OPERATING PROCEDURE AND POLICY FOR NORDIC TRANSPORT GROUP'S WHISTLEBLOWER SYSTEM AND INTERNAL INVESTIGATIONS

NTG NORDIC TRANSPORT GROUP A/S

STANDARD OPERATING PROCEDURE AND WHISTLEBLOWER POLICY

REGARDING INTERNAL INVESTIGATIONS

1 Introduction and purpose

1.1 This standard operating procedure and whistleblower policy (WB Policy) for NTG Nordic Transport Group A/S and all its subsidiaries ("**NTG**") describes e.g., the procedures for i) reporting to NTG's *Speak Up* whistleblower system (WB system), ii) investigating reports received in the WB system, and iii) follow up on reports.

1.2 Key aims of NTG's whistleblower system and WB Policy include a) explaining reporting procedures to NTG employees and stakeholders and b) meeting NTG's obligations under i) European Union (EU) Directive 2019/1937 of 23 October 2019 on the protection of persons who report violations of Union law (the "**Whistleblower Directive**"), the Danish Whistleblower Act and other EU national legislation implementing the Whistleblower Directive requiring employers to establish a whistleblower scheme, and ii) other applicable laws promoting corporate whistleblower systems. Additional aims include:

- Encouraging NTG colleagues to report suspected serious wrongdoing as soon as possible in the knowledge that their concerns will be taken seriously and investigated appropriately, and their confidentiality will be respected.
- Providing colleagues with guidance as to how to report those concerns.
- Reassuring colleagues that they can raise genuine concerns without fear of retaliation, even if they turn out to be mistaken.
- Establishing the procedures for NTG's handling of whistleblowers' reports through both the WB system and other ordinary channels of communication, and through external official channels.

2 The whistleblower system

2.1 The WB system may be used by employees, managers and members of the board of directors of NTG to report a) matters covered by the scope of the Whistleblower Directive, b) other actual or suspected violations of applicable laws or NTG's **Employee Code of Conduct**, and c) of actual or suspected violations by Suppliers of NTG's **Supplier Code of Conduct** and other serious matters. NTG's WB system is also accessible for NTG's external stakeholders, e.g., auditors, lawyers, suppliers, consultants, customers and other business partners.

2.2 The WB system may only be used to report suspected serious concerns about persons or incidents a) related to NTG e.g., NTG employees, managers and directors, and third-party stakeholders, and b) related to Suppliers' business dealings with NTG under NTG's **Supplier Code of Conduct**. NTG investigates reports made internally (reported within NTG or reported directly to someone at NTG by external stakeholders) and through the WB system in the same way, as described below.

3 The scope

3.1 The following concerns can be reported internally or through the WB system: (i) violations of EU law that fall within the scope of the Whistleblower Directive and (ii) other serious violations of Danish, EU and other applicable laws, and iii) other serious concerns, e.g., violations of NTG's **Employee Code of Conduct** or **Supplier Code of Conduct**.

3.2 Suspected violations of the specific EU legal acts within the scope of the Whistleblower Directive are listed exhaustively in Part I in the annex to the Whistleblower Directive, including:

- public procurement,
- transport safety,
- protection of the environment,
- protection of privacy and personal data,
- financial services, products and markets, prevention of money laundering and terrorist financing,
- security of network and information systems,
- product safety and compliance,
- food and feed safety, and animal health and welfare,
- public health,
- consumer protection.

Violations affecting the financial interests of the EU or relating to the internal EU market, including violations of EU competition and state aid rules, are also included in the scope. The Whistleblower Directive is available in all EU country languages here.

3.3

Serious violations of applicable laws and other serious offences include, e.g.,

- criminal acts such as violations of non-disclosure obligations, embezzlement, corruption, fraud, and bribery,
- serious or repeated infringements of the law, including legislation on the use of force, the Danish Public Administration Act, the Danish Act on Access to Public Records and legislation intended to protect public health, provide transport sector safety, or protect nature and the environment, etc.,
- sexual harassment in the workplace,
- serious person-related conflicts in the workplace, such as harassment on grounds of race, political affiliation, religious belief, etc.,
- violations of occupational safety rules, and
- violations of data protection and trade secrets laws.
- Violation of NTG internal rules provided that the violation may lead to:
    - serious, recurring security risks
    - serious financial risks
    - regulatory penalties or other official measures
    - a serious qualification from an auditor, or
    - serious damage to NTG's relations with employees or external parties.
- Other serious violations of NTG’s employee and supplier codes of conduct

- Matters not listed above that you suspect may involve a serious violation or breach.

3.4 The most effective way to report a concern is to directly contact the Whistleblower Unit described in 4.3, below, or to your immediate manager(s), who must escalate that report to Group Legal. The WB system is an alternative to internal communication channels and should be used, if for any reason, you are uncomfortable or uncertain about reporting internally. External stakeholders can contact the Whistleblower Unit or their usual NTG contact persons.

3.5 Reports made via the WB system are received by the global auditing firm Deloitte ("**Deloitte**") as an external and independent third-party operating and hosting the system. After screening the report and deciding who at NTG should receive the report for further processing, Deloitte forwards the report in accordance with section 4.

3.6 Subject to the conditions in section 4, reports are handled by NTG's Group General Counsel (Head of Group Legal) and the Head of Legal Compliance, in collaboration with the Audit Committee of the Board of Directors.

3.7 **NTG encourages colleagues to report serious concerns and to protect all whistleblowers who make a report in a good faith. Whistleblowers making good faith reports will not be subjected to adverse treatment or consequences (retaliation), as detailed below**.

3.8 The whistleblower system is not an emergency hotline. Issues involving immediate threats i.e. where there is a threat to health, life etc. should be reported through ordinary emergency channels. Likewise, reports that do not fall into the categories described above will be forwarded, if possible, to the appropriate persons in NTG, with the reporter's consent, e.g., ordinary employment matters, complaints about parking, etc.

4 The reporting procedure

4.1 *Reporting Channel for whistleblower system*

Reports are filed via "Deloitte Halo Whistleblower System" found on NTG's intranet *NTG Connect* and internet. The whistleblower system does not allow oral reports.

4.2 *Anonymous reporting – whistleblower system*

NTG encourages that you submit WB reports with your name and contact details, which helps the persons investigating the report ask questions and inform you about how the investigations will proceed. You can submit reports anonymously, however, if you are in any way uncomfortable or uncertain about disclosing your name.

If you select *Completely Anonymous*, no one at Deloitte or NTG will know your name; if you select *Confidential (Restricted)*, NTG will not know your name, but it will be available to Deloitte, which *may not* share it with NTG. If you select *Confidential*, your name will be available to Deloitte and NTG.

4.3 *The Whistleblower Unit*

The Whistleblower Unit comprises NTG's Group General Counsel, and the Head of Legal Compliance, who review reports with the Board of Directors' Audit Committee. When the report is filed, Deloitte forwards it to the Whistleblower Unit. If a report concerns Group Legal or a person within Group Legal, Deloitte will instead forward the report to NTG's Chief Financial Officer (CFO) or Chief Information Officer (CIO).

Reports concerning board members, the chairman of the board or the CEO, are forwarded to NTG's external auditor.

Reports received internally through ordinary channels of communication are handled by the Whistleblower Unit, but with the same exceptions as above for reports about Group Legal, the CEO, the board and Chairman.

4.4 *Self-obligation to ensure impartiality*

The Whistleblower Unit must ensure that a report does not concern them and that the reported content generally can be processed within the scope of the whistleblowing system, described in sec. 3, above.

4.5 *Obligation to investigate*

All reports must be investigated fairly, confidentially and thoroughly according to the complexity and severity of the report. If a reported concern is assessed to be manifestly unfounded, or outside the scope of whistleblower reporting, no further review or investigations will occur.

During the investigation, the Whistleblower Unit interviews i) the person(s) who submitted the report, if they wish to be interviewed, ii) persons the whistleblower recommends be interviewed because they witnessed or were aware of the incident reported, iii) other persons the Whistleblower Unit deems relevant and necessary to the investigation, and iv) the subject(s) of the investigation (reported person(s)). The investigators will give persons they have interviewed a written transcript of the interview for review and possible correction.

4.6 *Investigation conclusion*

Any investigation must be finalized by a written report containing a conclusion and/or recommendation for further action based on the findings of the report. The investigation report is passed to NTG's audit committee. The conclusion/recommendation can be:

- The investigation has been closed as manifestly unfounded
- The case ends with changes to internal procedures and possible remedial actions
- The case ends with a warning or termination of employment or business relationship
- The case ends with other disciplinary actions (expulsion/dismissal)
- The case will be submitted to the police for investigation
- The case will be submitted to other regulatory or investigative agencies, e.g. the Danish FSA, national agencies enforcing sanctions or anti-bribery laws

4.7 *Use of internal and external services*

The Whistleblower Unit will, as needed, engage internal and external assistance for the investigation of a report, including Group Finance performing a forensic accounting investigation, IT technical assistance, investigative and forensic assistance, and auditing and legal assistance.

4.8 *Confidentiality*

The Whistleblower Unit and individuals engaged under section 4.7, must keep confidential all information received in a report and collected during an investigation. Until the time the written report is delivered to the audit committee, only the Whistleblower Unit may authorize disclosure of information to third-parties, subject to applicable laws. The duty of confidentiality also applies to other persons who are authorised to receive or follow-up on reports and, in doing

so, receive information about the identity of the whistleblower and other confidential report-related information. Persons interviewed during the investigation must maintain the confidentiality of their interview and its content, and the investigation process, including all names.

NTG will disclose Information on the identity of the whistleblower, the reported person or any other third-party mentioned in the report, to external parties, e.g., government agencies, when a) NTG deems the reported matter to be a potential serious violation of a law, and/or doing so is in NTG's significant legal or financial interests, subject to applicable laws, or b) if NTG is otherwise subject to a legal obligation to do so, e.g. pursuant to anti money-laundering (AML) legislation. An investigation by a public authority may require that the names of the whistleblower, witnesses and/or reported person be disclosed.

4.9 *The reported person*

The reported person will, generally, not be notified of the name of the person submitting a report or the witnesses contacted during the investigation. It is possible that the reported person will be able to identify the whistleblower or witnesses based on the information they provide, e.g., the whistleblower has submitted a report about harassment by the reported person at a specific place and time. The reported person must maintain the confidentiality of their interview and investigation, as described in section 4.8, above.

4.10 *Information to the board of directors and/or executive management*

The board of directors and/or the executive management will be informed about individual reports and investigations in accordance with the relevant procedures herein. Names will be disclosed to the extent the Whistleblower Unit deems appropriate based on NTG's significant legal and financial interests. The same confidentiality obligations described in sec. 4.8 will apply.

4.11 *Feedback to the whistleblower*

The Whistleblower Unit confirms receipt of a report within seven business days through the system and/or emails, and the whistleblower will receive feedback within three months from the confirmed receipt of the report, or within six months if special circumstances warrant it. If you report anonymously, the Whistleblower system has a chat function enabling anonymous communication with the Head of Global Compliance.

Subject to compliance with applicable laws, including rules on non-disclosure, NTG will inform the whistleblower, to the extent the Whistleblower Unit deems appropriate, of the action planned or taken as follow-up to the report, and the grounds for the decisions made. Follow-up may include, for example, filing of a police report, launch of an internal enquiry, or referral to a supervisory authority.

4.12 *Annual report to the board of directors*

The Whistleblower Unit provides an annual report to the board of directors based on the reports received in a calendar year. The annual report summarizes the extent and types of reports, and information investigations and their conclusions, including names only when the Whistleblower Unit deems it necessary for accurate reporting.

5 Protection of whistleblowers

5.1 *Protection criteria under specific laws*

The whistleblower has protection under the Whistleblower Directive and the Danish Whistleblower Act only if they had reasonable grounds to believe, based on the information available to them at the time of reporting, that the matters reported were true, and that the matters were covered by the Whistleblower Directive as described in sec. 3.2, above. If the whistleblower reports inaccurate information on violations by honest mistake, however, they will still be entitled to protection. Whistleblowers reporting under other applicable laws will have the protection of those laws.

The whistleblower will not be protected under the Whistleblower Directive or the Danish Whistleblower Act if they deliberately report inaccurate information or information about violations that are manifestly unfounded, including unsubstantiated rumours and hearsay. Whistleblowers reporting under other applicable laws will lose the protection of those laws based on the specific provisions of those laws.

Auditors and lawyers are not listed as whistleblowers under the Whistleblower Directive and the Danish Whistleblower Act and thereby are not protected by the Whistleblower Directive and the Danish Whistleblower Act if they report to NTG directly or through the WB system.

If you report concerns in the whistleblower system that are not covered by the scope of the Whistleblower Directive or the Danish Whistleblower Act, you will not qualify for legal protection under the Whistleblower Directive or the Danish Whistleblower Act, as described in this WB Policy, but NTG protects whistleblowers and persons supporting investigations.

5.2 *Protection granted*

Exemption from liability for breach of confidentiality and acquisition of information

If the whistleblower meets the criteria for protection under applicable laws, they will not be deemed to have breached any statutory non-disclosure obligation and will not incur liability, if they had reasonable ground to believe that the report was necessary to disclose a breach within the scope of the Whistleblower Directive and/or the Danish Whistleblower Act. Nor will the whistleblower incur liability for getting access to the reported disclosures, provided that such access did not constitute a criminal offence.

Protection against retaliation

Whistleblowers meeting the criteria for protection under applicable laws will also enjoy statutory protection against retaliation, including threats of retaliation and attempts of retaliation as a result of the reporting, and no one can hinder or attempt to hinder the whistleblower from reporting their concerns.

Retaliation means any direct or indirect act or omission which occurs in a work-related context, which is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.

Likewise, NTG prohibits retaliation against persons who in good faith report concerns internally or through the WB system, and who support investigations with information and actions, and will protect such employees from retaliation. Retaliating against such an employee is itself a violation of our **Employee Code of Conduct** and can lead to serious employment consequences.

NTG will also provide reasonable and appropriate support to employees who submit good faith reports and/or support investigations, and will provide appropriate remedial actions to persons who have been harmed by violations of laws or NTG's codes of conduct. Good faith simply means that someone genuinely believes that a violation may have occurred – someone can act in good faith even if the subsequent investigation does prove that a violation actually occurred.

Request for dismissal of a case under applicable laws

The whistleblower may rely on a report to seek dismissal of a case, provided that they had reasonable grounds to believe that the reporting was necessary for revealing a breach that falls within the scope of the Whistleblower Directive and/or the Danish Whistleblower Act, and/or other applicable laws.

6 External whistleblowing

6.1 *Scope*

Persons within the EU can report concerns to national government agencies after having reported to a company, or if they do not wish to report concerns to a company. Pursuant to the Danish Whistleblower Act, the Danish Data Protection Agency (Datatilsynet) has established an external whistleblower scheme, allowing all persons defined as a whistleblower under the Danish Whistleblower Act to report the same matters as covered in section 3.2, above: Welcome to the National Whistleblower Scheme.

In addition, Danish public authorities have established external whistleblower schemes for reporting violations of special legislation, including the Danish Financial Supervisory Authority, the Danish Working Environment Authority, the Danish Environmental Protection Agency, and the Danish Business Authority.

Likewise, EU member states have also established national agencies to receive whistleblower reports. Persons outside Denmark should find the agency for their country of residence. Reporting criteria may vary from country to country.

6.2 *Procedure for external whistleblowing*

In Denmark, external whistleblower schemes allow for both written and oral reporting, and a report can also, upon request, be submitted at a physical meeting within reasonable time.

The public authority provides acknowledgement of receipt within seven days, and feedback as soon as possible and no later than three months or within six months in duly justified cases.

The whistleblower will receive the outcome of the investigation, if this information is not already received in connection with the feedback.

The Danish authority operating the external whistleblower scheme may refuse to accept a report if it does not fall within the scope of the Danish Whistleblower Act and will not be required to forward the report to another authority. If the number of reports received under an external whistleblower scheme is excessive, the authority may give priority to the reports with the most serious allegations.

6.3 *Choice of reporting channel*

Whistleblowers may report their concerns to NTG or to any relevant external whistleblower scheme or to both. However, NTG encourages people to use its internal and WB system reporting if the matter can be effectively addressed internally and if there is no apparent risk of retaliation.

7 Data security and data retention

7.1 *Data security*

Personal data that is processed within the whistleblower system, including investigative reports, are processed securely, and only authorised personnel may access the information.

7.2 *Whistleblower System*

Deloitte acts as a data processor on behalf of NTG in relation to the whistleblowing system, where employees may file reports. Deloitte has implemented necessary technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in applicable data protection legislation including the Danish Data Protection Act and the EU General Data Protection Regulation 2016/679 (GDPR). NTG has executed a data processor agreement with Deloitte.

7.3 *Data retention*

If a report turns out to be unfounded, the information will be deleted within **six** months after conclusion. Reports of matters that are not relevant for NTG's internal and WB reporting systems described above will be deleted within three months of receipt.

Substantiated reports are generally deleted within **12 months** of the conclusion of an investigation, unless continued storage may be justified where a) there are grounds to believe that the report will be confirmed by subsequent reports on the same matter and b) the reports combined will constitute a serious matter covered by the scope of the whistleblower scheme.

Where a disciplinary case or sanction is carried out on the employee or there are other grounds in which a continued storing of information about the employee is legitimate and necessary, information will be stored in the employee's personnel file. Information about the employee is stored up to **five years** after termination of the employment.

In general, information is deleted after the closing of the matter with the authorities where a report has been filed with the police or other relevant authorities, and they have determined no wrongdoing occurred, unless it is deemed necessary for NTG to store the information for a longer period due to documentation requirements. In cases where authorities determine wrongdoing occurred, NTG closes the case within **five years** of the termination of employment.

NTG notifies Deloitte when a case has been closed.

See also NTG's **Data Privacy Policy**.

---o0o---

NTG Group Legal, August 2026