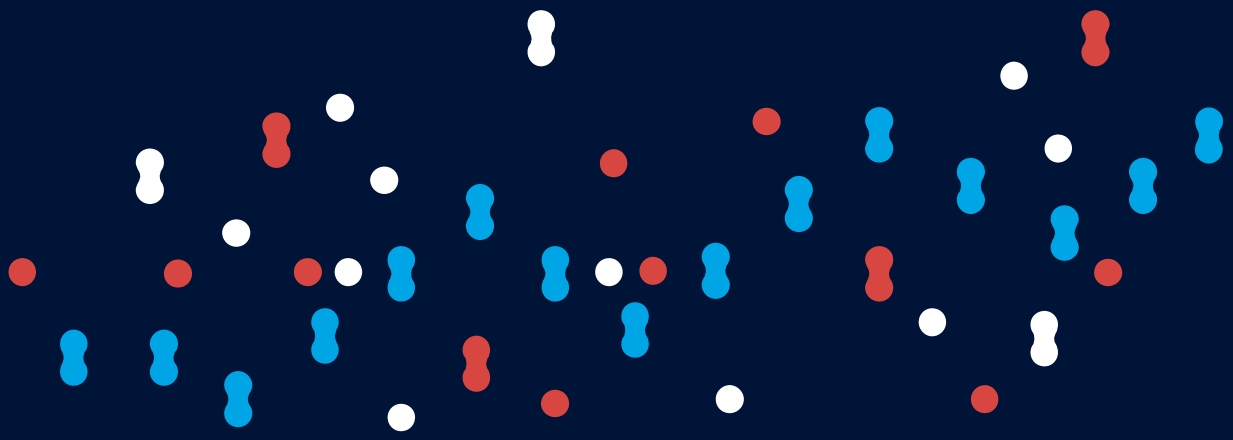

Global Whistleblowing Policy

ION Group

November 2024

Contents

Section 1: Purpose and overview

1.1 Applicability

This policy applies to all ION's businesses, divisions, and offices and to all personnel (including former and prospective personnel) of:

(i) ION ; or
(ii) suppliers / vendors with whom ION has/had a commercial relationship.

It also applies across all jurisdictions where ION operates other than those entities / jurisdictions where a local policy is in force in which case such policy will take precedence. If in any jurisdictions where ION operates, there are whistleblowing protection laws that provide a higher level of protection than what is included in this policy, the local legislation will take precedence.

1.2 Protected Disclosures

ION wants to know about any conduct which is detrimental to ION and could cause financial or non-financial loss amounts to ION including but not limited to any of the below listed:

- Anti-competitive practices;
- Breach of applicable laws;
- Breach of data privacy laws;
- Breach of internal policies;
- Bribery;
- Concealing or destroying evidence of wrongdoing;
- Conflict of interest;
- Corruption;
- Discrimination;
- Environmental and/ or social concern;
- Financing of terrorism;
- Fraud;
- Health and safety violations/ unsafe work environment;
- Human rights violations;
- Information security risk;
- Money laundering;
- Moral harassment, pressure or violence at work;
- Theft;
- Unethical practices

.

The above list is not exhaustive and is for illustrative purposes only.

The laws of a particular jurisdiction relating to whistleblowing will determine if the subject matter of a report falls within the scope of a protected disclosure in that jurisdiction and whether the whistleblower will benefit from the wider protections provided by such laws.

A whistleblower should have reasonable grounds to believe that the information reported was true at the time of reporting, even if the reported facts are found to be inaccurate during review of the report. Furthermore, a declaration of good faith is a prerequisite pursuant to some local whistleblowing laws.

False or fraudulent reports do not benefit from protected disclosure protections and may be the subject of disciplinary and / or further action including criminal and / or civil liabilities.

1.3 Exclusions

The following is non-exhaustive list of matters that will not generally fall within the scope of a protected disclosure:

- matters which fall within the scope of the applicable law of the whistleblower's jurisdiction;
- matters exclusively affecting the whistleblower;
- disputes with an employing entity about an individual's career path or employment contract;
- information that is disclosed in a legally privileged setting;
- requests for commercial information;
- complaints about day-to-day issues relating to commercial arrangements;
- complaints from customers; or
- reports related to aspects of personal life of ION personnel which are not connected to their working activities.

Section 2: Process For Making A Report

2.1 Channels

The following channels are available to make a whistleblowing report:

- Submit a report via ION's secure third-party platform, Whispli, at **https:// iongroup.whispli.com;**
- Request a meeting with a local HR Representative or a member of the whistleblowing team via email or via the Whispli platform;
- By telephone to +43 (316) 908030 520 if based in Austria or Germany; or
- To the relevant external authority established in a particular jurisdiction. The details of external bodies responsible, under the implementing legislation of the Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, concerning the protection of persons who report violations of Union law, are set out below in Appendix 2.

A full guide to using the Whispli platform can be found via the following link: **https://help.whispli.com/en/articles/informants**, including how to create a secure and confidential mailbox and a guide to a Whistleblower's journey on the platform. Whispli is certified to ISO 27001 and SOC2 security standards.

2.2 Anonymity

A whistleblower can choose to remain anonymous while making a report, interacting with case managers during an investigation of the report, as well as after a case is closed. However, certain jurisdictions do not support investigations in the absence of certain identifying information. Furthermore, there are limitations of what can be achieved if a whistleblower decides to remain anonymous.

To facilitate investigations, it is recommended that a whistleblower at a minimum identify themselves by name, bearing in mind that any identifying information they provide will be treated in strict confidence. If a whistleblower decides to disclose their identity at the outset or at a later date, ION will endeavor to protect their identity.

If a whistleblower does choose to remain anonymous, it is at ION's discretion, in accordance with applicable law, to determine whether the report is admissible and requires further investigation. Relevant considerations to the exercise of this discretion will include the seriousness of the subject matter, the level of detail included, the ability of ION to establish and verify the facts alleged and the implications and accordingly the appropriateness of commencing an investigation based on the information provided.

ION has implemented procedures to collect and process reports to maintain strict confidentiality of the identity of the informant, of the persons concerned by the report, and of the information collected by all the recipients of the report. Any information that could potentially identify an anonymous whistleblower will be held in the strictest confidence and will not be shared.

2.3 Investigative Process

The steps a case manager / member of ION's whistleblowing team will undertake once a report is received, until the case is closed, are set out below:

Receipt

1. If a whistleblowing report is received in a manner other than via the third-party Whispli platform, the individual who received the report will forward the details to the local HR representative to enter the details of the report into the Whispli platform.

Case manager designation / conflict resolution

2. Unless the whistleblower has indicated a conflict, the report will be routed in the first instance to the local HR representative for the relevant entity and / or jurisdiction.
3. If the report relates to multiple jurisdictions or multiple entities within ION or to a non-identified jurisdiction, the report will be routed internally to determine the most appropriate jurisdiction and then routed to the local HR representative for the relevant entity.
4. If a whistleblower indicated a conflict with a particular individual or team, that particular individual and / or team will, if practicable, be removed from the workflow and an alternative reviewer will be assigned.

Acknowledgment and assessment / triaging

5. The case manager assigned (based on the above criteria) will acknowledge receipt of the report within 7 days.
6. The case manager will undertake an initial assessment of the report to determine if the report is admissible or not admissible.
7. If the report is deemed inadmissible, the case manager will issue a confirmation of non-admissibility to the whistleblower.
8. If deemed admissible, the case manager will then assess the report to determine if there is sufficient information to assess the report fully and triage it appropriately.
9. The case manager may seek further information from the whistleblower, if required, to assess as to whether there is prima facie evidence that a relevant wrongdoing has occurred and to triage the report appropriately.
10. The case manager will prepare an investigation plan with a view to gathering further information via interview of relevant stakeholders, review of business reports, IT audit, surveillance or survey or other appropriate means ("Investigation").

Investigation

11. The case manager will conduct the Investigation into the alleged wrongdoing and prepare a report in accordance with the investigation report template outlined at Appendix 4.

12. Once the case manager's Investigation is concluded (inclusive of any proposed remediation actions), it will be escalated to a dedicated member of the legal team.
13. The dedicated member of the legal team may close the Investigation, determine the remedial actions to be taken (if any), route it back to the initial case manager or an alternative case manager to action or escalate to the Group General Counsel (depending on subject matter and / or criticality level).
14. ION will aim to finalize the investigation within 30 days of receipt of the report.

Feedback

15. Feedback on the outcome will be provided to the whistleblower at the conclusion of the investigation.
16. ION will endeavor to provide feedback on the investigation. However, there may be information that cannot be shared with the whistleblower for reasons of confidentiality, privacy, and/or the legal rights of all concerned. No information will be provided as part of the feedback that could prejudice the outcome of the investigation or any subsequent process, or which could undermine the fair procedures rights of any person against whom allegations have been made.
17. Actions taken in response to the report may include disciplinary action and / or civil or criminal action against the accused if the report if deemed well-founded, training, improvements to procedures, policy reform or such other action. Where applicable, Executive Management may be informed of the report and outcome (subject always to the confidentiality provisions outlined above). Executive Management will also take the final decision on the remedial and disciplinary actions proposed, if any.

2.4 Post feedback options

If, after receiving feedback, a whistleblower is not satisfied with the result, they can escalate this internally to the ION Group General Counsel via the Whispli platform or by emailing **generalcounsel@iongroup.com**. The whistleblower should provide this escalation in writing so that a formal review can take place.

While the ION Group General Counsel commits to review the request, ION is under no obligation to reopen the investigation. If the ION Group General Counsel concludes that the investigation was conducted properly and no new information exists that would change the results of the investigation, the investigation will be concluded, and the whistleblower will be informed accordingly.

The whistleblower also has the option to make a report to an external competent authority, the contact details of which are set out in Appendix 3.

Section 3: How Whistleblowers Are Protected

3.1 Anonymity after Submitting a Report

After submitting a report, the following policies around anonymity are in place to protect a whistleblower's identity.

- ION uses the Whispli platform to ensure the whistleblower's identity is not disclosed other than to specifically designated ION personnel during and after submitting a report.
- The whistleblower has the right to remain anonymous and does not need to identify themselves at any time during the investigation process. The whistleblower can refuse to answer questions they feel could identify themselves.
- If the whistleblower reveals themselves at any time, their identity will not be disclosed outside the ION personnel responsible for reviewing and investigating the report.
- Whispli as an external service provider does not generate or maintain any internal connection logs with IP addresses, so no information linking the whistleblower to ION is available. A high-grade AES256 encryption is used to protect data on the Whispli platform. IP addresses are deleted and not stored on servers or logs. A whistleblower may also wish to use a non-ION PC or other equipment to submit their report so that it does not appear on their browsing history.

3.2 Retaliation

ION does not tolerate any threats or attempts to retaliate against a whistleblower who has made a report (or against other parties that might have to bear witness or are involved in the investigation).

ION will protect such individuals from:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;

- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit; and / or
- psychiatric or medical referrals.

Any employee or associated person that is found to have taken action amounting to retaliation will face disciplinary action, including the potential to be terminated from their roles.

In cases of considered or actual perceived retaliation, the whistleblower should contact the whistleblowing team via the Whispli platform and the team will take such action as they feel is appropriate in the circumstances including but not limited to recommendations for how the situation can be resolved.

3.3 Separation Of Issues

Irrespective of a whistleblowing report, ION may still raise any performance or contract issues with the whistleblower as long as they are kept separate and not influenced at all from any reports that have been made.

3.4 Legislative/Regulation Protection & Assistance

A whistleblower may also be protected against liability in judicial proceedings provided that the whistleblower had reasonable grounds to disclose the information and the type of report is a category afforded protection under the relevant laws of the whistleblower’s jurisdiction.

Section 4: Roles & Responsibilities

4.1 ION Whistleblowing Team

The following are the responsibilities of each of the roles involved in ION's whistleblowing program.

Group General Counsel: This individual, a member of Executive Management with independent control functions, is responsible for ensuring the management of the reports and of related investigations in a professional manner in accordance with the provisions of the internal and external requirements. (S)/he owns the entire program and will be measuring its overall success. This includes knowing and understanding the program, having an overall view of the management of reports as well as being a point of escalation for any concerns or retaliation that has taken place.

Human Resources: Regional HR representatives represent the first line of receipt of reports and are responsible for the initial triage of a report. They are assigned reports and their role is to investigate or escalate these reports. This includes considering the admissibility of the report interacting and asking questions of whistleblowers, as well as using the information provided to investigate the report submitted. They may also be called upon to provide advice and guidance during any investigation. The whistleblowing program leverages their expertise and acumen to ensure ION is using HR best practices during investigations and all personnel are treated fairly.

Legal Case Managers: Legal Counsel are assigned reports and their role is to investigate reports received depending on subject matter and criticality or to review an initial case manager's actions and provide legal input and advice. This may include interacting and asking questions of whistleblowers, as well as using the information provided to investigate the report submitted. Their investigation can be internal or external to the organization depending on what was documented in the report. Their goal is to gather the facts and put forth a final report to the Group General Counsel and Executive Management on what happened and what action (if any) they feel needs to take place.

Legal & Commercial Operations Team: This team provides support to the Group General Counsel on the implementation, functioning and improvement of the whistleblowing program in line with legal requirements and best practice.

4.2 Investigations

The following all play a role in HR investigations:

- HR local representative;
- A member(s) of the legal team;
- Group General Counsel;
- Head of HR;
- Individuals proximate to the subject matter of the report (e.g the accused individual(s)); and /or
- Executive Management as deemed appropriate.

The procedures implemented to collect and process whistleblowing reports guarantee strict confidentiality of the identity of the whistleblower, of the persons concerned by the report, and of the information collected by all the recipients of the report.

Any information that could potentially identify an anonymous whistleblower will be held in the strictest confidence and will not be shared, unless ION is compelled by law or a whistleblower subsequently consents to its disclosure.

The identity of any accused individual(s) by a report is treated as strictly confidential and can be disclosed only to a relevant legal Authority or only when the report is well founded. Further, it will only be disclosed internally, following Investigation and due process to the accused, if the allegations appear to be well founded in accordance with applicable law and policies.

4.3 Third Parties

At ION, third parties are utilized in our whistleblowing program and strategy as follows.

Whistleblowing Platform: ION uses a third- party whistleblowing platform, Whispli, to ensure it can protect whistleblower's identities and leverage technologies to ensure no one organization can identify them (unless the Whistleblower chooses to do so). This platform also allows for two-way, anonymous communication as well as case management and data protection features. It sits externally to ION servers and the information contained in the system is strictly confidential and accessible by a select number of trained individuals on the whistleblowing team.

Legal Firms: ION uses specialist legal firms to investigate specific cases and / or where required jurisdiction specific legal advice. They are also used for investigations that we would prefer a third party execute on, due to the nature of the report.

4.4 Protection of Personal Data

ION is committed to protecting the privacy of all users of its whistleblowing solution.

ION collects and processes personal information provided in connection with the whistleblowing program in accordance with applicable laws and regulations that relate to data protection and privacy, including the EU General Data Protection Regulation (GDPR), as applicable. Personal data will only be retained for as long as there is a need for it, and when there is no longer a need for retaining the registered information, it will be anonymized or deleted as required.

Whistleblowers should only submit information that is necessary to undertake an investigation of the concerns raised. Information about an individual's private life or sensitive data (including details of their health or sex life) should not be submitted unless it is strictly required and directly

relates to the concern. Further, personal information about individuals that are not connected to the concern raised should not be submitted.

It may be necessary to share the details of the report within ION and/or its professional advisers located abroad. Where this occurs, it will be provided in compliance with the relevant data protection legislation and ION will take appropriate steps to ensure the confidentiality of the data.

4.5 Communication and Training

ION will ensure that employees receive training as appropriate on this policy and the facility to report any concerns they may have.

Section 5: Governance

5.1 Changes to ION's Whistleblowing Policy

From time to time, ION's whistleblowing policy will need to change to reflect changes in ION's values, best practices, improvements, as well as updates to legislation and regulations.

Any changes to ION's whistleblowing policy must be approved by the ION Group General Counsel following, where appropriate, comments and feedback from Executive Management. All changes will also be documented in ION's whistleblowing policy and will be made available to all employees.

This policy and any changes made do form part of any contract of employment.

Appendix 1: Change Log

Version	Date	Amendments
Version 1	01/01/2024	N/A
Version 2	15/05/2024	Updated to align with improvements in workflows and to capture nuanced local jurisdictional requirements.
Version 3	11/11/2024	Minor updates for conciseness

Appendix 2: Relevant Legislation

Jurisdiction	Legislation
EU	Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, concerning the protection of persons who report violations of Union law
Austria	Whistleblower Protection Act (WPA) HinweisgeberInnenschutzgesetz
Bulgaria	Protection of Persons Reporting or Publicly Disclosing Information on Breaches Act
France	LOI n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte
Germany	Whistleblower Protection Act (Hinweisgeberschutzgesetz, HinSchG)
Hungary	Act XXV of 2023 on complaints, whistleblowing and rules related to whistleblowing
Ireland	Protection Disclosures Act 2014 (as amended)
Italy	Legislative Decree No 24/2023

Appendix 3: External Reporting Contacts

Jurisdiction	Competent external authority	Contact details
Austria	The Federal Bureau of Anti-Corruption* *The Money Laundering Reporting Office and the Federal Competition Authority operate external reporting channels for their respective areas.	• Website: http://www.bak.gv.at/ • Email: BMI-III-BAK-SPOC@bak.gv.at • Post: Federal Bureau of Anti-Corruption (BAK), Herrengasse 7, 1010 Vienna, Austria • Phone: +43 1 53 126-906800
Bulgaria	Commission for Personal Data Protection	• Website: www.cpdp.bg • Email: sofia2018@cpdp.bg • Post: Address: 2 Prof. Tsvetan Lazarov Blvd., Sofia 1592, Bulgaria
France	L'Agence française anticorruption	• Website: https://www.agence-francaise-anticorruption.gouv.fr • Email: afa@afa.gouv.fr • Post: AFA, 23 avenue d'Italie, 75013 Paris
Germany	Federal Office of Justice	• Website: https://www.bundesregierung.de
Hungary	The Office of the Commissioner for Fundamental Rights	• Website: https://www.ajbh.hu • Email: panasz@ajbh.hu; hungarian.ombudsman@ajbh.hu • Post: The Office of the Commissioner for Fundamental Rights 1055 Budapest, Falk Miksa utca 9-11. • Phone: (+36) (1) 475-7129; (+36) (1) 475-7100
Italy	National Anti-Corruption Authority	• Website: www.anticorruzione.it • Email: protocollo@pec.anticorruzione.it • Post: National Anti-Corruption Authority, c/o Palazzo Sciarra, Via Minghetti, 10, 00187 Rome • Phone: +39 06 62289571
Ireland	Office of the Protected Disclosures Commissioner	• Email: info@opdc.ie • Post: Office of the Protected Disclosures Commissioner 6 Earlsfort Terrace, Dublin 2, D02 W773 • Phone: 01 639 5650

Appendix 4: Investigation report

If this template is saved on a network other than within the Whispli platform no identifying details relating to the whistleblower should be included (other than the unique Whispli code assigned to the report) and the document should be password protected.

Whispli report ID	
Criticality level assigned	

Investigation Methodology

Phase 1: Investigation plan
Identify relevant information, documents and other material required to be examined as part of the investigation plan. • Prepare background summary. • Identify any risks to investigation and / or stakeholders and immediate actions required. • List distinct allegations made. • Complete key stakeholders list. • Identify any potential evidence sources. • Identify any further information required from the whistleblower. • Prepare investigation plan including questions to be addressed.
Phase 2: Inquiries
Review relevant documents and conduct interview(s) • Email and forensic review. • 'Open-source' (i.e. publicly available) review. • Business records review. • IT audit. • Background checks. • Schedule interviews with complainants, witnesses and respondents. • Conduct interviews and record findings. • Maintain communication record.

Phase 3: Evidence review

Cross check / collaboration of evidence phase

- Identify evidence that is relevant, credible and probative in relation to each allegation.
- Cross check / collaborate that evidence if possible.
- If there is contradictory evidence, consider whether further exploration is necessary.
- Ensure that appropriate witnesses have been questioned and any conflicting witness statements or conflicting evidence verified or otherwise checked.

Phase 4: Reporting

- Drafting of initial findings.
- Allowing the accused to provide a response to the findings and comment on any contradictory evidence obtained in the investigation.
- Briefing with decision maker/s and other stakeholders.
- Drafting action timeline.
- Issuing the investigation summary of findings to Whistleblower.

Phase 1: Investigation plan

Background summary

Example: set out a summary of the whistleblowing report and any relevant background facts (omitting any identifying information relating to the whistleblower).

Urgency / risk identification

List any potential risks that and your proposal for managing these risks as part of the investigation.

Nature of Risk	**Proposal for resolution**
Examples: • Health / safety • Relationships to named parties (potential or actual conflicts of interests) • Personal data impact assessment • Resignation of stakeholders • Financial risks / impact • Media and / or reputational risks • Litigation risks – e.g. involves a customer or supplier • Regulator interest / potential interest • External agency notification required	• Click or tap here to enter text.

Objectives of investigation

Example: set out the objectives of the investigation to examine the complaint or allegations and specifically list the questions or issues that need to be examined or answered.

Allegations

List the allegations to be investigation, as reported by the informant.

Allegation 1	Click or tap here to enter text.
Allegation 2	Click or tap here to enter text.

Stakeholder details (not including whistleblower)

Set out the key stakeholder name and contact details – accused, witnesses, management (line and executive), other persons of interest.

Details	Name	Accused or proxy to the incident	Role (executive or non-executive)	Role is internal or external to ION	Contact details (phone, email, Linkedin profile, etc.)
Stakeholder 1					
Stakeholder 2					
Stakeholder 3					

Possible sources of evidence

Example: identify relevant evidence/documentation provided by whistleblower that should be sought from organization/whistleblower/witnesses/third parties etc.

Investigation plan

Please select which investigation plan you are proposing: **Choose an item.**

Note, "external agency" is referring to external bodies such Data Protection Authority, local/national law enforcement agency, competition authorities, etc.

Set out the proposed steps to be undertaken in line with the proposed investigation plan selected above. If “Record but no further investigation required” is selected, please state the reasons for this selection.

Phase 2 & 3: Inquiries & Evidence review

For each allegation listed in the Investigation plan, the following should be documented as evidence of conducting the Investigation, as well as the outcome. If any action was not taken, include reason for not including as part of the Investigation.

[Copy and paste the below table for each Allegation reviewed as part of the Investigation]

Allegation [#]	
Action taken	**Details of action taken and key findings**
Documents reviewed	Click or tap here to enter text.
Stakeholder interviews conducted	Click or tap here to enter text.
Review of publicly available information	Click or tap here to enter text.
Background checks completed	Click or tap here to enter text.
Internal IT audit completed	
Allegation review outcome	Choose an item.

Phase 4: Conclusion

Investigation report – Key findings and conclusion

Example: Present the factual findings of the investigation. Be objective and avoid speculation. Use clear language to describe what was discovered.

Provide a summary of the evidence you took into account in making your decision and any evidence or established facts that were not taken into account and reasons why you did not consider that evidence relevant.

Set out your findings of fact on the balance of probabilities about what happened, that is the act or acts suspected of being misconduct.

Set out your decision as to whether those acts amount to misconduct, and, if so, which elements of policy, regulation or legislation have been breached and why.

Include reference to the relevant evidence and links to access it which you seek to rely upon and any contradictory / conflicting evidence.

Identify if there any mitigating or extenuating factors.

Investigation report – Course of action

Example: Based on the investigation findings, please provide specific details of the recommended course of action and why.

These may include:

- Disciplinary measures
- Training
- No action
- Other

Investigation report – Response to informant

Please draft the proposed response to the informant here. Note all communication with the informant should be completed within the Whispli platform.