Privacy incident management policy and procedure

(Section 3.2 Act respecting the protection of personal information in the private sector, chapter P-39.1 and Regulation respecting confidentiality incidents; Act respecting the Barreau du Québec, chapitre B-1 and regulations in force)

PREAMBLE

The law firm is responsible for protecting the personal information it holds. Personal information is confidential except as provided by law. Any person who, in the course of their duties, has access to personal information held by the law firm must take the necessary means to ensure its protection and confidentiality. This procedure determines the measures to be taken to reduce the risks of harm being caused, in such a case, and to prevent new incidents of the same nature from occurring.

1. OBJECTIVE AND NORMATIVE FRAMEWORK

This procedure specifies the steps to be taken when the law firm has reasonable grounds to believe that a confidentiality incident has occurred, involving personal information that it holds, or if such an incident is proven, and this, in accordance with the Act respecting the protection of personal information in the private sector (chapter P-39.1 and the Regulation respecting confidentiality incidents).

2. DEFINITIONS

The definitions to be considered for the application of this procedure, which may be supplemented by any other regulation, policy, directive, or procedure referring to it, are as follows:

Here are some examples:

- A staff member consults personal information not necessary for the performance of their duties;
- A hacker infiltrates a system;
- A person uses personal information from a database to which he has access in the course of his duties with the aim of usurping the identity of a person;
- A communication is made by mistake to the wrong person;
- A person loses or has documents containing personal information stolen;
- A person interferes with a database containing personal information in order to alter it.

Personal information: any information concerning a person that allows them to be identified. A person's name, taken in isolation, does not constitute personal information. However, when this name is associated or combined with other information relating to the same person, it then becomes personal information.

Examples of personal information include:

- A person's name and date of birth;
- Social Security number ;
- Credit Card Number ;
- Medicare card number ;
- Information of a medical or financial nature;
- A person's name and personal telephone number;
- A person's name and home address.

Sensitive personal information: personal information is considered sensitive when, by its nature, in particular medical, biometric or otherwise intimate, or because of the context of its use or communication, it gives rise to a high degree of reasonable expectation in terms of respect for private life.

This may include, for example, medical, biometric, genetic or financial information, or information on ethnic origin, political belief, sexual life or orientation, religious beliefs.

3. PROTECTION OF PERSONAL INFORMATION

The law firm implements appropriate and reasonable security measures to protect personal information against loss or theft, and against access, disclosure, copying, use or modification not authorized by law. Only staff members who absolutely must have access to personal information as part of their duties are authorized to access it.

Persons who are members of the staff of the law firm or who work on its behalf must, in particular:

- Make reasonable efforts to minimize the risk of unintentional disclosure of personal information;

- Take special precautions to ensure that personal information is not monitored, heard, consulted or lost when working in premises other than the offices of the law firm;

  and

- Take reasonable steps to protect personal information when moving from one location to another.

4. REPORTING A CONFIDENTIALITY INCIDENT

Any person to whom the law firm communicates personal information (colleagues, suppliers, partners, experts including subcontractors) must make a report when they have reasonable grounds to believe that a confidentiality incident involving a personal information held by the law firm. To do this, this report must be made without delay to the person responsible for the protection of personal information.

The member of the board of directors of the law firm or a staff member who has reasonable grounds to believe that a confidentiality incident involving personal information held by the law firm has occurred must also notify his hierarchical superior or the person responsible for the protection of personal information without delay.

5. RESPONSIBLE FOR PERSONAL INFORMATION (PRP): ROLES AND RESPONSIBILITIES

The person responsible for the protection of personal information (hereinafter “PRP”) for the firm is the president, Me Marie-Joëlle Demers. She can be reached at the following contact details:

- Email: mjdemers@solutionavocat.com
- Telephone: 514-658-6111

Its role is in particular to:

- Contribute to the implementation of the information security incident management process;

- Maintain the register of information security incidents that may have jeopardized information security, document these incidents and keep the director of information security informed as well as the general secretary;

- Contribute to information security risk analyzes in order to identify threats and vulnerable situations and implement appropriate solutions.

In the event of a confidentiality incident, the person responsible for the protection of personal information takes charge of handling the incident and partners with any other useful person depending on the nature of the incident.

As such, the PRP:

- Assesses the risk of harm being caused and determines the degree of severity. During this assessment, the sensitivity of the information concerned, the anticipated consequences of its use and the probability that it will be used for harmful purposes are considered.

- Notifies, with diligence, the person whose personal information is concerned by the incident, when it presents a risk that serious harm will be caused, except when this would be likely to hinder an investigation carried out by a person or by a body which, under the law, is responsible for preventing, detecting or repressing crime or breaches of laws. This notice must contain the following information:

a. A description of the personal information affected by the incident or, if this information is not known, the reason justifying the impossibility of providing such a description;
b. A brief description of the circumstances of the incident;
c. The date or period when the incident took place or, if the latter is not known, an approximation of this period;
d. A brief description of the measures that the organization has taken or intends to take following the occurrence of the incident, in order to reduce the risk of harm being caused;
e. The measures that the organization suggests that the person concerned take in order to reduce the risk of harm being caused to them or in order to mitigate such harm;
f. Contact details allowing the person concerned to find out more about the incident.

- Notify, where applicable, any person or organization likely to reduce the risk, by communicating only the personal information necessary for this purpose, without the consent of the person concerned.

- Notify, diligently and in writing, the Commission for Access to Information of the confidentiality incident when it presents a risk of serious harm being caused. The notice must contain the following information:

a. The name of the firm and the Quebec business number assigned to it under the Act respecting the legal publicity of businesses;

b. The name and contact details of the person to contact within the firm regarding the incident;

c. A description of the personal information affected by the incident or, if this information is not known, the reason justifying the impossibility of providing such a description;

d. A brief description of the circumstances of the incident and, if known, its cause;

e. The date or period when the incident took place or, if the latter is not known, an approximation of this period;

f. The date or period during which the law firm became aware of the incident;

g. The number of people affected by the incident and, among these, the number of people who reside in Quebec or, if they are not known, an approximation of these numbers;

h. A description of the elements which lead the law firm to conclude that there is a risk of serious harm being caused to the persons concerned, such as the sensitivity of the personal information concerned, the possible malicious uses of this information, the anticipated consequences of their use and the likelihood that they will be used for harmful purposes;

i. The measures that the law firm has taken or intends to take to notify people whose personal information is affected by the incident, as well as the date the people were notified or the expected execution time;

j. The measures that the law firm has taken or intends to take following the occurrence of the incident, in particular those aimed at reducing the risks of harm being caused or at mitigating such harm and those aimed at preventing further incidents of the same nature occur, as well as the time frame during which the measures were taken or the expected time frame for execution;

k. Where applicable, a statement specifying that a person or organization located outside Quebec and exercising responsibilities similar to those of the Information's Commission access with regard to monitoring the protection of information personnel was notified of the incident.

- Diligently notifies the insurers of the law firm, if applicable.

- Record the confidentiality incident in the register provided for this purpose.

- At the request of the Commission for Access to Information, send a copy of this register.

6. REGISTER OF CONFIDENTIALITY INCIDENTS

The law firm must keep a register of confidentiality incidents.

1. Duration of retention of information contained in the register

   The information contained in the register must be kept up to date and retained for the longer of the two following periods: for a minimum period of five years after the date on which the law firm became aware of the incident or the required period by the Quebec Bar for the conservation of files.

7. ENTRY INTO FORCE

This procedure comes into force on September 25, 2023.

Signed in Montréal, this September 25, 2023.

Me Marie-Joëlle Demers
President of the law firm Solution Avocat, Criminalistes Inc.