SCAN GLOBAL LOGISTICS

WHISTLEBLOWER POLICY FOR SCAN GLOBAL LOGISTICS

Version 4.0

OBJECTIVE

The objective of this Whistleblower Policy is to set the framework for the whistleblower system of Scan Global Logistics ("SGL"), which, in addition to SGL's usual reporting channels, can be used to raise any serious concerns, including any suspicion or knowledge of illegal, unethical or irregular conduct.

WHO CAN RAISE CONCERNS?

The whistleblower system of SGL can be used by the employees of SGL. The system can also be used by the directors, customers, suppliers and other business associates of SGL.

HOW ARE CONCERNS RAISED?

Concerns are raised by accessing the whistleblower system on the website SGL. The whistleblower system will inform and guide the whistleblower about matters of importance to the assessment of the concern raised.

WHAT CONCERNS CAN BE RAISED?

You can use the whistleblower system to raise all serious concerns which fall within the scope of the current regulation regarding the protection of whistleblowers. It could be suspicion or knowledge of any illegal, unethical or irregular conduct, including matters regarding bribery and corruption, abuse of funds, theft, deceit, embezzlement, fraud and other white-collar crime as well as any personal data security violation, severe environmental damage, conflicts of interest, sexual harassment or other gross harassment as well as other gross or repeated breaches of law or SGL's internal policies, including SGL's Code of Conduct.

We will assess in each case whether the concern is within the scope of the whistleblower system. The concern will be within the scope of the whistleblower system if it is within the scope of the current regulation regarding the protection of whistleblowers.

If you are an employee, we note that dissatisfaction with your employment such as salary and management style and other contractual terms and conditions are not to be reported to the whistleblower system. Instead, such matters are to be addressed through the usual channels to your line manager or HR.

Concerns must be raised in good faith. In particular, it means that the system may not be used to raise any concerns containing information that the whistleblower knows is wrong.

HANDLING CONCERNS RAISED

The law firm Poul Schmith will screen every concern raised through the whistleblower system.

The whistleblower will receive confirmation of the receipt of the concern as soon as possible and no later than 7 days.

During the screening, the law firm Poul Schmith will perform an assessment of the concern. After the assessment of the concern, Poul Schmith will deliver the concern to the Global VP, People, Leadership & Culture and the Global General Counsel at SGL. The concern will hereafter be the subject of an investigation. The extent of the investigation will depend on the specific circumstances of the concern. The further investigation will, as a starting point, be carried out by SGL's whistleblower entity.

If the initial screening shows that the concern is outside the scope of SGL's system, it will not be processed further in the system, and the whistleblower will be informed accordingly.

The whistleblower will receive feedback on the status of the concern within 3 months, including the type of follow-up that has been made, if any.

FROM OBSERVATION TO CLOSED CASE - WHISTLEBLOWER FLOW

1. Observation of a Concern: An employee observes or becomes aware of an activity or behaviour within SGL, our suppliers or with our agents that they believe is illegal, unethical, or against our policies or virtues. This could include witnessing fraud, corruption, safety violations, harassment, discrimination, or other misconduct.

2. Understanding Whistleblower Policies: The employee familiarises themselves with SGL's Whistleblower Policy and related procedures. These documents outline the process for reporting concerns confidentially and without fear of retaliation.

3. Choosing Reporting Channel: The employee selects the appropriate reporting channel. This might involve reporting directly to a Supervisor, Manager, People & Culture, Compliance Officer, Global General Counsel etc.

4. Submitting a Report: If voicing the concern as mentioned in number 3 is insufficient, the employee submits a detailed report outlining the concern, providing relevant evidence or documentation if available. You may also include any witnesses or individuals involved in the situation. You choose whether you want to be anonymous when reporting a concern or not. The whistleblower will receive confirmation of receipt of the concern as soon as possible, and no later than 7 days. Please be aware of following up on your report in the system. You will not receive notifications.

5. Investigation: Once a report is submitted, it will be viewed by a third-party company (the law firm, Poul Schmith) and assessed. After the assessment, the Global General Counsel and Global VP of People, Leadership & Culture will be involved and initiate an investigation into the concern. This may include interviewing relevant

parties, gathering evidence, reviewing documents, and assessing the claim's validity. The whistleblower will receive feedback on the status of the concern within 3 months. Please be aware of following up on your report in the system. You will not receive notifications.

6. Protection of Whistleblower: Throughout the investigation process, SGL ensures the confidentiality and protection of the whistleblower. This may include safeguarding their identity, providing support, and prohibiting retaliation against the whistleblower.

7. Resolution and Action: Based on the investigation findings, SGL takes appropriate action to address the concern. This could involve disciplinary action against individuals involved in misconduct, implementing corrective measures to prevent future occurrences, or making changes to procedures.

8. Closing the Case: The case is officially closed once the concern has been addressed satisfactorily. SGL communicates the resolution to the whistleblower, ensuring transparency and providing any necessary updates or follow-up actions.

9. Monitoring and Follow-Up: SGL may continue to monitor the situation to ensure compliance with corrective measures and to prevent the recurrence of similar issues. We may also conduct follow-up checks with the whistleblower to ensure there is no retaliation or further concerns.

10. Evaluation and Improvement: Periodically, SGL reviews its Whistleblower Policy and related procedures to evaluate our effectiveness and make improvements as necessary. This may involve soliciting feedback from employees and stakeholders to enhance the reporting process and ensure a supportive environment for whistleblowers.

ANONYMITY AND PROTECTION OF THE WHISTLEBLOWER

The whistleblower can decide whether to raise the concern anonymously or give their personal contact details.

If the whistleblower decides to raise the concern anonymously, neither SGL nor a third party will process the whistleblower's personal data. If, when raising the concern, the whistleblower provides data that makes SGL able to identify the whistleblower, SGL will, however, be entitled to process such data. This is the case even if the whistleblower has raised the concern anonymously.

If the whistleblower raises the concern anonymously, the whistleblower will have the option to decide whether they want to be available for any further investigation by setting up a secure and anonymous mailbox through which SGL can contact the whistleblower. We recommend that the whistleblower sets up a mailbox as it can be difficult for SGL to conduct an investigation without any further information from the

whistleblower.

If the whistleblower decides to reveal their identity when raising a concern, which falls within the scope of the system, SGL's whistleblower entity shall preserve the confidentiality of the whistleblower's identity in accordance with the applicable rules regarding protection of whistleblowers. Thus, the whistleblower's identity will only, in principle, be disclosed if the whistleblower explicitly consents to this. The whistleblower's identity can, however, also be disclosed to public authorities, such as the police or public prosecutor, if deemed necessary to respond to reported matters or for the purpose of ensuring the right to defence for the affected people.

A whistleblower, who reports serious matters which fall within the scope of the whistleblower system, may not face retaliation of any kind as a result of the concern raised. A whistleblower is protected against reprisals, including threats of reprisals or attempts reprisals. This means that it cannot have employment-related consequences to make a report in good faith.

The reporting system does not log the IP address or the machine ID of the computer on which the concern is raised, and the system does not use any cookies. If the computer on which the concern is raised is owned by SGL or connected to the network of SGL , there is a risk that the IP address and/or the machine ID of the computer from which the concern is raised will be logged in the browser history and/or the log of SGL through the log that is made in the IT systems of SGL . The whistleblower can eliminate this risk by raising the concern from a computer that is not owned by SGL or connected to the network of SGL.

REPORTING TO EXTERNAL REPORTING CHANNELS

The whistleblower may also raise a concern through an external reporting channel – i.e. a whistleblower system established by a public authority. Thus, the Danish Data Protection Agency has, for example, established an external reporting channel, which supplements employers' duty to establish a whistleblower system. Raising a concern through an external reporting channel is not conditioned by a preceding report to SGL's whistleblower system. However, we encourage you to raise your concern through SGL's whistleblower system so that SGL will be able to quickly and immediately follow up on the matter concerned.

CONTACT DETAILS

Questions about this policy may be addressed to Scan Global Logistics'

Global VP, People, Leadership and Culture via e-mail bidam@scangl.com; or

Global General Counsel via e-mail hchr@scangl.com