Annex 1

Procedure to follow to comply with legal requirements

in sections 63.8 to 63.11 of the Access Act3

The following steps can be carried out simultaneously.

1. **Assess the situation**. A company that has reason to believe that a confidentiality incident involving personal information it holds has occurred must, in particular:

- Establish the circumstances of the incident.
- Identify the personal information involved.
- Identify the people concerned.
- Find the problem, be it an error, a vulnerability, etc.

This evaluation must continue until all elements have been identified.

2. **Reduce risks**. The company must quickly take the necessary reasonable measures to reduce the risks of harm, whether serious or not, being caused and to prevent new incidents of the same nature from occurring, for example:

- Cease the unauthorized practice.
- Recover or require the destruction of the personal information involved.
- Correct IT deficiencies.

3. **Identify the nature of the harm**. The objective is to determine whether it is necessary to notify the CAI (Commission for Access to Information) and the persons concerned as well as to establish the measures to be put in place to reduce the risks, in particular:

- Enter a note in the files affected by a risk of identity theft.
- Impose additional vérifications if required.

Assessment of harm

During a confidentiality incident, **PCP Aluminium** must assess whether there is a risk that harm will be caused to a person whose personal information is concerned. He must then consider several factors, including:

- The sensitivity of personal information such as financial information or identity information.
- The anticipated consequences of the use of this information such as:
    - Identity theft.
    - Financial fraud.
    - A significant invasion of privacy.
- The likelihood that this information could be used for harmful purposes.

Serious harm corresponds to an act or event likely to harm the person concerned or their property and harm their interests in a significant way. It can lead, for example:

- To humiliation.
- Damage to reputation.
- To a financial loss.
- Identity theft.
- Has negative consequences on a credit file.
- Job loss.

4. **Enter the incident in the register**, whether the risk of harm is classified as serious.

5. **If there is a risk of serious harm**. The public body must:

- Notify the CAI as soon as possible, even if he has not collected all the information relating to the incident and complete the declaration subsequently. He can thus notify the CAI of the incident and, later, confirm the number of people concerned.
- Notify any person whose personal information is affected by the incident unless this notice is likely to hinder an investigation. A delay may apply between the time the company becomes aware of the incident and the time it notifies the people concerned.

  This delay may be necessary in order, for example, to identify the personal information involved, the people concerned, the security breach and to close it or to avoid hindering an ongoing investigation.

These notices are mandatory.

6**. If there is a risk of serious harm**: **PCP Aluminium** may also notify any person or organization likely to reduce this risk. To this end, he can only communicate the personal information that is necessary to pursue this objective.

Obtaining the consent of the person concerned by the information transmitted is not required.

However, the person responsible for the protection of personal information must record the communication to keep documentary traces of it such as:

- To whom this information is communicated.
- In which circumstances.
- What information was transmitted.
- What are the objectives of this approach.