

Whistleblower Hotline: EU Privacy Notice

The Canada Pension Plan Investments Board and its affiliates (**CPPIB**) relies on the trust of all our stakeholders to fulfill our important public mandate. Our Code of Conduct and Guiding Principles of integrity, partnership and high performance provide the ethical framework for our practices. We also believe it is important for our stakeholders to have the ability to report ethical or other issues, or breaches of laws related to CPPIB. This helps us further safeguard our stakeholders' confidence and protect our world-class reputation and opportunities. The ClearView Connects™ whistleblower hotline (the **Hotline**) is a tool stakeholders can use to report on ethical issues related to CPPIB. It complements the confidential counsel provided by CPPIB's Conduct Review Advisor who is also available to our stakeholders. (See our Code of Conduct for additional information.)

The whistleblower hotline provides an additional independent, secure and anonymous reporting tool, with benefits including:

- (i) anytime confidential access available online, by phone or by mail, globally and in several languages; and
- (ii) a transparent access point for employees, external partners and other stakeholders.

This Privacy Notice explains how CPPIB collects, uses and discloses personal data in connection with the Hotline in the European Union (**EU**). Personal data means any information relating to an identified or identifiable individual.

In order to comply with certain requirements of EU and other applicable data protection law, CPPIB has established this Privacy Notice and specific procedural rules for the implementation of the Hotline.

Identification of Reporting Employees

Whenever possible, you should provide your name and contact information when reporting concerns and allegations via the Hotline. This information may help us to better investigate the issue and enables us to contact you if further information is needed. If you identify yourself, your identity will be kept confidential, subject to applicable law and our need to investigate and remediate the issue. CPPIB's affiliates may disclose the reporting employee's identity as required by law, such as in response to a court or administrative order or equivalent legal requirement or to relevant persons involved in conducting an investigation or any subsequent adjudication.

No Retaliation

CPPIB won't permit, and will take actions necessary within CPPIB, to prevent retaliation against anyone who:

- seeks help, or
- has reported a breach or suspected breach in good faith.

Personal Data We Process

CPPIB processes personal data from employees through the Hotline to the extent necessary to pursue our legitimate interests in preparing a report, conducting an investigation and responding to the concern. When you submit a report to the Hotline, you will be given a report number that you may use to check the status of the report. In connection with a report, we may collect and process personal data, including the identity, position, location and contact information of:

- the individual submitting the report;
- the individual who is the subject of the report;
- other individuals with information relating to the report; and
- the individuals responsible for investigating the report.

In addition, personal data may be included in:

- the facts that are reported to the Hotline;
- follow-up questions that you may be asked to clarify;
- evidence gathered in the course of the investigation;
- any reports generated as part of the investigation; and
- any response taken by CPPIB's affiliates as a result of the report.

The Hotline is not intended to collect or process sensitive personal data (i.e., information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation) or criminal convictions and offences. To the extent such data is intrinsic to the facts that have been reported through the Hotline, we will seek to minimize any resulting collection and further processing of such data.

How We Will Handle Reports

CPPIB's third-party Hotline service provider will receive reports made through the Hotline. We require our service providers by contract to process personal data only on our behalf and to maintain the security and confidentiality of your personal data. The service provider's system will generate a report based on the concern raised. Depending on the nature and seriousness of the alleged facts, reports may be forwarded for review to specially trained CPPIB personnel in Canada such as representatives from the Legal Department, Human Resources Department, Finance Reporting & Analytics Department, Technology & Data Department or other relevant

departments. We may use external advisors in reviewing a reported concern or allegation of misconduct.

Data Transfers

We are part of a global organization. To the extent permitted by applicable law, your personal data may be transferred to, stored or accessed by CPPIB personnel located in Canada or elsewhere for the purpose of managing the Hotline and investigating an allegation. In addition, our third-party Hotline service provider is located in Canada. CPPIB and our third-party Hotline service provider are subject to and comply with the provisions of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), pursuant to article 45 of the GDPR. When your personal data is transferred to (or accessed from) a country outside the EU for which the European Commission has not issued an adequacy decision, we will ensure that appropriate safeguards are implemented to protect your personal data in accordance with applicable law. This may include (intra-group) data transfer agreements incorporating the European Commission's Standard Contractual Clauses, pursuant to article 46 of the GDPR, a copy of which you can obtain by contacting us as indicated below.

Security and Retention

We make reasonable efforts to ensure a level of security appropriate to the risk of the data processing and have implemented technical and organizational measures to protect your personal data. We will endeavor to destroy or anonymize (i.e., all personal identifiers will be removed) personal data contained in a Hotline report within a reasonable amount of time after the conclusion of the relevant investigation, unless the investigation leads to disciplinary or legal proceedings, in which case we may need to retain your personal data until the conclusion of those proceedings and the period permitted under applicable law.

Your Rights

Subject to applicable law, you may have the right to request access to and receive details about the personal data we maintain about you in connection with a report made through the Hotline. You also may have the right to request that certain personal data about you be rectified, erased or restricted, in accordance with applicable law. You also may have the right to object at any time, on legitimate grounds, to the processing of your personal data in the context of a report to the Hotline. We will respond to your questions or complaints relating to the processing of your personal data. If you are not satisfied with our responses, you may consult the data protection authority of your country. The exercise of your rights may be restricted as necessary to protect others in the context of a particular allegation.

How to Contact Us

If you have any questions or comments about the Hotline, or if you would like to exercise your rights of access, correction, erasure, restriction or objection to the processing of your personal data, please contact privacy@cppib.com.