PRIVACY POLICY FOR WHISTLEBLOWER ARRANGEMENT

This Privacy Policy explains how subsidiaries of Copenhagen Infrastructure Partners P/S and Copenhagen Infrastructure Partners II P/S located outside Denmark hereinafter referred to as "**CIP"**, "**we**" or "**us**") processes personal information in connection with reports to CIP's Whistleblower Arrangement.

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

Below is a description of the personal data processing that takes place and the rights you have if you are reported through the Whistleblower Arrangement, as well as your rights if you use the Whistleblower Arrangement to report another person.

Reference is also made to CIP's Whistleblower Policy, containing information about who can submit reports and who can be reported.

This policy only concerns the handling and the investigation of reports submitted through the Whistleblower Arrangement. Therefore, this policy must - in relation to employees - be seen in connection with CIP's other relevant policies and procedures.

1 DATA CONTROLLER

The legal entity responsible for the processing of your personal information is the company to which your report relates. Reference is made to Appendix 1 to this Privacy Policy containing a list of the companies comprised by this Privacy Policy.

2 DESCRIPTION OF THE PROCESSING

The following is a description of how CIP will process information on the person who is reported about (the "**Reported Person**") as well as the person who is submitting the report (the "**Whistleblower**") in connection with reports to CIP's Whistleblower Arrangement.

Purpose	**Categories of Personal Data**	**Legal Basis for the Processing**	**Recipients**	**Data Retention**
#1 Handling and investigation of reports under CIP's Whistleblower Arrangement regarding: • The Reported Person **Sources** We can collect information from the following sources: • Plesner Law Firm • Employees of CIP • Self-employed persons • Members of the executive board, board of directors, or similar governing body in the undertaking • Volunteers • Paid and/or unpaid trainees/interns • Persons working under the supervision and management of contracting parties, suppliers, and sub-suppliers • Persons who are reporting information to which they have gained access in a work-related relationship that has ceased since then. • Persons in work-related relationships that have not yet commenced, who report information on violations to which they have gained access during the course of the recruitment process or other pre-contractual negotiations.	We can process the following personal data categories about you: Ordinary personal data: • Name, email, telephone number, • Other information included in the report. Sensitive information, including information on sexual matters, may be included in the processing. Information on criminal offences or possible criminal offences may also be included in the processing.	CIP processes your personal data subject to and in compliance with local law.	We can share your personal information with: • Plesner Law Firm • CIP group companies • IT suppliers • External advisors • The police • Public authorities.	We will retain personal data for as long as it is necessary for the purposes listed. • The data are retained for as long as the investigation is in progress. The retention period depends on the outcome of the investigation. • Reports submitted to the Arrangement are in principle deleted after 45 days, unless CIP has legitimate reasons for continued retention. • Reports falling outside the scope of the Arrangement, but not appearing to be unfounded, may - with your prior written consent - be passed on to CIP's HR Legal Team where they will be processed in accordance with CIP's relevant policies and procedures. • Reports turning out to be unfounded will be immediately closed in the Arrangement and deleted within 45 days after having been deemed to be unfounded. • If a report is conveyed to the police or another public authority, the data will be retained for at least as long as the investigation is in progress at the police/public authority. • Otherwise, the data will be retained in accordance with CIP's deletion policy.

Purpose	Categories of Personal Data	Legal Basis for the Processing	Recipients	Data Retention
#2 Handling and investigation of reports under CIP's Whistleblower Arrangement regarding: • The Whistleblower If there is suspicion of the report being deliberately false, this purpose also comprises investigation of the Whistleblower. **Sources** We can collect information from the following sources: • Plesner Law Firm • You	We can process the following categories of personal data about you, provided that your report is not anonymous: <u>Ordinary personal data</u>: • Name, email, telephone number, • The contents of your report. As a rule, no sensitive information about you will be processed as part of the handling of the report - unless you choose to provide such information yourself. However, information on criminal offences or possible criminal offences may be included in the processing if there is a suspicion that the submitted report is deliberately false.	CIP processes your personal data subject to and in compliance with local law.	We can share your personal information with: • Plesner Law Firm • CIP group companies • IT suppliers • External advisors • The police • Public authorities.	We will retain personal data for as long as it is necessary for the purposes listed. • The data are retained for as long as the investigation is in progress. The retention period depends on the outcome of the investigation. • Reports submitted to the Arrangement are in principle deleted after 45 days, unless CIP has legitimate reasons for continued retention. • Reports falling outside the scope of the Arrangement, but not appearing to be unfounded, may - with your prior written consent - be passed on to CIP's HR Legal Team where they will be processed in accordance with CIP's relevant policies and procedures. • Reports turning out to be unfounded will be immediately closed in the Arrangement and deleted within 45 days after having been deemed to be unfounded. • If a report is conveyed to the police or another public authority, the data will be retained for at least as long as the investigation is in progress at the police/public authority. • Otherwise, the data will be stored in accordance with CIP's deletion policy.

3 INFORMATION TO THE REPORTED PERSON AND RECTIFICATION

If you are subject to a report submitted through the Whistleblower Arrangement, you will be notified as soon as possible after an initial investigation has taken place and all relevant evidence is secured. In this connection, you will receive information about:

- The identity of the person(s) who is/are responsible for the investigation of the report
- A description of the contents of the report

As mentioned below in the section about your general rights, you have a right of access to the report that was submitted about you. However, your right to access to the report might be limited in accordance with local law.

You also have the right to request rectification of the information in the report if you believe this to be false, misleading, or incomplete. If your request in this respect cannot be met, the information will be supplemented with your comments.

4 CONSEQUENCES OF THE PROCESSING

Reports and investigation of reports to the Whistleblower Arrangement may have significant consequences for the person who is reported, as reports concern violations or suspected violations of the law, as further outlined in the separate guidelines for the Arrangement.

Likewise, a report to the Whistleblower Arrangement may have significant consequences for the person who has submitted the report in case of a deliberately false report. Such cases may have criminal consequences.

5 TRANSFERS TO COUNTRIES OUTSIDE THE EU/EEA

We transfer personal data to the following types of recipients, located in countries outside the EU/EEA:

Transfers of personal data to a third country or an international organisation
Category of recipient: Microsoft, incl. Microsoft's sub-processors in various countries Country: USA
Category of recipient: Placement Agents, accountants, legal advisors, other relevant advisors and cooperating partners Country: Countries where CIP or funds that CIP is appointed manager for are active, including USA, Canada, Japan, South Korea, Australia, New Zealand, Israel, Taiwan, Chile, Mexico, Singapore, India, Thailand, Brazil, the Philippines and Vietnam.
Category of recipient: IT Service Providers, providers of online communication, file storage platforms Country: Countries where CIP or funds that CIP is appointed manager for are active, including USA, Canada, Japan, South Korea, Australia, New Zealand, Israel, Taiwan, Chile, Mexico, Singapore, India, Thailand, Brazil, the Philippines and Vietnam.

We may transfer your personal data to countries outside EU/EEA, where the European Commission has decided that the country offers an adequate level of data protection, pursuant to article 45 of the GDPR ("**Adequacy Decision**")

When transferring your personal data to insecure third countries outside the EU/EEA without an adequacy decision, the legal basis for transferring is the European Commission's Standard Contractual Clauses in order to ensure an adequate level of protection for the personal data equivalent to the level ensured in the EU.

We note that the US and other third countries usually do not ensure a level of protection essentially equivalent to that ensured within the EU/EEA. Therefore, you must be aware that the third countries may not provide for effective legal remedies to exercise your rights and may allow unjustifiable access to personal data by public authorities.

6 YOUR GENERAL RIGHTS

You have the following rights:

- You have the right to request access to and rectification or deletion of your personal data.
- You also have the right to object to the processing of your personal data and have the processing of your personal data restricted.
- You have the right to receive the personal information provided by yourself in a structured, commonly used and machine-readable format (data portability).
- You may always lodge a complaint with a data protection supervisory authority, e.g. The Danish Data Protection Agency.

There may be conditions or limitations on these rights, e.g., you may not be entitled to deletion of your personal data in a specific case – this depends on the specific circumstances of the processing activities.

You can make use of your rights by contacting

Copenhagen Infrastructure Partners P/S	Copenhagen Infrastructure Partners II P/S
CVR.no.: 37 99 40 06	CVR.no.: 35 68 27 75
Amerika Plads 29, 2.	Amerika Plads 29, 2.
2100 Copenhagen Ø	2100 Copenhagen Ø
Email: cip@cip.com	Email: cip@cip.com

7 IT POLICY

For employees of CIP, reference is made to CIP's IT Policy containing information on CIP's IT and email policy.

8 QUESTIONS

If you have any questions regarding this policy, please feel free to contact CIP's Compliance Function at compliance@cip.com

Last updated: 29 November 2023

APPENDIX 1 - LIST OF DATA CONTROLLERS

New York:
Copenhagen Infrastructure Partners Inc.
412 W 15th Street, 15th Floor
New York, NY 10011
United States
Email: cip@cip.com

Tokyo:
CIP GK
5F Prime Terrace Kamiyacho, 4-1-13
Toranomon
Minato City 105-0001, Tokyo
JAPAN
Email: cip@cip.com

Utrecht:
Copenhagen Infrastructure Partners
Stadsplateau 7
3521 AZ Utrecht
The Netherlands
Email: cip@cip.com

Hamburg:
CIP P/S German Branch
Kaiser-Wilhelm-Straße 14
20355 Hamburg
Germany
Email: cip@cip.com

Melbourne:
CIP AUS PTY LTD
Level 34/477 Collins Street
Melbourne, Victoria 3000
Australia
Email: cip@cip.com

Singapore:
Copenhagen Infrastructure Partners Singapore Pte Ltd
1 Wallich Street #15-02 Guoco Tower
Singapore 078881
Singapore
Email: cip@cip.com

London:
CIP London Ltd
61 Curzon Street
W1J 8PD London
Great Britain
Email: cip@cip.com

Munich:
CIP Munich
Maximilian Strasse 13,
80539 Munich,
Germany
Email: cip@cip.com

Luxembourg:
CIP Luxembourg S.a r.l.
53 Boulevard Royal
L-2449 Luxembourg
Luxembourg
Email: cip@cip.com

Seoul:
CIP Korea Ltd.
16th F, Tower A, Centropolis 26
Ujeongguk-ro, Jongno-gu
Seoul
Korea
Email: cip@cip.com

Madrid:
Copenhagen Infrastructure Partners Spain S.L.U.
Paseo de la Castellana, 40 bis, Floor 2
28046 Madrid
Spain
Email: cip@cip.com