Whistleblowing policy and procedure

CLdN

Summary

PURPOSE

- This Whistleblowing Policy is a result of recent developments at the European level, which require the CLdN Group to establish channels for whistleblowing. Whistleblowing is when an individual brings information about a wrongdoing to the attention of their employer or another relevant organisation.
- Our Whistleblowing Policy explains how concerns can be raised and is aimed at encouraging individuals to promptly report suspected breaches that may affect the CLdN Group.
- It provides safe channels to report such breaches without fear of retaliation in order to strengthen the compliance and information culture within the CLdN Group. We guarantee that anyone who discloses perceived breaches will be provided with the full protection of the law.

SAFE CHANNELS

- A central reporting channel has been established where concerns can be sent to central management. Please click here to access this central reporting channel: https://whistleblowersoftware.com/
- In addition, several local reporting channels have been established per country where concerns can be sent to local management. Please click here to access these local reporting channels: https://whistleblowersoftware.com/
- The scope of the reporting channels is limited (please see the policy for more information). If the concern you wish to raise does not fall under the scope of this policy, please contact Whistleblower@cldn.com to address your concern.
- Rest assured that any report made will be treated confidentially and may even be made on an anonymous basis. The reports will furthermore be treated in accordance with the applicable privacy and data protection legislation.
- If you make a report, you will receive an acknowledgement of receipt within seven (7) days. No later than three (3) months after this acknowledgment, you will also receive feedback on the measures contemplated or taken to address your report.
- If you have any questions about the internal reporting channels or if you need assistance, please contact Whistleblower@cldn.com

1. Purpose

The CLdN group of companies (the “Group”) is committed to conducting business operations in accordance with the highest standards of ethical and legal business conduct. For this reason, any violation of this Group Whistleblower Policy (the “Policy”) will be treated with the utmost seriousness.

The purpose of this Policy is to encourage Employees and Third Parties to promptly report suspected Breaches (as all these terms are defined below) which may affect the subsidiaries of CLdN in Europe, the UK and Guernsey (the “Subsidiary”, all of them, “the Group”, and each of the European countries in which each Subsidiary is located, the “Relevant Country”), providing safe channels to report them without fear of retaliation with the aim of strengthening the compliance and information culture within the Group.

2. Structure of this policy

The main body of this Policy sets out general information in connection with the reporting channels in place within the Group. In order to comply with specific local law requirements applicable in the Relevant Country, a country-specific addendum (“the Country-specific Addendum”) sets out specific information which applies to any Subsidiary in addition to or in deviation from the general information for the Relevant Country. In the event of a discrepancy, the Country-specific Addendum prevails over the main body of this Policy.

3. Scope

A. PERSONAL SCOPE

The reporting channels described in this Policy, and the corresponding safeguards, apply to Employees and Third Parties of any Subsidiary of the Group who acquired information on breaches (in the sense of acts or omissions that are unlawful or defeat the object or purpose of the applicable rules, "Breaches") in the areas identified under section 3.B. below in a work-related context (the "Reporting Person"), including:

- Employees, namely all employees, officers, directors, managers, shareholders, non-executive members, temporary staff, volunteers, paid or unpaid trainees;
- Third Parties, namely freelance workers and any person working under the supervision and direction of contractors, subcontractors and suppliers.

This Policy also applies to those persons reporting or publicly disclosing information on Breaches acquired in a work-based relationship which has since ended, or which is yet to begin in cases where information on Breaches was acquired during the recruitment process or other pre-contractual negotiations.

B. MATERIAL SCOPE

Employees and Third Parties are invited to report any Breaches falling within the scope of the following areas ("In-scope areas"), which are:

- Breach of European Union law falling within the scope of the Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of the Union law and implementing national laws in EU Member States (the "EU Whistleblower Directive"), including:
- Breaches falling within the scope of the Union acts set out in the Annex to the EU Whistleblower Directive that concern the following areas:
  - (I) Public procurement;
  - (II) Financial services, products and markets, and prevention of money laundering and terrorist financing;
  - (III) Product safety and compliance;
  - (IV) Transport safety;
  - (V) Protection of the environment;
  - (VI) Radiation protection and nuclear safety;
  - (VII) Food and feed safety, animal health and welfare;
  - (VIII) Public health;
  - (IX) Consumer protection;
  - (X) Protection of privacy and personal data, and security of network and information systems.
- Breaches affecting the financial interests of the European Union as referred to in Article 325 TFEU and as further specified in relevant Union measures; and
- Breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.
- Any other Breach in the areas prescribed by national laws as further listed in the relevant Country-specific Addendum below.

Facts / information / documents, regardless of their form or medium, the disclosure of which is prohibited because they are covered by national security, the protection of classified information, the protection of legal and medical professional privilege, the secrecy of judicial deliberations and rules on criminal procedure are excluded from the scope of this Policy.

4. Safeguards

A. NON-RETALIATION

A Reporting Person who had reasonable grounds to believe that the information on Breaches reported was true at the time of reporting and fell within the scope of this Policy will be protected from any form of retaliation, including threats of retaliation and attempted retaliation as detailed below and in the Group's Code of Conduct, as applicable, in accordance with applicable law.

Retaliation will also not be tolerated against:

- facilitators (i.e. a natural person who assists a Reporting Person in the reporting process in a work-related context, and whose assistance should be confidential);
- third parties (such as colleagues or relatives) who are connected with the Reporting Person and who could suffer retaliation in a work-related context; and
- legal entities that the Reporting Person owns, works for or is otherwise connected with in a work-related context.

In this Policy, "retaliation" means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external report or by public disclosure, and which causes or may cause unjustified detriment to the Reporting Person. Examples of impermissible retaliation may include one or more of the following acts, attempts or threats against the Reporting Person in response to a Report: 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 or salary, or changes in working hours or conditions; withholding of training; negative performance assessment or employment references; imposition or administering of any disciplinary measure, reprimand or penalty (including any financial penalty); coercion, intimidation, harassment or ostracism; discrimination, disadvantageous or unfair treatment; etc.

The relevant Group Subsidiary will take disciplinary action up to and including dismissal (in accordance with local labour laws in each Relevant Country) against anyone who threatens or engages in retaliation or harassment of any Reporting Person or person who is considering reporting a Breach in accordance with this Policy.

Malicious or dishonest Reports by a Reporting Person may be subject to disciplinary action under the Group's policies or applicable regulation in the Relevant Country.

B. CONFIDENTIALITY AND PRIVACY/DATA PROTECTION

Any Report received will be treated with appropriate confidentiality and comply with current privacy and data protection legislation in force in each Relevant Country from time to time, in particular Regulation (EU) 2016/679 (GDPR) and implementing national laws, the data protection laws in Guernsey (in particular the Data Protection (Bailiwick of Guernsey) Law of 2017) or UK GDPR, as applicable ("Data Protection Laws").

The identity of the Reporting Person will be processed in a confidential manner. This means that the identity of the Reporting Person will not be disclosed to anyone beyond the authorized staff members competent to receive or follow up on reports, except where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, or with the Reporting Person's explicit consent. This also applies to any other information from which the identity of the Reporting Person may be directly or indirectly deduced.

More generally, any processing of personal data, including the collection, exchange, transmission or storage of personal data as part of the collection and handling of reports and their investigation, shall be carried out in accordance with applicable Data Protection Laws, as further detailed in the Group's relevant data protection information notices as may be amended from time to time, in particular the Privacy Notice for Employees, as available on our intraweb or from your local HR, as far as employees are concerned, and the general Data Protection Policy for non-employees, as available on our

website, CLdN, as the case may arise, together with the concerned Subsidiary, is the data controller of personal data collected and processed in relation to the Central Reporting Channel. Each Subsidiary, as identified in the Country-specific Addendum below, acts as the controller of personal data collected and processed in relation to the Local Reporting Channel for its jurisdiction. The Central Reporting Channel and the Local Reporting Channels are operated by a third-party administrator, Whistleblower Software, acting on behalf and under the instructions of CLdN and/or the concerned Subsidiary, as applicable, in accordance with applicable Data Protection Laws.

Personal data which is manifestly irrelevant to the handling of a specific Report shall not be collected or, if accidentally collected, shall be deleted without undue delay. More generally, personal data will be kept for no longer than it is necessary and proportionate for the purpose for which it has been collected in compliance with applicable law, as further described in the relevant Country-specific Addendum below, and, as applicable, the Group's data retention policy available on request by sending an e-mail to GDPR@cldn.com.

Data subjects can exercise their rights of access, rectification, deletion, transfer (portability), limitation of the processing and objection as described in the Group's relevant data protection information notices identified above. They also have the right to withdraw their consent at any time, and to file complaints with the competent data protection authority(ies).

C. ANONYMITY

The Group's internal reporting channels allow for the submission and subsequent processing of anonymous reports. In this case, anonymous Reports will be handled with increased care, such as preliminary review by the first recipient of the Report as to whether it is appropriate to process it through the reporting mechanism.

As a general rule, the Reporting Person is however encouraged to disclose his or her identity rather than proceed with an anonymous Report. The reason is that it is more difficult to follow up on a Report and to conduct a thorough and complete investigation if it is impossible or difficult to contact the source for further information. If the Reporting Person identifies himself or herself, it may be easier to protect him or her against retaliation.

5. Internal reporting channels and procedures

The Group hopes that in many cases individuals will be able to raise any concerns with their line manager or usual contact person within the Group. Concerns may be shared in person or the matter may be put in writing. Line managers may be able to agree a way of resolving the concern quickly and effectively. In some cases they may refer the matter to the internal reporting channel(s) as outlined below.

A. CENTRAL REPORTING CHANNEL

A central reporting channel has been established where concerns can be sent to central management. Please click here to access this central reporting channel: https://whistleblowersoftware.com/

I. Access to the central reporting channel

The central reporting channel is accessible:

- via the reporting platform at https://whistleblowersoftware.com/, which allows the reporter to make online reports in writing or orally, and is administered by an independent third party on behalf of the relevant Subsidiary;
- upon request, a Report may also be made by means of a physical meeting or videoconference within a reasonable timeframe by contacting whistleblower@cldn.com.

II. Reception and handling of Reports

All Reports made through the central reporting channel will be received by the person or department in charge of the central reporting channel, this being C.Legal BV.

When the relevant Report Manager receives the Report, he or she will provide written acknowledgment of receipt of the Report to the Reporting Person within seven (7) working days of the receipt of the Report. The following can subsequently occur:

- If the concern does not meet the requirements set out under this Policy and therefore is not admissible, it will not be considered a Report and the Reporting Person will be informed of the reasons underlying this inadmissibility.
- If the Report Manager considers that the Report reveals a structural problem within the Group or facts that affect two (2) or more Subsidiaries and that can only be effectively addressed with a cross-border approach, the Report Manager may inform – and, where legally required, obtain the consent of the Reporting Person – to share or transfer the Report with other members of the Group.
- If the Report Manager considers that the Report would be handled more effectively by another Subsidiary or by the Group alone, it may invite the Reporting Person to withdraw the Report it has initially filed so that the matter can be investigated by the other Subsidiary or Group instead. In such case, the Reporting Persons understands that he or she may still report externally to the relevant competent authority as described below and in the Country-specific Addendum.

  In any case, the relevant Subsidiary will remain responsible and accountable until the Report is withdrawn, including for maintaining confidentiality, giving feedback, and addressing the reported Breach.

Persons referred to in the Report will be informed of the Report and the facts identified therein in accordance with applicable data protection law. Such Information may be delayed in exceptional circumstances (for ex., risk of destruction of evidence). This information may however be deferred when it is likely to seriously jeopardize the purpose for which information is being processed.

III. Investigation of the Report

The relevant Report Manager will make a preliminary assessment of the Report and decide on the next course of action.

The Report Manager will handle and investigate the Report locally to the fullest possible.

Depending on the severity and scope of the reported Breach, where legally permissible and subject to the Reporting Person's right to object, the Reporting Manager may request the assistance of the Group's investigation team, subject to the following:

- Requirement of specific expertise within the Group to continue the investigation

In addition, to the extent necessary, the Reporting Manager may rely on external counsel bound by professional secrecy obligations to assist with the investigation and the handling of the Report. In any case, confidentiality and data protection obligations will be duly complied with

In any case, the investigation will be carried out and the feedback will be provided in writing within a maximum of three (3) months from the acknowledgement of receipt of the Report (or, if no acknowledgment was sent, three (3) months from the expiry of a seven (7) working day period after the Report was made) with measures contemplated or adopted to follow up on the Report to address the Breach in question, with reasons for such measures.

IV. How is information retained?

Where a person requests a meeting with the staff members or where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the Reporting Person, the oral reporting may be documented by making a recording of the conversation in a durable and retrievable form or through a complete and accurate transcript of the conversation.

Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, the oral reporting will be documented in the form of accurate minutes of the conversation.

The Reporter will be able to check, rectify and agree the minutes of the conversation by signing them.

V. Resolution

Once the investigation is concluded, if the reported Breach is shown to be justified, then the corresponding actions will be adopted according to the relevant Subsidiary's and Group's procedures and applicable local legislation.

B. THE LOCAL REPORTING CHANNELS

I. Access to the local reporting channels

In addition to the Central Reporting Channel described above, where permitted under applicable legislation, Breaches may be locally reported to each Subsidiary in the Relevant Country, as described below and in the relevant Country-specific Addendum below (the "Local Internal Channels").

The local reporting channels are accessible:

- via the reporting platform at https://whistleblowersoftware.com/, which allows the reporter to make online reports in writing or orally, and is administered by an independent third party on behalf of the relevant Subsidiary;
- upon request, a Report may also be made by means of a physical meeting or videoconference within a reasonable timeframe by contacting the Local Reporting Manager identified in the Country-specific Addendum.

II. Reception and handling of Reports

All Reports made through the local reporting channels will be received by the person or department in charge of such local reporting channel in the relevant Subsidiary as identified in the relevant Country-specific Addendum (each of them, the "Local Report Manager").

When the relevant Local Report Manager receives the Report, he or she will provide written acknowledgment of receipt of the Report to the Reporting Person within seven (7) working days of the receipt of the Report. The following can subsequently occur:

- If the concern does not meet the requirements set out under this Policy and therefore is not admissible, it will not be considered a Report and the Reporting Person will be informed of the reasons underlying this inadmissibility.
- If the Local Report Manager considers that the Report reveals a structural problem within the Group or facts that affect two (2) or more Subsidiaries and that can only be effectively addressed with a cross-border approach, the Local Report Manager may inform – and, where legally required, obtain the consent of the Reporting Person – to share or transfer the Report with the Central Reporting Channel.
- If the Local Report Manager considers that the Report would be handled more effectively by another Subsidiary or by the Group alone, it may invite the Reporting Person to withdraw the Report it has initially filed so that the matter can be investigated by the other Subsidiary or Group instead. In such case, the Reporting Persons understands that he or she may still report externally to the relevant competent authority as described below in 6. External reporting channels and in the Country-specific Addendum.

In any case, the relevant Subsidiary will remain responsible and accountable until the Report is withdrawn, including for maintaining confidentiality, giving feedback, and addressing the reported Breach.

Persons referred to in the Report will be informed of the Report and the facts identified therein in accordance with applicable data protection law. Such Information may be delayed in exceptional circumstances (for ex., risk of destruction of evidence). This information may however be deferred when it is likely to seriously jeopardize the purpose for which information is being processed.

III. Investigation of the Report

The relevant Local Report Manager will make a preliminary assessment of the Report and decide on the next course of action.

The Local Report Manager will handle and investigate the Report locally to the fullest possible.

Depending on the severity and scope of the reported Breach, where legally permissible and subject to the Reporting Person's right to object, the Local Reporting Manager may request the assistance of the Group's investigation team, subject to the following:

- Requirement of specific expertise within the Group to continue the investigation

In addition, to the extent necessary, the Local Reporting Manager may rely on external counsel bound by professional secrecy obligations to assist with the investigation and the handling of the Report. In any case, confidentiality and data protection obligations will be duly complied with

In any case, the investigation will be carried out and the feedback will be provided in writing within a maximum of three (3) months from the acknowledgement of receipt of the Report (or, if no acknowledgment was sent, three (3) months from the expiry of a seven (7) working day period after the Report was made) with measures contemplated or adopted to follow up on the Report to address the Breach in question, with reasons for such measures.

IV. How is information retained?

Where a person requests a meeting with the staff members or where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the Reporting Person, the oral reporting may be documented by making a recording of the conversation in a durable and retrievable form or through a complete and accurate transcript of the conversation.

Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, the oral reporting will be documented in the form of accurate minutes of the conversation.

The Reporter will be able to check, rectify and agree the minutes of the conversation by signing them.

V. Resolution

Once the investigation is concluded, if the reported Breach is shown to be justified, then the corresponding actions will be adopted according to the relevant Subsidiary's and Group's procedures and applicable local legislation.

6. External reporting channels

While the Group expects Employees and Third Parties to feel comfortable reporting their concerns through the Internal Channels, whether through the Central Reporting Channel or through the Local Internal Channel of the relevant Subsidiary, if any, they may also be occasions where they feel more appropriate to report Breaches externally to the competent external authorities mentioned in the Country-specific Addendum. Where relevant, Reporters may report to EU institutions, bodies, offices or agencies.
The Group however strongly encourages employees to use the internal report channels outlined in this Policy, so that the Group has an opportunity to investigate and remedy any concerns.

7. Key contacts

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact:
Whistleblower@cldn.com

8. Key policy infromation

A. VIOLATIONS AND DISCIPLINARY ACTION

Any Group officer, director, manager, employee or other stakeholder that engages in conduct contrary to this Policy and/or Group's ethical standards and principles, as set forth in the Code of Conduct, may be subject to disciplinary action, including, in appropriate circumstances, termination, in accordance with the requirements of applicable law upon a finding of:

- violation of law or the Group's Policies;
- retaliation;
- failure to cooperate with any investigation undertaken under this Policy;
- providing by false or misleading information to an investigative team conducting an investigation into suspected misconduct hereunder; or
- bad faith reporting for malicious or improper purposes.

B. POLICY REVIEW

This Policy will be reviewed as circumstances dictate.

Management are responsible for the implementation, monitoring and review of this Policy. However, all employees are obliged to adhere to, and support the implementation of this Policy. This Policy does not form part of any contract of employment and does not create contractual rights or obligations.

Whistleblowing policy and procedure

COUNTRY-SPECIFIC ADDENDA

Overview

Country-specific addendum:

Belgium

This Country-specific Addendum for Belgium (the "Belgium Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Belgium:

- **C.LEGAL BV** with registered offices at Sint-Amandsstraat 93, 1853 Grimbergen, Belgium, RPM/RPR Brussels, VAT BE 0880.195.222.
- **CLdN IT Applications NV,** with registered offices at Sneeuwbeslaan 14, 2610 Antwerp, Belgium, RPM/RPR Antwerp, VAT BE 0473.462.740
- **CLdN RoRo AGENCIES NV,** with registered offices at Hendrik van Minderhoutstraat 50, 8380 Bruges, Belgium, RPM/RPR Ghent (division Bruges), VAT BE 0467.484.273.
- C**LdN CARGO NV,** with registered offices at Alfred Ronsestraat 100, 8380 Bruges, Belgium, RPM/RPR Ghent (division Bruges), VAT BE 0475.233.187.
- **CLdN PORTS ZEEBRUGGE NV,** with registered offices at Hendrik van Minderhoutstraat 50, 8380 Bruges, Belgium, RPM/RPR Ghent (division Bruges), VAT BE 0418.294.979.
- **CLdN TECH NV,** with registered offices at Hendrik van Minderhoutstraat 50, 8380 Bruges, Belgium, RPM/RPR Ghent (division Bruges), VAT BE 0435.508.323.

hereafter referred as "CLdN Belgium", in accordance with the provisions of the Act of November 28, 2022 on the protection of persons who report breaches of national or Union law within legal entities in the private sector ("the Belgian Whistleblower Act"), which implements the EU Whistleblower Directive.

This Belgium Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. PERSONAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the scope described in section 3.A of the Policy, this Policy also applies to Employees and Third Parties who have obtained information outside a work-related context, if the Report relates to financial services, products and markets and the money laundering legislation.

2. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Belgium's local reporting channel(s):

- any violation of the legal or regulatory (Belgian) provisions or the directly applicable European provisions, as well as the provisions taken in execution of these provisions, specifically for (i) the areas listed in section 3.B of the Policy, (ii) the fight against tax fraud and (iii) the fight against social fraud.

3. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

C.LEGAL BV	Joshi Grosemans (joshi.grosemans@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN IT Applications NV	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN RoRo AGENCIES NV	Trango BV duly represented by Joost Rubens (joost.rubens@cldn.com) and VOF Navira duly represented by Florent Maes (florent.maes@cldn.com)
CLdN CARGO NV	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN PORTS ZEEBRUGGE NV	Trango BV duly represented by Joost Rubens (joost.rubens@cldn.com) and VOF Navira duly represented by Florent Maes (florent.maes@cldn.com)
CLdN TECH NV	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

4. INVESTIGATIONS AND SHARING RESOURCES

For the Subsidiaries with less than 250 employees, Employees and Third Parties are informed that the Subsidiary may benefit from the investigative capacity of the Group level in the investigation of Reports and a designated person/department at Group level will be authorised to access the Report (for the purpose of carrying out the necessary investigation), it being noted that the Reporting Person maintains the right to object and to request that the investigation be conducted only at the Subsidiary level. In any case, any follow-up measure will be taken and feedback to the Reporting Person is given at the level of the Subsidiary.

5. SAFEGUARDS

In addition to the safeguards described under section 4 of the Policy, it is underlined that the identity of the Reporting Person may only be communicated with their express and free consent, save for the exceptions under Article 20 of the Belgian Whistleblower Act. This also applies to any information from which the identity of the Reporting Person may be directly or indirectly deduced.

In accordance with the Belgian Whistleblower Act, when the identity of the Reporter and any information from which this identity may be directly or indirectly deduced are disclosed without the consent of the Reporter pursuant to specific legislation in the context of investigations by national authorities or judicial proceedings the Reporting Person will be informed thereof beforehand, unless such information would risk jeopardising the investigations or judicial proceedings concerned.

The Reporting Person maintains at all times the right not to incriminate themselves when making a Report.

6. EXTERNAL REPORTING CHANNELS

CLdN Belgium strongly encourages reports to be made internally so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, besides the federal coordinator, they can report to the relevant Belgian competent authorities, i.e.:

- the Federal Public Service Economy;
- the Federal Public Service Finance;
- the Federal Public Service Public Health, Food Chain Safety and Environment;
- the Federal Public Service Mobility and Transportation;
- the Federal Public Service Employment, Labour and Social Dialogue;
- the Programming Public Service for Social Integration, Poverty Reduction, Social Economy and Metropolitan Policy;
- the Federal Agency for Nuclear Control; the Federal Agency for Medicines and Health Products;
- the Federal Agency for the Safety of the Food Chain;
- the Belgian Competition Authority; the Data Protection Authority; the Financial Services and Markets Authority;
- the National Bank of Belgium;
- Belgian Audit Oversight Board;
- the authorities mentioned in article 85 of the law of September 18, 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash;
- the National Committee for the Security of Drinking Water Supply and Distribution;
- the Belgian Institute for Postal Services and Telecommunications;
- the National Institute for Health and Disability Insurance;
- The National Institute for the Social Security of the Self-employed;
- the National Employment Office;
- the National Social Security Office;
- the Social Intelligence and Investigation Service;
- the Autonomous Anti-Fraud Coordination Service; and
- the Shipping Control.

The way to make external reports can be found on the websites of the relevant competent authorities.

7. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the Reporting Person, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations and the specific retention periods contained in the Belgian Whistleblower Act. In particular:

- Reports will be kept for the duration of the work-related relationship of the Reporter with CLdN Belgium.
- The name, function and contact details of the Reporting Person and of any person to whom the protection and support measures under the Belgian Whistleblower Act extend, as well as the subjects of the Report and any third parties mentioned in the Report (including, where applicable, their company number) will be saved until the reported violation is time-barred.
- In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will in any event be retained until the end of the proceedings or the end of the limitation period for appeals against the decision.
- Further, CLdN Belgium may retain personal data relating to a Report for up to five (5) years, in intermediate storage, if it is legally obliged to do so (for example, to meet accounting, social or tax obligations).

Personal data relating to out-of-scope Reports will be destroyed without undue delay.

8. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following person(s):
Whistleblower@cldn.com

Country-specific addendum:

United Kingdom

This Country-specific Addendum for the United Kingdom (the "UK Addendum") describes the specific requirements applying to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in the United Kingdom:

- **CLdN Automotive Ltd** with registered office at 130, Shaftesbury, 2nd Floor, London, WI1D 5EU, Company Number 04999257, VAT GB832530452
- **CLdN Ports London Ltd** with registered office at 130, Shaftesbury, 2nd Floor, London, WI1D 5EU, Company Number 02535265, VAT GB583098118
- **CLdN RoRo Agencies Ltd.** with registered office at 130, Shaftesbury, 2nd Floor, London, WI1D 5EU, Company Number 01651777, VAT GB407023006
- **CLdN Cargo UK Ltd** with registered office at 130, Shaftesbury, 2nd Floor, London, WI1D 5EU, Company Number 05523357, VAT GB868949735
- **CLdN Ports Killingholme Ltd** with registered office at 130, Shaftesbury, 2nd Floor? London, WI1D 5EU, Company Number 00278815, VAT GB668335014
- **CLdN Automotive Ltd** with registered office at 130, Shaftesbury, 2nd Floor, London, WI1D 5EU, Company Number 04999257, VAT GB832530452
- **CLdN Ports BCP Ltd** with registered office at 130, Shaftesbury, 2nd Floor, London, WI1D 5EU, Company Number 13402718, VAT GB394834061
- **Seatruck Ferries Ltd** with registered office at North Quay, Port Of Heysham, Morecambe, Lancashire, LA3 2UH, Company Number 05651131, VAT GB882496085

hereafter referred as "CLdN UK"

This UK Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. PERSONAL SCOPE OF LOCAL REPORTING CHANNEL(S)

The scope of the Policy is broader than the protection available to Reporting Persons under local law. You may therefore wish to take advice before you make your Report. Contact details for Protect, the whistleblowing charity, appear at section 6 of this UK Addendum.

2. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN UK's local reporting channel(s):

- criminal offences;
- breach of a legal obligation;
- miscarriages of justice;
- danger to health and safety;
- damage to the environment;
- information tending to show that these types of wrongdoing have been or are likely to be concealed.

3. LOCAL REPORT MANAGER

The impartial person or department who is competent for receiving and following-up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN Automotive Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
CLdN Ports London Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
CLdN RoRo Agencies Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
CLdN RO-RO Agencies Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)

CLdN Ports Killingholme Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
CLdN Automotive Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
CLdN Ports BCP Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
CLdN Ports BCP Ltd	Benjamin Dove-Seymour (benjamin.dove-seymour@cldn.com) and Joost Rubens (joost.rubens@cldn.com)
Seatruck Ferries Ltd	Alexis Donaghey (ado@seatruckgroup.co.uk) and Joost Rubens (joost.rubens@cldn.com)

4. EXTERNAL REPORTING CHANNELS

CLdN UK strongly encourages reports to be made internally so that any concerns can be resolved.

The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. It will very rarely if ever be appropriate to alert the media. We strongly encourage you to seek advice before reporting a concern to anyone external. The independent whistleblowing charity, Protect, operates a confidential helpline. They also have a list of prescribed regulators for reporting different types of concern. The contact details for Protect are available here: https://protect-advice.org.uk/ Their helpline number is currently 0203 117 2520.

5. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

The appropriate retention period will vary depending on the person making the report, the nature of the report and any legal, investigatory or regulatory context. Reports by Employees will typically be retained for the duration of the employment relationship and seven (7) years after its termination.

6. LOCAL CONTACTS

In case of questions regarding the internal reporting channels or in case of need for support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Country-specific addendum:

The Netherlands

This Country-specific Addendum for the Netherlands (the "Dutch Addendum") describes the specific requirements applying to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in the Netherlands:

- **CLdN Ports Netherlands BV Rotterdam** with registered office at Merseyweg 70, 3197KG Botlek Rotterdam, KvK number 24314655, VAT NL8094.18.204B01
- **CLdN Ports Netherlands BV Vlissingen** with registered office at Ritthemsestraat 497, 4389PA Ritthem, KvK number 24314655, VAT NL8094.18.204B01
- **CLdN Automotive B.V.** with registered office at Merseyweg 50, 3197KG Botlek Rotterdam, KvK number 24143674, VAT NL0056.43.302b01
- **Rotterdam Car Center B.V**. with registered office at Merseyweg 50, 3197KG Botlek Rotterdam, KvK number 24160973, VAT NL0071.47.636B01
- **Rotterdam Automotive Services B.V.** with registered office at Merseyweg 50, 3197KG Botlek Rotterdam, KvK number 24368901, VAT NL8137.12.890B01
- **CLdN Tech BV** with registered office at Ritthemsestraat 497, 4389PA Ritthem, KvK number 24330184, VAT NL8105.20.151B01.
- **CLdN RoRo Agencies B.V.** with registered office at Ritthemsestraat 497, 4389PA Ritthem, KvK number 22055726, VAT NL8134.10.393B01
- **CLdN Cargo B.V. (Rotterdam**) with registered office at Merseyweg 70, 3197KG Botlek Rotterdam, KvK number 22054131, VAT NL8127.27.666B01
- **CLdN Fleet Supervision B.V**. with registered office at Oostkade 25, 4551CM Sas van Gent, KvK number 50675885, VAT NL8228.66.523B01

hereafter referred as "CLdN the Netherlands", in accordance with the provisions of the Dutch Whistleblower Protection Act ("the Dutch Whistleblower Act"), which implements the EU Whistleblower Directive.

This Dutch Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of discrepancy.

1. PERSONAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN the Netherlands' local reporting channel(s):

- An act or omission involving the public interest in: (i) the violation or risk of violation of a statutory regulation or internal rules containing a concrete obligation and established by an employer pursuant to a statutory regulation; or (ii) the danger to public health, to the safety of persons, to damage to the environment or to the proper functioning of the company by improper acts or omissions.

2. LOCAL REPORT MANAGER

The impartial person or department who is competent for receiving and following-up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN Ports Netherlands BV Rotterdam	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Ports Netherlands BV Vlissingen	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Automotive B.V.	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
Rotterdam Car Center B.V.	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
Rotterdam Automotive Services B.V.	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Tech BV	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN RoRo Agencies B.V.	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Cargo B.V.	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

CLdN Fleet Supervision B.V.	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

3. INVESTIGATIONS AND SHARING RESOURCES

For the Subsidiaries with less than 250 employees, Employees and Third Parties are informed that the Subsidiary may benefit from the investigative capacity of the Group level in the investigation of Reports and a designated person/department at Group level will be authorised to access the Report (for the purpose of carrying out the necessary investigation), it being noted that the Reporting Person maintains the right to object and to request that the investigation be conducted only at the Subsidiary level. In any case, any follow-up measure will be taken and feedback to the Reporting Person is given at the level of the Subsidiary.

4. SAFEGUARDS

In addition to the safeguards described under section 4 of the Policy, it is underlined that the identity of the Reporting Person will not be disclosed to anyone beyond the individuals competent and designated to receive, follow-up on Reports, unless the Reporting Person provides consent for further disclosure, save for the exceptions under Article 1(a) of the Dutch Whistleblower Act. This also applies to any information from which the identity of the Reporting Person may be directly or indirectly deduced. Only persons on a strict need-to-know basis will collect and process the Reports, including any personal data of the Reporting Person. These persons will be subject to a duty of confidentiality.

In accordance with Article 1(a) of the Dutch Whistleblower Act, when the identity of the Reporter and any information from which this identity may be directly or indirectly deduced are disclosed without the consent of the Reporter pursuant to specific legislation in the context of investigations by national authorities or judicial proceedings, the Reporting Person will be informed thereof beforehand, unless such information would risk jeopardising the investigations or judicial proceedings concerned.
The Reporting Person maintains at all times the right not to incriminate themselves when making a Report.

5. EXTERNAL REPORTING CHANNELS

CLdN the Netherlands strongly encourages reports to be made internally so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, besides the federal coordinator, they can report to the relevant Dutch competent authorities, i.e.:

- Authority for Consumer & Markets, ACM (in Dutch: “Autoriteit Consument en Markt”);
- Authority for Financial Markets, AFM (in Dutch: “Autoriteit Financiële Markten”);
- Data Protection Authority (in Dutch: “Autoriteit Persoonsgegevens”);
- De Nederlandsche Bank N.V.;
- Whistleblowers Authority (in Dutch: “Huis voor Klokkenluiders”);
- Health and Youth Care Inspectorate, IGJ (in Dutch: “Inspectie gezondheidszorg en jeugd”);
- Dutch Healthcare Authority, NZa (in Dutch: “Nederlandse Zorgautoriteit”);
- Nuclear Safety and Radiation Protection Authority (in Dutch: “de Autoriteit Nucleaire Veiligheid en Stralingsbescherming”); and
- Other authorities appointed by the minister or statute.

You may also seek advice on a confidential basis from the Advice Department of the Dutch Whistleblowers Authority before making a Report (advies@huisvoorklokkenluiders.nl).

The relevant modalities for external reports can be found on the websites of the relevant competent authorities.

6. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the Reporting Person, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations and the specific retention periods contained in the Dutch Whistleblower Act. In particular:

- Reports will be kept for the duration of the work-related relationship of the Reporter with CLdN the Netherlands.
- The name, function and contact details of the Reporting Person and of any person to whom the protection and support measures under the Dutch Whistleblower Act extend, as well as the subjects of the Report and any third parties mentioned in the Report (including, where applicable, their company number) will be saved until the reported violation is time-barred.
- In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will in any event be retained until the end of the proceedings or the end of the limitation period for appeals against the decision.
- Further, CLdN the Netherlands may retain personal data relating to a Report for up to two (2) years after the Report has been dealt with, unless the personal data are necessary for compliance with a statutory retention obligation (e.g. seven (7) years, in intermediate storage, if it is legally obliged to do so to meet accounting, social or tax obligations).

Personal data relating to out-of-scope Reports will be destroyed without undue delay.

7. LOCAL CONTACTS

In case of questions regarding the internal reporting channels or in case of need for support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Country-specific addendum:

Luxembourg

This Country-specific Addendum for Luxembourg (the "Luxembourg Addendum") describes the specific requirements applying to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Luxembourg:

- **CLdN IT Systems SA** with registered office at 3-7, rue Schiller L-2519 Luxembourg – RCS Luxembourg B122977, VAT LU27657653
- **CLdN RoRo SA** with registered office at 3-7, rue Schiller L-2519 Luxembourg – RCS Luxembourg B103758, VAT LU22055614
- **CLdN Links SA** with registered office at 3-7, rue Schiller L-2519 Luxembourg – RCS Luxembourg B73465, VAT LU19041241
- **CLdN Cargo SA** with registered office at 3-7, rue Schiller L-2519 Luxembourg – RCS Luxembourg B171978, VAT LU25840235

hereafter referred as "CLdN Luxembourg", in accordance with the provisions of the *Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union* (the "Luxembourgish Whistleblower Act"), which implements the EU Whistleblower Directive.

This Luxembourgish Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of discrepancy.

1. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Luxembourg's local reporting channel(s):

- Any acts or omissions that are unlawful or are contrary to the object or purpose of directly applicable provisions of national or European law.

2. LOCAL REPORT MANAGER

The impartial person or department who is competent for receiving and following-up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN IT Systems SA	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN RoRo SA	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Links SA	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Cargo SA	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

3. EXTERNAL REPORTING CHANNELS

CLdN Luxembourg strongly encourages reports to be made internally so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, besides the office de signalement as created by articles 8 seq. of the Luxembourgish Whistleblower Act, they can report to the relevant Luxembourgish competent authorities, i.e.:

- The Financial Sector Supervisory Commission;
- The Insurance Commission;
- The Competition Authority;
- The Administration of Registration, Domains and VAT;
- The Labour and Mines Inspectorate;
- The National Commission for Data Protection;
- The Centre for Equal Treatment;
- The Ombudsman in the context of his external control of places where people are deprived of their liberty;
- The Ombudsman for kids and youth;
- The Luxembourg Regulatory Institute;
- The Luxembourg Independent Audiovisual Authority;
- L'Ordre des avocats du Barreau de Luxembourg and l'Ordre des avocats du Barreau de Diekirch; The Luxembourg Bar Association;

- The Chamber of Notaries;
- The Medical College;
- The Administration of Nature and Forests;
- The Administration of Water Management; The Administration of Air Navigation;
- The Administration of Air Navigation;
- The National Consumer Ombudsman Service;
- The Order of Architects and Consulting Engineers;
- he Order of Chartered Accountants;
- The Institute of Company Auditors; and
- The Direct Tax Administration.

The relevant modalities for external reports can be found on the websites of the relevant competent authorities.

4. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the Reporting Person, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations and the specific retention periods contained in the Luxembourg Whistleblower Act. In particular:

- Reports will be kept for the duration of the work-related relationship of the Reporter with CLdN Luxembourg.
- The name, function and contact details of the Reporting Person and of any person to whom the protection and support measures under the Luxembourg Whistleblower Act extend, as well as the subjects of the Report and any third parties mentioned in the Report (including, where applicable, their company number) will be saved until the reported violation is time-barred.
- In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will in any event be retained until the end of the proceedings or the end of the limitation period for appeals against the decision.
- Further, CLdN Luxembourg may retain personal data relating to a Report for up to five (5) years, in intermediate storage, if it is legally obliged to do so (for example, to meet accounting, social or tax obligations).

Personal data relating to out-of-scope Reports will be destroyed without undue delay.

5. LOCAL CONTACTS

In case of questions regarding the internal reporting channels or in case of need for support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

B. RETENTION PERIODS

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the Reporting Person, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations and the specific retention periods contained in the Dutch Whistleblower Act. In particular:

- Reports will be kept for the duration of the work-related relationship of the Reporter with CLdN the Netherlands.
- The name, function and contact details of the Reporting Person and of any person to whom the protection and support measures under the Dutch Whistleblower Act extend, as well as the subjects of the Report and any third parties mentioned in the Report (including, where applicable, their company number) will be saved until the reported violation is time-barred.
- In the case of disciplinary or legal proceedings initiated pursuant to a Report, the personal data relating to the Report will in any event be retained until the end of the proceedings or the end of the limitation period for appeals against the decision.
- Further, CLdN the Netherlands may retain personal data relating to a Report for up to two (2) years after the Report has been dealt with, unless the personal data are necessary for compliance with a statutory retention obligation (e.g. seven (7) years, in intermediate storage, if it is legally obliged to do so to meet accounting, social or tax obligations).

Personal data relating to out-of-scope Reports will be destroyed without undue delay.

7. LOCAL CONTACTS

In case of questions regarding the internal reporting channels or in case of need for support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Country-specific addendum:

Portugal

This Country-specific Addendum for Portugal (the "Portuguese Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Portugal:

- **CLdN Agencies, Unipessoal Lda.**, with registered offices at Calçada Bento Rocha Cabral, 1, 1250-047 Lisboa, VAT 513720006;
- **CLdN Cargo Portugal, Unipessoal Lda.**, with registered offices at Calçada Bento Rocha Cabral, 1, 1250-047 Lisboa, VAT 513011170;
- **CLdN Ports Porto, S.A.**, with registered offices at Rua Dom Marcos da Cruz, 2029, 2.º Direito, Frente, 4455-482 Perafita, VAT 514535547;

hereafter referred as "CLdN Portugal", in accordance with the provisions of Law no. 93/2021, of 20 December ("the Portuguese Whistleblower Act"), which implements the EU Whistleblower Directive.

This Portuguese Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Portugal's local reporting channel(s):

- violent crime, especially violent and highly organised crime, as well as organised and economic-financial crime.

In the field of national defence and security, only an act or omission contrary to the procurement rules contained in the European Union acts referred to in part i.A of the Annex to Directive (EU) 2019/1937, or contrary to the purposes of those rules, shall be considered an infringement for the purposes of the Portuguese Whistleblower Act.

2. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN Agencies, Unipessoal Lda.,	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Cargo Portugal, Unipessoal Lda.,	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)
CLdN Ports Porto, S.A.,	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

3. INVESTIGATIONS AND SHARING RESOURCES

Employees and Third Parties are informed that the Subsidiary may benefit from the investigative capacity of the Group level in the investigation of Reports and a designated person/department at Group level will be authorised to access the Report (for the purpose of carrying out the necessary investigation), it being noted that the Reporting Person maintains the right to object and to request that the investigation be conducted only at the Subsidiary level. In any case, any follow-up measure will be taken and feedback to the Reporting Person is given at the level of the Subsidiary.

Independence, impartiality, confidentiality, data protection, secrecy, and absence of conflict of interest in the performance of the relevant functions will be guaranteed in the reporting channel operations.

4. SAFEGUARDS

In addition to the safeguards described under section 4 of the Policy, in accordance with the Portuguese Whistleblower Act, disclosure of the identity of the Reporter and any confidential information shall be preceded by written communication to the Reporter informing of the reasons for disclosure, unless such information to the Reporter would risk jeopardising the investigations or judicial proceedings concerned.

5. EXTERNAL REPORTING CHANNELS

Internal reporting is the preferential channel to report a concern.
The Reporter may only report a concern externally if:

- the Reporter has reasonable grounds to believe that the breach cannot be effectively known or resolved internally or that there is a risk of retaliation;
- the Reporter was not informed of the actions or the conclusion follow-up within the timeframes referred in the Policy;
- a criminal offence or an administrative offence punishable with a fine of more than EUR 50,000 may be involved.

The Reporter will not be protected under this Policy if the concerns are reported externally without complying with the abovementioned rules of precedence.

External complaints shall be submitted to the authorities which, in accordance with their duties and powers, should or may have knowledge of the matter covered by the complaint, including:

- the Public Prosecutor's Office;
- the criminal police agencies;
- the Bank of Portugal;
- the independent administrative authorities;
- public institutes;
- inspectorates-general and similar entities and other central services of the direct administration of the State endowed with administrative autonomy;
- local authorities; and
- public associations.

The way to make external reports can be found on the websites of the relevant competent authorities.

6. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Records of reports received shall be stored for no longer than what is necessary and proportionate for CLdN Portugal to comply with requirements imposed by the Portuguese Whistleblower Act.
In particular, whistleblowing reports and related investigation documentation will be kept for at least five (5) years. Longer retention time may apply if further processing is necessary for the establishment, exercise or defence of legal claims. When whistleblowing reports and related investigation document relate to anti-money laundering and countering the financing of terrorism legislation, these will be kept for seven (7) years.

7. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact:
Whistleblower@cldn.com

Country-specific addendum:

Sweden

This Country-specific Addendum for Sweden (the "Swedish Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary in Sweden:

- **CLdN RoRo Agencies AB,** with registered address at Box 2381, 403 16 Göteborg, Sweden, corporate registration number 556573-0479.

hereafter referred as "CLdN Sweden", in accordance with the provisions of the Act on protection for persons who report breaches (in Swedish: "lagen om skydd för personer som rapporterar om missförhållanden") ("the Swedish Whistleblower Act"), which implements the EU Whistleblower Directive, as well as the Regulation on Processing of Personal Data Relating to Criminal Convictions (DIFS 2018:2) issued by the Swedish Authority for Privacy Protection (in Swedish: "IMY").

This Swedish Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. PERSONAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the scope described in section 3.A of the Policy, this Policy also applies to who otherwise are available for performing work under CLdN Sweden's control and instruction, as well as shareholders who are available to be or are active in the company.

2. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

Given the number of headcount at CLdN Sweden, the In-Scope areas are strictly limited to the following matters when using the Central Reporting Channel or the Local Internal Channel:

- serious improprieties committed by individuals in key or leading positions within CLdN or the Group concerning one or several of the following subject matters:
  - accounting;
  - internal accounting controls;
  - auditing;
  - prevention of bribery;
  - criminal activity within banking or finance; or
  - other serious improprities concerning the organisation's vital interests or the life or health of an individual.

3. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN RoRo Agencies AB	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

4. SAFEGUARDS

The safeguards described under section 4 of the Policy apply where reports are made internally (i.e. by using the Central Reporting Channel or the Local Internal Channel), externally (i.e. by reporting to the relevant competent authorities as set out below), and by public disclosure, always subject to the conditions under the Swedish Whistleblower Act, as applicable from time to time.

In addition to the safeguards described under section 4 of the Policy, kindly note that under the Swedish Freedom of Press Act (in Swedish: "*tryckfrihetsförordningen*") and the Swedish Fundamental Law on Freedom

of Expression (in Swedish: "*yttrandefrihetsgrundlagen*") everyone is free to communicate information on any subject whatsoever for the purpose of publication in programmes or technical recordings (freedom to communicate information, in Swedish: "*meddelarfrihet*") as well as right to procure information on any subject whatsoever in order to communicate or publish it (freedom to procure information, in Swedish: "*anskaffarfrihet*"). An employee's duty of loyalty to his or her employer may restrict these rights.

5. EXTERNAL REPORTING CHANNELS

CLdN Sweden strongly encourages reports to be made internally using the Central Reporting Channel or the Local Internal Channel so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, they can report to the relevant Swedish competent authorities, i.e.:

Swedish competent authority	**The authority's area of responsibility**
Konkurrensverket	Breaches falling within the scope of public procurement that is covered by the authority's supervisory responsibility
Fastighetsmäklarinspektionen, Finansinspektionen, länsstyrelserna i Stockholms, Västra Götalands and Skåne län, Revisorsinspektionen and Spelinspektionen	Breaches falling within the scope of financial services, products and markets, and prevention of money laundering and terrorist financing that is covered by the authority's supervisory responsibility
Arbetsmiljöverket, Boverket, Elsäkerhetsverket, Folkhälsomyndigheten, Inspektionen för strategiska produkter, Kemikalieinspektionen, Konsumentverket, Livsmedelsverket, Läkemedelsverket, länsstyrelserna, Myndigheten för samhällsskydd och beredskap, Naturvårdsverket, Post-och telestyrelsen, Statens energimyndighet, Statens jordbruksverk, Styrelsen för ackreditering och teknisk kontroll and Transportstyrelsen	Breaches falling within the scope of product safety and compliance that is covered by the authority's supervisory responsibility
Transportstyrelsen	Breaches falling within the scope of transport safety that is covered by the authority's supervisory responsibility
Havs-och vattenmyndigheten, Kemikalieinspektionen, Livsmedelsverket, länsstyrelserna, Naturvårdsverket, Skogsstyrelsen and Statens jordbruksverk	Breaches falling within the scope of protection of the environment that is covered by the authority's supervisory responsibility
Livsmedelsverket and Strålsäkerhetsmyndigheten	Breaches falling within the scope of radiation protection and nuclear safety that is covered by the authority's supervisory responsibility
Livsmedelsverket and Statens jordbruksverk	Breaches falling within the scope of food and feed safety, animal health and welfare that is covered by the authority's supervisory responsibility
Folkhälsomyndigheten, Inspektionen för vård och omsorg, Konsumentverket and Läkemedelsverket	Breaches falling within the scope of public health that is covered by the authority's supervisory responsibility
Finansinspektionen and Konsumentverket.	Breaches falling within the scope of consumer protection that is covered by the authority's supervisory responsibility
Finansinspektionen, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Livsmedelsverket, Post-och telestyrelsen, Statens energimyndighet and Transportstyrelsen.	Breaches falling within the scope of protection of privacy and personal data, and security of network and information systems that is covered by the authority's supervisory responsibility
Ekobrottsmyndigheten	Breaches falling within the scope of the union's financial interests as referred to in 2.1 b Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, regarding fraud
Skatteverket	Breaches falling within the scope of the union's financial interests as referred to in 2.1 b Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, regarding taxes
Regeringskansliet	Breaches falling within the scope of the union's financial interests as referred to in 2.1 b Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, regarding state aid
Konkurrensverket	Breaches falling within the scope of the union's financial interests as referred to in 2.1 b Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, regarding the area of competition

Regeringskansliet	Breaches falling within the scope of the union's financial interests as referred to in 2.1 b Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, regarding the area of state aid
Skatteverket	Breaches falling within the scope of the union's financial interests as referred to in 2.1 b Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, regarding corporate taxes
Arbetsmiljöverket	Breaches not covered by another authority's supervisory responsibility

The way to make external reports can be found on the websites of the relevant competent authorities.

6. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Reports, including recordings, transcripts and minutes, will only be kept for as long as is strictly necessary and proportionate for their investigation and for the protection of the Reporting Person, the subjects of the Report and any third parties mentioned in the Report, taking into account the time required for any further investigations and the specific retention periods contained in the Swedish Whistleblower Act. Personal data in the Report will normally be stored for two (2) years after the follow-up of the matter has been ended at the most. Longer retention time may apply if further processing is necessary for the establishment, exercise or defence of legal claims.
Personal data relating to out-of-scope Reports will be destroyed without undue delay.

7. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact:
Whistleblower@cldn.com

Country-specific addendum:

Spain

This Country-specific Addendum for Spain (the "Spanish Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Spain:

- **CLdN Ports Spain**, SL with registered office at Calle Gran Via 17 – Dpto. 402 - Bilbao 48007, Bizkaia, Spain – NIF B66981671, VAT ES B66981671

hereafter referred as "CLdN Spain", in accordance with the provisions of the Law 2/2023, of February 20, 2023, regulating the protection of persons who report regulatory violations and the fight against corruption ("the Spanish Whistleblower Act"), which implements the EU Whistleblower Directive.

This Spanish Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Spain's local reporting channel(s):

- Acts or omissions that may constitute a "serious" or "very serious" administrative infringements or criminal offences, including all those serious or very serious administrative infringements or criminal offences that involve economic loss for the Public Treasury and for Social Security.

If Employees (as defined in the Policy) do not report any breach that she/he is aware of, this could result in disciplinary actions.

2. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN Ports Spain, SL	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

In the event that Joost Rubens is absent from work (e.g. due to holidays), C.Legal will substitute him. In the event that the Local Reporting Manager is conflicted (e.g. when he/she is the subject of the report), the report can be submitted through the central group channel or sent by email to the Board of Directors Whistleblower@cldn.com

3. INVESTIGATIONS AND SHARING RESOURCES

Access to the personal data contained in the Local Reporting Channel(s) will be limited to: (i) the Local Report Manager; (ii) any other persons that directly manage the Local Reporting Channel(s); (iii) the local head of Human Resources or the corresponding duly appointed body; (iv) any data processors that may be appointed; (v) the Data Protection Officer ("DPO"), and (v) any third parties on need to know basis. The Local Report Manager Team may also involve, where necessary, the Group's investigation team or other internal professionals for the purpose of conducting an internal investigation, who are subject to a strict duty of confidentiality.

4. SAFEGUARDS

In addition to the safeguards described under section 4 of the Policy, the following individuals will be protected against retaliation:

- The legal representatives of employees in the exercise of their functions of advising and supporting the reporting person.
- Individuals for whom the reporting person works or with whom he/she has any other type of relationship in an employment context or in which he/she has a significant shareholding.

In addition to the safeguards described under section 4 of the Policy, during the investigation process the person affected by a report would be entitled to be heard, to have his/her honor respected and to benefit from the presumption of innocence.

In addition, the following safeguards should be noted:

- The following data must not be collected and, if so, must be immediately deleted:
- Personal data that are not manifestly relevant to the processing of a specific Report.
  - Any personal data that may have been communicated and which relate to a conduct that does not fall within the scope of the Spanish Whistleblower Act.
  - Special categories of personal data.
  - Any Report that is proven to be untrue, unless the lack of truthfulness may constitute a criminal offense. In case a criminal offense is identified, the information should be stored until the corresponding judicial proceeding terminates.
- Reports that have not been followed up (i.e., that have not been investigated) and that are intended to be retained must be anonymized.

The Local Reporting Channel(s) will include adequate technical and organizational measures to preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information provided, especially the identity of the Reporting person, in case he/she has been identified. In particular, the identity of the Reporting person may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, or disciplinary investigation but CLdN Spain will inform the Reporting person in advance, unless this jeopardizes investigation or legal proceedings or contravenes applicable regulations.

5. EXTERNAL REPORTING CHANNELS

CLdN Spain strongly encourages reports to be made internally through any of the reporting channels available so that any concerns can be resolved appropriately and quickly. However, should the Reporting person decide to report their concerns externally in compliance with applicable provisions, they can report to the Independent Authority for the Protection of Informants or the corresponding independent authorities for the protection of informants created at regional level.

6. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Personal data processed within the Local Reporting Channel(s) will be kept only for the time necessary to decide on the appropriateness of initiating an investigation into the facts reported. In any case, according to Article 32 §4 of the Spanish Whistleblower Act, they will be deleted or duly anonymized after three (3) months have elapsed from the receipt of the Report without any investigation having been initiated, unless the purpose of the storage is to leave evidence of the operation of the Local Reporting Channel(s).
The personal data relating to internal investigations arising from Reports will be retained for the period that is necessary and proportionate for the purposes of complying with the Spanish Whistleblower Act and, in no case may they be retained for a period exceeding ten (10) years pursuant to Article 26 §2 of the Spanish Whistleblower Act, unless it is necessary to keep the data for a longer period of time to preserve the CLdN Spain's defence right.

C. PRIVACY RIGHTS

Data subjects will be able to exercise their data protection rights in accordance with section 4.B of the Policy. However, where a data subject to whom the facts described in a Report or public disclosure exercises his/her right to object, and in the absence of proof to the contrary, it will be presumed that there are compelling legitimate grounds for processing. Also, such data subjects may not exercise their right to access in order to identify the Reporting person.

7. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Please note that if a Report is not received through the reporting channels mentioned in this Policy but through other unofficial channels (e.g. a direct supervisor or other managers), the employee receiving such Report must immediately communicate the same to the Local Reporting System Manager within a maximum period of 48 hours, immediately deleting the Report received. The person who has received the Report must keep the Report strictly confidential. Failure to comply with these reporting and confidentiality obligations may lead to disciplinary action.

Country-specific addendum:

Germany

This Country-specific Addendum for Germany (the "German Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Germany:

- **CLdN Cargo Deutschland GmbH** with registered office at Christophstrasse 10, 54290 Trier, Germany - Handelsregister B des Amtsgerichts Wittlich HRB 42193, VAT DE 813807304

hereafter referred as "CLdN Germany", in accordance with the provisions of the Law on the Protection of Whistleblowers ("the German Whistleblower Act"), which implements the EU Whistleblower Directive.

This German Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to and supplementing the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Germany's local reporting channel(s):

- violations that are subject to criminal liability (in German: "Verstöße, die strafbewehrt sind")
- violations which are subject to administrative fines (in German: "Verstöße, die bußgeldbewehrt sind") provided the violated regulation serves to protect life, limb or health or to protect the rights of employees or their representative bodies
- other violations of federal and state legislation and directly applicable legal acts of the EU and EAEC that concern the following areas:
- the areas listed under section 3.B of the Policy
- Renewable energy
- infringements covered by Sec. 4d of the Financial Services Supervision Act (in German: "Finanzdienstleistungsaufsichtsgesetz")
- tax violations
- statements made by federal civil servants that constitute a breach of the duty of loyalty to the Constitution

2. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN Cargo Deutschland GmbH	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

3. SAFEGUARDS

The safeguards described under section 4 of the Policy apply to Germany as well including the prohibition of retaliation. In this context we note that the German Whistleblower Act foresees a legal presumption that an act or omission was retaliatory if it occurred after a report was made and if the Reporting Person invokes this presumption.

4. EXTERNAL REPORTING CHANNELS

CLdN Germany strongly encourages reports to be made internally so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, they can report to the relevant German competent authorities, i.e.:

- Federal Office of Justice
- Federal Financial Supervisory Authority
- Federal Cartel (Antitrust) Office
- additional external reporting channels may be established under the German Whistleblower Act, in which case the German Addendum will be modified accordingly in due course.

The way to make external reports can be found on the websites of the relevant competent authorities.

5. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Documentation of reports shall be deleted three (3) years after the conclusion of the procedure, unless it is necessary and proportionate to retain the documentation for longer than three (3) years in order to comply with the requirements under the German Whistleblower Protection Act or other legal provisions.

6. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Country-specific addendum:

Malta

his Country-specific Addendum for Malta (the "Maltese Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Malta:

- **CLdN Malta Ltd**, a limited liability company having its registered address at Europa Centre, Office 8/9, John Lopez Street, Floriana FRN 1400, Malta and bearing company registration number C67976;

hereafter referred as "CLdN Malta", in accordance with the provisions of the Protection of the Whistleblower Act, Chapter 527 of the Laws of Malta ("the Maltese Whistleblower Act"), which implements the EU Whistleblower Directive.

This Maltese Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. PERSONAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the scope described in section 3.A of the Policy, this Policy also applies to persons who have undertaken personally to execute any work or service for, and under the immediate direction and control of another person, including outworkers but excluding work or service performed in a professional capacity to which an obligation of professional secrecy applies when such work or service is not regulated by a specific contract of service, and persons who are or were under secondment.

2. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Malta's local reporting channel(s):

- Health and safety of individuals
- Corrupt practices
- Criminal offences
- Miscarriages of justice
- Bribery
- Breaches relating to any legal obligation in general

3. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN Malta Ltd	Lisanne Den Hollander (Lisanne.denhollander@cldn.com) and Joost Rubens (joost.rubens@cldn.com)

4. INVESTIGATIONS AND SHARING RESOURCES

For the Subsidiaries with less than 250 employees, Employees and Third Parties are informed that the Subsidiary may share Group resources as regards the receipt of reports and any investigation that shall be carried out. In doing so, the Malta Group subsidiaries' will ensure that confidentiality is maintained, and remain obliged to provide feedback to the Reporting Person and to address the Report.

5. SAFEGUARDS

In addition to the safeguards described under section 4 of the Policy, the prohibition of disclosure of information that identifies or may lead to the identification of the Reporting Person is not subject to any exceptions, and no court may order the disclosure of the identity of a Reporting Person without their consent.

If the Reporting Person is the perpetrator or an accomplice in the reported Breach, and such reported Breach constitutes a criminal offence or contravention in accordance with Maltese law, criminal proceedings may still be instituted against the Reporting Person, although the punishment may be mitigated.

Knowingly providing false information by means of a report shall be an offence punishable in accordance with Article 101 of the Criminal Code, Chapter 9 of the Laws of Malta.

6. EXTERNAL REPORTING CHANNELS

CLdN Malta strongly encourages reports to be made internally so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, they can report to the relevant Maltese competent authorities, i.e.:

- The Auditor General - Failure to observe laws, rules and regulations relating to public finance and misuse of public resources
- Commissioner for Revenue - Income tax, corporate tax, capital gains tax, stamp duties, national insurance contributions, value added tax or "revenue acts" as defined in the Commissioner for Revenue Act
- Commissioner for Voluntary Organisations - Activities of a voluntary organisation
- Financial Intelligence Analysis Unit - Money Laundering or financing of terrorism in terms of the Prevention of Money Laundering Act
- Malta Financial Services Authority - The business of credit and financial institutions, the business of insurance and the activities of insurance intermediaries, the provision of investment services and collective investment schemes, pensions and retirement funds, regulated markets, central securities depositors, the carrying out of trustee business either in a professional or a personal capacity and such other areas of activity or services as may be placed from time to time under the supervisory and regulatory competence of the Malta Financial Services Authority
- Ombudsman - Conduct involving substantial risk to public health or safety or the environment that would if proved, constitute a criminal offence and all matters which constitute improper practices and which are not designated to be reported to any other authority
- Permanent Commission Against Corruption – Corrupt practices

The way to make external reports can be found on the websites of the relevant competent authorities.

7. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

Reports shall be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by the Maltese Whistleblower Act or other requirements imposed by law. This means that in principle Reports will be stored for five (5) years after the end of the Reporter's contractual relationship with the Subsidiary concerned or two (2) years in case no such contractual relationship exists. Longer retention time may apply if further processing is necessary for the establishment, exercise or defence of legal claims. Any personal data which is manifestly not relevant for the handling of a specific Report shall not be collected, or if accidentally collected, shall be deleted without undue delay.

8. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Country-specific addendum:

Ireland

This Country-specific Addendum for Ireland (the "Irish Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Ireland:

- **CLdN RoRo S.A. Dublin** with registered office at Port Centre, Alexandra Road – Dublin 1, Company Number 906298, VAT IE9752002D

hereafter referred as "CLdN Ireland", in accordance with the provisions of the Protected Disclosures Act 2014 as amended by the Protected Disclosures (Amendment) Act 2022 ("the Irish Whistleblower Act"), which implements the EU Whistleblower Directive.

This Irish Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. PERSONAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the scope described in section 3.A of the Policy, this Irish Addendum applies to all Employees and Third Parties whether permanent, temporary, full-time, part-time or fixed-term basis and includes ex-employees and agency staff.

2. MATERIAL SCOPE OF LOCAL REPORTING CHANNEL(S)

In addition to the In-scope areas listed under section 3.B of the Policy, Breaches in the following areas may also be reported through CLdN Ireland's local reporting channel(s):

- criminal offences that have been, are being or are likely to be committed;
- a failure or likely failure to comply with any legal obligation, other than one arsing under a contract of employment or a contract to provide services personally;
- a miscarriage of justice that has occurred, is occurring or is likely to occur;
- the actual or likely endangerment of the health or safety of any individual;
- damage or likely damage to the environment;
- an unlawful or otherwise improper use (or likely improper use) of funds or resources of a public body or other public money;
- an act or omission by or on behalf of a public body that is oppressive, discriminatory or grossly negligent or which constitutes gross mismanagement; and
- information tending to show that any of the Breaches has been, is being or is likely to be concealed or destroyed or that an attempt has been, is being or is likely to be made to conceal or destroy such information.

The Irish Addendum does not cover Reports relating to a Reporting Person's own personal circumstances, grievances, complaints or employment relationship. Such concerns will generally fall outside the scope of this Irish Addendum and it may be more appropriate to raise such matters under a different CLdN Ireland policy or procedure. For example, a complaint of bullying/harassment against the individual only would not fall within the scope of this Irish Addendum and would in the normal course be dealt with under the [CLdN Ireland Bullying and Harassment Policy].

3. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

CLdN RoRo S.A. Dublin	C.Legal (info@clegal.be) and Joost Rubens (joost.rubens@cldn.com)

4. INVESTIGATIONS AND SHARING RESOURCES

The Subsidiaries of CLdN Ireland with less than 250 employees may utilise the resources of the Group to receive and investigate any Reports. The individual Subsidiaries will retain responsibility to maintain confidentiality, follow up on and provide feedback on, the Reports.

If a Reporting Person makes a Report that falls within the scope of this Irish Addendum, the Report will be acknowledged within seven (7) days of the Report being made. If a Reporting Person requests a physical meeting, this will be set up within a reasonable timeframe.

If the Reporting Person's identity is known, they will be provided with feedback within three (3) months of acknowledgment of the receipt of the Report. Furthermore, if requested in writing, the Reporting Person will be provided with further feedback at intervals of 3 (three) months until such time as the procedure relating to the Report is closed.

Fair procedures requires that any individual accused of any Breach will be made aware of, and have the opportunity to respond to, the information reported.

5. SAFEGUARDS

In addition to the safeguards described under section 4 of the Policy, please note the following:

A. NON-RETALIATION

A Reporting Person who discloses information will be protected from any form of retaliation where the Reporting Person reasonably believes that information tends to show one (1) or more Breaches and the information came to the attention of the Reporting Person in a work-related context.

For the purposes of the Irish Addendum, examples of "retaliation" also include, but are not limited to:

- injury, damage or loss,
- failure to convert a temporary employment contract into a permanent one, where the worker had a legitimate expectation that he or she would be offered permanent employment,
- failure to renew or early termination of a temporary employment contract,
- harm, including to the worker'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
- psychiatric or medical referrals.

B. CONFIDENTIALITY

CLdN Ireland will not, without the explicit consent of the Reporting Person, disclose their identity or any information from which their identity may be directly or indirectly deduced, to another person, other than those (including members of staff designated under legislation) whom CLdN Ireland reasonably considers may be necessary for the purposes of the receipt or transmission of, or follow-up on, reports as required under legislation.

The prohibition on disclosure will not apply where:

a) the disclosure is a necessary and proportionate legal obligation in the context of investigations or judicial proceedings;
b) the person to whom the Report was made or transmitted:
    a. shows that they took all reasonable steps to avoid disclosing the identity or any information from which it could be deduced, or
    b. reasonably believes that disclosing the identity or any such information is necessary for the prevention of serious risk to the security of the State, public health, public safety or the environment;
c) the disclosure is otherwise required by law.

Where the identity of the Reporting Person or any other information from which the identity may be directly or indirectly deduced is disclosed to another person, the Reporting Person will be notified in writing in advance, together with the reasons for the disclosure unless this would jeopardise:

a) the effective investigation of the Breach(es);
b) the prevention of serious risk to the security of the State, public health, public safety or the environment; or
c) the prevention of crime or the prosecution of a criminal offence.

6. EXTERNAL REPORTING CHANNELS

CLdN Ireland strongly encourages Reports to be made internally so that any concerns can be resolved. However, should the Reporting Person decide to report their concerns externally in compliance with applicable provisions, they can report certain Breaches externally to "prescribed persons" who are set out in the Protected Disclosures Act 2014 (Disclosure to Prescribed Persons) Order 2020 (SI 367/2020), available here.

The Reporting Person may also make a Report to the Office of the Protected Disclosures Commissioner or, where relevant, to institutions, bodies offices or agencies of the European Union.

7. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

CLdN Ireland will keep a record of all Reports made in accordance with this Irish Addendum. Records will be retained for no longer than is necessary and proportionate for CLdN Ireland to comply with its legal obligations. As a guideline, subject to the circumstances, records of Reports will be retained for a period of up to six (6) years.

8. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

Country-specific addendum:

Guernsey

This Country-specific Addendum for Guernsey (the "Guernsey Addendum") describes the specific requirements that apply to the local reporting channel(s) implemented by the following Group local Subsidiary(ies) in Guernsey:

- **Seaway Manning Services (Guernsey) Limited** with registered office at PO Box 112,First Floor St Martins House, Le Bordage ,St Peter ,Port Guernsey, GY1 1BR, Company Number 44577;
- **Vessel Manning Services (Guernsey) Limited** with registered office at PO Box 112,First Floor St Martins House, Le Bordage ,St Peter ,Port Guernsey, GY1 1BR, Company Number 58617;

hereafter referred as "CLdN Guernsey".

This Guernsey Addendum supplements the Group Whistleblowing Policy (the "Policy") and prevails over the Policy in the event of a discrepancy.

1. LOCAL REPORT MANAGER

The impartial person or department who is competent to receive and follow up on the Reports, which will maintain communication with the Reporting Person and, where necessary, ask for further information from and provide feedback to that Reporting Person is:

Seaway Manning Services (Guernsey) Limited	Alexis Donaghey (ado@seatruckgroup.co.uk) and Joost Rubens (joost.rubens@cldn.com)
Vessel Manning Services (Guernsey) Limited	Alexis Donaghey (ado@seatruckgroup.co.uk) and Joost Rubens (joost.rubens@cldn.com)

2. EXTERNAL REPORTING CHANNELS

CLdN Guernsey strongly encourages reports to be made internally so that any concerns can be resolved. However, in certain circumstances it may be appropriate for the Reporting Person to report their concerns externally in compliance with applicable procedures.

For example, it may be appropriate for the Reporting Person to report their concerns to an external body such as a regulator or a law enforcement agency, including under the following circumstances:

- A report should be made in accordance with the provisions of the Disclosure (Bailiwick of Guernsey) Law 2007, as read with the relevant provisions of the Terrorism and Crime (Bailiwick of Guernsey) Law 2002, if the Reporting Person knows, suspects or has reasonable grounds for knowing or suspecting that any business is engaged in terrorist financing and / or is engaged in money laundering or that certain property is the proceeds of criminal conduct. A failure to make the required disclosure may amount a criminal offence in certain circumstances.
- A Reporting Person may contact the Office of the Data Protection Authority ('ODPA') in Guernsey in confidence if they are concerned that CLDN Guernsey has not complied with their legal data protection obligations in relation to personal data. The contact details for the ODPA are available here: https://www.odpa.gg/for-individuals/protecting-whistleblowers/.

It will rarely if ever be appropriate to alert the media. We strongly recommend that the Reporting Person takes advice before reporting a concern to anyone external.

3. PERSONAL DATA PROCESSING

A. DATA CONTROLLER

The data controller of the personal data processed within the Local Internal Channel and during any internal investigation of the matter reported is the Subsidiary (amongst the list above in this Addendum) which is acting as the employer of, or with which a professional relationship exists with, the Reporter.

B. RETENTION PERIODS

The appropriate retention period will vary depending on the person making the Report, the nature of the Report and any legal, investigatory or regulatory context. Reports by Employees will typically be retained for the duration of the employment relationship and seven (7) years after its termination.

4. LOCAL CONTACTS

For any questions regarding the internal reporting channels or where you need support, you may consult and/or seek advice from the following contact: Whistleblower@cldn.com

CLdN Links SA
3-7, rue Schiller
2519 Luxembourg
Luxembourg
Phone: +352 26 44 66 1