Penalties for non-compliance

Administrative financial penalties

The Commission may impose administrative financial penalties on companies that fail to comply with certain obligations of the *Act Respecting the Protection of Personal Information in the Private Sector*. These penalties can be up to 2% of global sales or $10 million.

An administrative financial penalty may be imposed on any person who:

- Collects, uses, discloses, retains or destroys personal information in violation of the Act
- Fails to properly inform the persons concerned about the collection of their personal information
- Fails to report a privacy incident that poses a risk of serious harm to the Commission or the persons concerned
- Fails to take appropriate security measures to ensure the protection of personal information
- Fails to inform the persons concerned about:
- Decisions based exclusively on automated processing (without human intervention)
- Their right to make representations to a staff member of the organization who can review the decision
- Fails to meet their personal information agent obligations.

OLLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Following a breach of the Act, a person can pledge to the Commission that they will take the necessary measures to remedy or mitigate the consequences of the breach. The Commission may also specify conditions or the obligation to pay a certain amount of money. If the Commission approves the measures pledged and the person follows through, there can be no administrative financial penalty imposed for acts or omissions found by the Commission.

As set out in the Act, the Commission has developed and published a general framework for administrative financial penalties, including:

- The purpose of the penalties

- The criteria for deciding whether to impose a penalty when a breach is found and the amount of the penalty
- The circumstances under which criminal proceedings are more appropriate
- Other terms and conditions relating to the imposition of penalties

Refer to the document.

Criminal proceedings

Companies that violate certain obligations under the Act are subject to a fine.

Violations of the *Act Respecting the Protection of Personal Information in the Private Sector* are subject to a fine of:

- If committed by a natural person: $5,000 to $100,000
- If committed by an organization: $15,000 to $25,000,000 or, if greater, an amount corresponding to 4% of worldwide turnover for the preceding fiscal year

These fines can be imposed on anyone who:

- Collects, uses, discloses, retains or destroys personal information in violation of the Act
- Fails to report, when required to do so, a privacy incident to the Commission or to the persons concerned
- Violates the prohibitions relating to a credit file security freeze
- Fails to take appropriate security measures to ensure the protection of personal information
- Identifies or attempts to identify an individual based on de-identified information without the consent of the person holding the information or based on anonymized information
- Fails to meet their obligations as personal information agent
- Obstructs an investigation, inspection or request by the Commission by providing the latter with false or inaccurate information, or by failing to provide the Commission with information requested by it, or otherwise
- Retaliates against a person on the ground that the person has, in good faith, filed a complaint with the Commission or cooperated in an investigation, or threatens a person with retaliation so that he or she will refrain from pursuing the matter

CSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

- Refuses or fails to comply with a formal request within the time limit determined by the Commission
- Contravenes an order issued by the Commission

Factors for determining punitive action

In the event of guilt, a judge must consider the following factors in determining the amount of the fine:

- Nature, severity, repetitiveness and duration of the offence
- Sensitivity of the personal information concerned
- Intentional, negligent or reckless nature of the offence
- Predictability of the offence or failure to act on recommendations or warnings to prevent it
- Attempts by the offender to conceal the offence or their failure to attempt to mitigate the consequences
- The fact that the offender failed to take reasonable steps to prevent the offence from happening
- The fact that the offender, by committing the offence or failing to take measures to prevent it, increased their revenues or reduced expenditures or intended to do so
- The number of persons affected by the offence and the risk of harm to them

In the event of a repeat offence, the Act provides for fines to be doubled.

Time limit to initiate proceedings

For both public bodies and companies, the Commission has five years from the time the offence is committed to initiate criminal proceedings.

September 19, 2023

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE