# Whistleblower Policy

CONCERNING

Copenhagen Infrastructure Service Company ApS ("CISC") outside of Denmark

**List of content**

## 1. Introduction and purpose

1.1 This Whistleblower Policy describes the purpose of introducing a Whistleblower Arrangement (hereinafter the "Arrangement"), how it works, who can make use of the Arrangement, and what may be reported through the Arrangement.

1.2 This Whistleblower Policy covers any subsidiary or affiliate of Copenhagen Infrastructure Service Company ApS outside of Denmark (hereinafter referred to as "**CISC**"). **Reference is made to Appendix 1 to this Whistleblower Policy.**

1.3 **The Arrangement is subject to local law in the country of which the affected company is located. In case of any discrepancies between this Whistleblower Policy and local law, *local law shall apply*. Consequently, the following sections of this Whistleblower Policy shall apply, unless otherwise regulated in local law.**

1.4 The purpose of the Arrangement is to ensure that a Whistleblower, as defined in this Whistleblower Policy, can swiftly and confidentially, through a special, independent and autonomous channel, report violations or potential violations within the scope of this Arrangement, allowing an independent and autonomous whistleblower unit to assess which steps are required in this respect.

## 2. Who can use the Arrangement?

2.1 The Arrangement can be used by persons who report information on violations the person in question has gained access to in connection with his or her work-related activities, and who belong to the following categories of persons (hereinafter referred to as "Whistleblower"):

a) Employees
b) Self-employed persons
c) Members of the executive board, board of directors
d) Volunteers
e) Paid or unpaid trainees
f) Persons working under the supervision and management of contracting parties, subcontractors, and suppliers
g) Persons who are reporting or publishing information to which they have gained access in a work-related relationship that has ceased since then
h) Persons in work-related relationships that have not yet commenced, who report information on violations they have gained access to during the course of the recruitment process or other pre-contractual negotiations

2.2 Persons listed under section 9.4 can also file reports under the Arrangement.

2.3 Persons not included in the categories of persons stated in sections 2 or 9.4 cannot file reports under the Arrangement but have to report through ordinary communication channels.

## 3. What may be reported through the Arrangement?

3.1 The Arrangement covers reports regarding serious offences or other serious matters (see section 3.4 i)) as well as reports regarding violations (see section 3.4 ii)).

3.2 "Violations" means acts or omissions that

i) are illegal or constitute a serious offence or other serious matters comprised by section 3.4; or
ii) allow circumventions of the purpose of the rules under section 3.4.

3.3 Any information may be reported, including reasonable suspicion about actual or potential violations or serious matters comprised by section 3.4, which have

occurred or most probably will occur at the affected company, as well as any attempts to cover up such violations.

3.4 The report must concern violations or potential violations, defined as acts or omissions which:

i) are serious offences or other serious matters, like for instance:

- Violation of any duty of confidentiality
- Abuse of financial means
- Theft
- Deceit
- Embezzlement
- Fraud
- Bribery
- Violation of industrial safety rules
- Any form of sexual harassment
- Severe harassment, e.g. bullying, violence, and harassment due to race, political or religious affiliation

ii) are illegal, including for instance:

- Public procurement
- Money-laundering
- Protection of privacy and personal data
- Security of network and information systems.

3.5 The Arrangement may only be used for reporting violations or potential violations in relation to the issues described in section 3.4 that have occurred or most probably will occur in the affected company, committed for instance by employees, executive board, or members of the Board of Directors of the company in question. In connection with reports on incidents committed by the company in question, please note that such incidents may be reported although the incident cannot be attributed to an individual person but may be due to a basic systemic failure at the company in question.

3.6 Offences that are not comprised by the Arrangement must be reported through ordinary communication channels.

## 4. Contents of the report

4.1 To facilitate further investigation of the reported issue, and to be able to identify the offence, it is important that the Whistleblower describes the offence in the best possible way. It is thus not possible to make any further investigations of a report if the report is not specified or if it only contains very general allegations without any further clarification.

4.2 Therefore, it is important that the Whistleblower - to the utmost extent - provides the following information:

- a description of the matter;
- the person(s) involved;
- whether others are aware of the suspicion about the matter;
- whether the executive board knows about the matter;
- whether documents exist that support the matter;
- whether and where further information may be found about the matter;
- for how long the matter has gone on; and
- whether the Whistleblower knows about any attempts to hide the offence.

4.3 Manifestly unfounded reports will not be investigated further.

## 5. How can a report be submitted and who is to receive the report?

5.1 A whistleblower unit has been appointed, and the whistleblower unit

a) will receive the reports and be in contact with the Whistleblower;
b) will follow-up on the reports; and
c) give feedback to the Whistleblower.

5.2 The whistleblower unit in charge of the tasks mentioned in section 5.1 consists partly of two lawyers from Plesner Law Firm (hereinafter "Plesner"), and partly of an impartial group of persons at the company in question.

5.3 Written reports are submitted through the following website:

www.cisc.dk/whistleblower/

5.4 Written reports are received by two lawyers at Plesner. Plesner will make a legal capacity assessment of the persons of the whistleblower unit who are able to process the report, after which the report will be forwarded to the relevant persons (hereinafter referred to as "Case Managers") in the whistleblower unit.

5.5 It is only possible to submit written reports under the Arrangement.

5.6 The whistleblower unit will treat all written reports as confidential.

5.7 The Case Managers appointed to receive and follow up on the reports are subject to a duty of confidentiality regarding the information contained in the reports.

## 6. Anonymity

6.1 The Whistleblower is encouraged to state his or her name when submitting a report so that the Case Managers are able to ask clarifying questions and subsequently provide feedback on the further course of the investigation. However, anonymous communication between Plesner and a Whistleblower who chooses to be anonymous is possible (see sections 6.4 and 6.5).

6.2 If the Whistleblower chooses to submit an anonymous report, it is recommended - to ensure full anonymity - that the Whistleblower uses a private PC or, for instance, a PC located at a public library.

6.3 Plesner will make a communication module available, allowing the Whistleblower to communicate with Plesner for the purpose of providing additional information about the reported matter, which Plesner will then pass on to the Case Managers.

6.4 The Whistleblower can provide additional information to Plesner through the communication module and remain anonymous. In connection with the reporting, a one-off code is generated which, in order to safeguard the anonymity, cannot be re-created. Therefore, it is **important** that the Whistleblower keeps the code and remembers to log on the communication module to communicate with the whistleblower unit.

6.5 The communication module can be accessed through the above-mentioned link under the Arrangement (see section 5.3) to log on the communication module. If the Whistleblower chooses to be anonymous, it is important that the Whistleblower regularly enters the communication module to check whether Plesner has asked any questions. If the Whistleblower is anonymous, Plesner is not able to come into contact with the Whistleblower in any other ways, for instance to inform the Whistleblower that additional questions etc. have been submitted.

## 7. Information to the whistleblower

7.1 The Whistleblower will receive:

- an acknowledgement of receipt of the report within three days of that receipt; and
- feedback soonest possible and in principle within three months from the acknowledgement of receipt of the report.

7.2 "Feedback" means a notification about the measures taken by the company in question to assess the correctness of the allegations made in the report and, where relevant, to counter the reported offence. The feedback provided by the whistleblower unit must, at any time, observe the rules under local data protection law, which may entail limitations in relation to the contents of the feedback to the Whistleblower.

7.3 Depending on the circumstances, an extension of the timeframe for the feedback may be required, where necessary due to the specific circumstances of the case, in particular the nature and complexity of the report, which may require a lengthy investigation. If this is the case, the Whistleblower must be notified in this respect.

## 8. Information to and protection of the reported person

8.1 After a preliminary investigation has taken place and all relevant evidence has been secured, the person concerned, i.e., the person reported under the Arrangement, will among other things be informed about:

- the identity of the Case Manager(s) responsible for the investigation of the report; and
- the issues of the report.

8.2 The person concerned is entitled to protection of his or her identity during the case management and has a right to effective defence.

8.3 The reported person may have the right of access to information about the Whistleblower's identity where necessary for the reported person to exercise his or her right to an effective defence.

## 9. Protection of the whistleblower

9.1 The Whistleblower is protected against retaliation when submitting a report through the Arrangement, if the following conditions are fulfilled:

- The person submitting the report meets the conditions to be considered a Whistleblower (see section 2).
- The Whistleblower had reasonable grounds to believe that the reported information was correct at the time of reporting and that the reported information falls under the scope the Arrangement (see section 3.4).

9.2 "Retaliation" means unfavourable treatment or unfavourable consequences as a reaction to a report. This may be suspension, dismissal, demotion, or equivalent measures.

9.3 If the Whistleblower submits a report in bad faith and is fully aware of the fact that the reported information is not correct, the Whistleblower is not protected against retaliation.

9.4 In addition to the group of persons mentioned in section 2, the protection described in this section 9 also applies to the following persons or entities:

1) Intermediaries, is a natural person who confidentially assists a whistleblower with the reporting process in a work-related context (for example, a representative of the whistleblower)

2) Third parties who are connected to the Whistleblower and who risk being subject to retaliation in a work-related context (e.g. a colleague).

3) Undertakings and authorities which the Whistleblower owns or works for or is otherwise connected with in a work-related context (e.g. an undertaking owned by the Whistleblower).

9.5 If the Whistleblower has deliberately revealed his or her identity in connection with a publication of the reported matter, the special considerations regarding the protection of the Whistleblower's identity are not applicable.

## 10. Data security and data storage

10.1 All reports under the Arrangement will be registered. The registration is subject to local data protection law.

10.2 All information reported through the Arrangement, including information on persons reported through the Arrangement, will be processed in accordance with applicable law.

10.3 All reports will be stored properly, and it will only be possible for relevant persons of the whistleblower unit to access the information.

10.4 A report falling outside the scope of the Arrangement will be closed in the Arrangement and - if relevant and with the Whistleblower's prior consent - forwarded to another relevant department.

10.5 In principle, reports will be deleted from the Arrangement 45 days after finalizing the processing, unless - and subject to local law - there is a legitimate reason to store the report for longer.

10.6 If the matter is reported to the police or another authority, the report will be closed in the Arrangement immediately after the case has been closed by the authorities in question.

10.7 If – on basis of the collected data – a disciplinary sanction is implemented against the reported person, or if there are other grounds justifying and requiring the continued storage of the data on the person concerned, such data will be stored, where an employee is involved, in the employee's personnel file.

10.8 Otherwise, the information is stored in accordance with the affected company's deletion policy.

## 11. Questions

11.1 If you have any questions regarding this Whistleblower Policy contact CISCs Compliance function at cisc@cisc.dk

## 12. Approval

12.1 This Whistleblower Policy was approved by the Board of Directors on December 13, 2023.

## 13. Approval history

| Version: | Effective from: | Changes: | Performed by: |
|---|---|---|---|
| 1 | December 13, 2023 | Initiation | Board of Directors |

**APPENDIX 1**

- CISC AUS PTY LTD (Australia)
- CISC GK (Japan)
- CISC GmbH (Germany)
- CISC Korea Ltd (Korea)
- CISC London Limited (United Kingdom)
- Copenhagen Infrastructure Partners Inc. (United States)
- Copenhagen Infrastructure Partners Luxembourg S.a.r.l. (Luxembourg)
- Copenhagen Infrastructure Partners Singapore PTE. Ltd (Singapore)
- Copenhagen Infrastructure Partners Spain S.L.U. (Spain)