**p-39.1**

***Act respecting the protection of personal information in the private sector***

**PROFESSOR MENDELSOHN NOTES:**

* Highlighted clauses or portions of clauses were added / modified by Bill 64 aka Law 25 in 2021
* Green highlighted clauses were added / modified by Bill 64 aka Law 25 in 2021 and are especially important in relation to the internet and / or technology generally
* (…) indicates there are missing sections you are not responsible for, though you are smart law students you could have figured it out yourselves by the missing numbers! But I’m nice and helpful.

**DIVISION I**

**APPLICATION AND INTERPRETATION**

**1**. The object of this Act is to establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code.

The Act applies to such information, whether the enterprise keeps the information itself or through the agency of a third person, whatever the nature of its medium and whatever the form in which it is accessible, whether written, graphic, taped, filmed, computerized, or other.

This Act also applies to personal information held by a professional order to the extent provided for by the Professional Code (chapter C-26) and to that held by a political party, an independent Member or an independent candidate to the extent provided for by the Election Act (chapter E-3.3).

This Act does not apply to journalistic, historical or genealogical material collected, held, used or communicated for the legitimate information of the public.

Divisions II and III of this Act do not apply to personal information which by law is public. Nor do they apply to personal information concerning the performance of duties within an enterprise by the person concerned, such as the person’s name, title and duties, as well as the address, email address and telephone number of the person’s place of work.

**1.1**. For the purposes of this Act, any person who collects personal information relating to another person for a serious and legitimate reason is deemed to be establishing a file within the meaning of the Civil Code and the rights concerning such a file conferred by articles 35 to 40 of that Code apply to the personal information collected.

**2.** Personal information is any information which relates to a natural person and directly or indirectly allows that person to be identified.

**3.** This Act does not apply

(1) to a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A‐2.1);

(2) to information held on behalf of a public body by a person other than a public body.

**DIVISION I.1**

**RESPONSIBILITIES RELATING TO PROTECTION OF PERSONAL INFORMATION**

**3.1**. Any person carrying on an enterprise is responsible for protecting the personal information held by the person.

Within the enterprise, the person exercising the highest authority shall see to ensuring that this Act is implemented and complied with. That person shall exercise the function of person in charge of the protection of personal information; he may delegate all or part of that function in writing to any person.

The title and contact information of the person in charge of the protection of personal information must be published on the enterprise’s website or, if the enterprise does not have a website, be made available by any other appropriate means.

**3.2**. Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information. Such policies and practices must, in particular, provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information. The policies and practices must also be proportionate to the nature and scope of the enterprise’s activities and be approved by the person in charge of the protection of personal information.

Detailed information about those policies and practices, in particular as concerns the content required under the first paragraph, must be published in simple and clear language on the enterprise’s website or, if the enterprise does not have a website, made available by any other appropriate means.

**3.3**. Any person carrying on an enterprise must conduct a privacy impact assessment for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of personal information.

For the purposes of such an assessment, the person must consult the person in charge of the protection of personal information within the enterprise from the outset of the project.

The person must also ensure that the project allows computerized personal information collected from the person concerned to be communicated to him in a structured, commonly used technological format.

The conduct of a privacy impact assessment under this Act must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

**3.4**. The person in charge of the protection of personal information may, at any stage of a project referred to in section 3.3, suggest personal information protection measures applicable to the project, such as

(1) the appointment of a person to be responsible for implementing the personal information protection measures;

(2) measures to protect the personal information in any document relating to the project;

(3) a description of the project participants’ responsibilities with regard to the protection of personal information; or

(4) training activities for project participants on the protection of personal information.

**3.5**. Any person carrying on an enterprise who has cause to believe that a confidentiality incident involving personal information the person holds has occurred must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature.

If the incident presents a risk of serious injury, the person carrying on an enterprise must promptly notify the Commission d’accès à l’information established by section 103 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1). He must also notify any person whose personal information is concerned by the incident, failing which the Commission may order him to do so. He may also notify any person or body that could reduce the risk, by communicating to the person or body only the personal information necessary for that purpose without the consent of the person concerned. In the latter case, the person in charge of the protection of personal information must record the communication of the information.

Despite the second paragraph, a person whose personal information is concerned by the incident need not be notified so long as doing so could hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences.

A government regulation may determine the content and terms of the notices provided for in this section.

**3.6**. For the purposes of this Act, “confidentiality incident” means

(1) access not authorized by law to personal information;

(2) use not authorized by law of personal information;

(3) communication not authorized by law of personal information; or

(4) loss of personal information or any other breach of the protection of such information.

**3.7**. In assessing the risk of injury to a person whose personal information is concerned by a confidentiality incident, a person carrying on an enterprise must consider, in particular, the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes. The person must also consult the person in charge of the protection of personal information within the enterprise.

**3.8**. A person carrying on an enterprise must keep a register of confidentiality incidents. A government regulation may determine the content of the register.

**DIVISION II**

**COLLECTION OF PERSONAL INFORMATION**

**4**. Any person carrying on an enterprise who, for a serious and legitimate reason, collects personal information on another person must determine the purposes for collecting the information before doing so.

**4.1**. The personal information concerning a minor under 14 years of age may not be collected from him without the consent of the person having parental authority or of the tutor, unless collecting the information is clearly for the minor’s benefit.

**5**. Any person collecting personal information on another person may collect only the information necessary for the purposes determined before collecting it.

Such information must be collected by lawful means.

**6.** Any person collecting personal information relating to another person may collect such information only from the person concerned, unless the latter consents to collection from third persons.

However, he may, without the consent of the person concerned, collect such information from a third person if the law so authorizes.

He may also do so if he has a serious and legitimate reason and either of the following conditions is fulfilled:

(1) the information is collected in the interest of the person concerned and cannot be collected from him in due time;

(2) collection from a third person is necessary to ensure the accuracy of the information.

**7**. Any person collecting personal information from another person carrying on an enterprise must, at the request of the person concerned, inform the latter of the source of the information.

This section does not apply to a file established for the purposes of an inquiry to prevent, detect or repress a crime or statutory offence.

**8**. Any person who collects personal information from the person concerned must, when the information is collected and subsequently on request, inform that person

(1) of the purposes for which the information is collected;

(2) of the means by which the information is collected;

(3) of the rights of access and rectification provided by law; and

(4) of the person’s right to withdraw consent to the communication or use of the information collected.

If applicable, the person concerned is informed of the name of the third person for whom the information is being collected, the name of the third persons or categories of third persons to whom it is necessary to communicate the information for the purposes referred to in subparagraph 1 of the first paragraph, and the possibility that the information could be communicated outside Québec.

On request, the person concerned is also informed of the personal information collected from him, the categories of persons who have access to the information within the enterprise, the duration of the period of time the information will be kept, and the contact information of the person in charge of the protection of personal information.

The information must be provided to the person concerned in clear and simple language, regardless of the means used to collect the personal information.

**8.1**. In addition to the information that must be provided in accordance with section 8, any person who collects personal information from the person concerned using technology that includes functions allowing the person concerned to be identified, located or profiled must first inform the person

(1) of the use of such technology; and

(2) of the means available to activate the functions that allow a person to be identified, located or profiled.

“Profiling” means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour.

**8.2**. Any person who collects personal information through technological means must publish on the enterprise’s website, if applicable, a confidentiality policy drafted in clear and simple language and disseminate it by any appropriate means to reach the persons concerned. The person must do the same for the notice required for any amendment to such a policy.

**8.3**. Any person who provides his personal information in accordance with section 8 consents to its use and its communication for the purposes referred to in subparagraph 1 of the first paragraph of that section.

(…)

**9**. No person may refuse to respond to a request for goods or services or to a request relating to employment by reason of the applicant’s refusal to disclose personal information except where

(1) collection of that information is necessary for the conclusion or performance of a contract;

(2) collection of that information is authorized by law; or

(3) there are reasonable grounds to believe that the request is not lawful.

In case of doubt, personal information is deemed to be non-necessary.

**9.1**. Any person carrying on an enterprise who collects personal information when offering to the public a technological product or service having privacy settings must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the person concerned.

The first paragraph does not apply to privacy settings for browser cookies.

**DIVISION III**

**CONFIDENTIALITY OF PERSONAL INFORMATION**

*§ 1. — Retention, use and non-communication of information*

**10**. A person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

**11**. Every person carrying on an enterprise must ensure that any personal information held on another person is up to date and accurate when used to make a decision in relation to the person concerned.

The information used to make such a decision is kept for at least one year following the decision.

**12**. Unless the person concerned gives his consent, personal information may not be used within the enterprise except for the purposes for which it was collected. Such consent must be given expressly when it concerns sensitive personal information.

Personal information may, however, be used for another purpose without the consent of the person concerned, but only

(1) if it is used for purposes consistent with the purposes for which it was collected;

(2) if it is clearly used for the benefit of the person concerned;

(3) if its use is necessary for the purpose of preventing and detecting fraud or of assessing and improving protection and security measures;

(4) if its use is necessary for the purpose of providing or delivering a product or providing a service requested by the person concerned; or

(5) if its use is necessary for study or research purposes or for the production of statistics and if the information is de-identified.

In order for a purpose to be consistent within the meaning of subparagraph 1 of the second paragraph, it must have a direct and relevant connection with the purposes for which the information was collected. However, commercial or philanthropic prospection may not be considered a consistent purpose.

For the purposes of this Act, personal information is

(1) de-identified if it no longer allows the person concerned to be directly identified;

(2) sensitive if, due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, it entails a high level of reasonable expectation of privacy.

Every person carrying on an enterprise who uses de-identified information must take reasonable measures to limit the risk of someone identifying a natural person using de-identified information.

**12.1**. Any person carrying on an enterprise who uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly not later than at the time it informs the person of the decision.

He must also inform the person concerned, at the latter’s request,

(1) of the personal information used to render the decision;

(2) of the reasons and the principal factors and parameters that led to the decision; and

(3) of the right of the person concerned to have the personal information used to render the decision corrected.

The person concerned must be given the opportunity to submit observations to a member of the personnel of the enterprise who is in a position to review the decision.

**13**. No person may communicate to a third person the personal information he holds on another person, unless the person concerned consents to, or this Act provides for, such communication.

Such consent must be given expressly when it concerns sensitive personal information.

**14**. Consent under this Act must be clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language. If the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.

The consent of a minor under 14 years of age is given by the person having parental authority or by the tutor. The consent of a minor 14 years of age or over is given by the minor, by the person having parental authority or by the tutor.

Consent is valid only for the time necessary to achieve the purposes for which it was requested.

Consent not given in accordance with this Act is without effect.

**15**. Consent to the communication of personal information by a third person may be given by the person concerned to the person who collects the information from the third person.

**16.** Any person holding personal information on behalf of a person carrying on an enterprise may refer to the latter every request for access or rectification received from a person to whom such information relates.

Nothing in this section limits a person’s right to obtain, from a personal information agent, access to, or rectification of, personal information concerning him held by that agent.

**17**. Before communicating personal information outside Québec, a person carrying on an enterprise must conduct a privacy impact assessment. The person must, in particular, take into account

(1) the sensitivity of the information;

(2) the purposes for which it is to be used;

(3) the protection measures, including those that are contractual, that would apply to it; and

(4) the legal framework applicable in the State in which the information would be communicated, including the personal information protection principles applicable in that State.

The information may be communicated if the assessment establishes that it would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information. The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.

The same applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on his behalf.

This section does not apply to a communication of information under subparagraph 7 of the first paragraph of section 18.

(…)

**18.3**. A person carrying on an enterprise may, without the consent of the person concerned, communicate personal information to any person or body if the information is necessary for carrying out a mandate or performing a contract of enterprise or for services entrusted to that person or body by the person carrying on an enterprise.

In such a case, the person carrying on an enterprise must

(1) entrust the mandate or contract in writing; and

(2) specify in the mandate or contract the measures the mandatary or the person performing the contract must take to protect the confidentiality of the personal information communicated, to ensure that the information is used only for carrying out the mandate or performing the contract and to ensure that the mandatary or person does not keep the information after the expiry of the mandate or contract. A person or body carrying out a mandate or performing a contract of enterprise or for services referred to in the first paragraph must notify the person in charge of the protection of personal information without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated, and must also allow the person in charge of the protection of personal information to conduct any verification relating to confidentiality requirements.

Subparagraph 2 of the second paragraph does not apply if the mandatary or the person performing the contract is a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1) or a member of a professional order.

(…)

**23**. Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy the information, or anonymize it to use it for serious and legitimate purposes, subject to any preservation period provided for by an Act.

For the purposes of this Act, information concerning a natural person is anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly.

Information anonymized under this Act must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation.

(…)

**DIVISION IV**

**ACCESS BY PERSONS CONCERNED**

*§ 1. — General provisions*

**27**. Every person carrying on an enterprise who holds personal information on another person must, at the request of the person concerned, confirm the existence of the personal information, communicate it to the person and allow him to obtain a copy of it.

At the applicant’s request, computerized personal information must be communicated in the form of a written and intelligible transcript.

If the person concerned is handicapped, reasonable accommodation must be provided on request to enable the person to exercise the right of access provided for in this division.

**28**. In addition to the rights provided under the first paragraph of article 40 of the Civil Code, any person may, if personal information concerning him is inaccurate, incomplete or equivocal, or if collecting, communicating or keeping it are not authorized by law, require that the information be rectified.

**28.1**. The person to whom personal information relates may require any person carrying on an enterprise to cease disseminating that information or to de-index any hyperlink attached to his name that provides access to the information by a technological means, if the dissemination of the information contravenes the law or a court order.

The person may do likewise, or may require that the hyperlink providing access to the information be re-indexed, where the following conditions are met:

(1) the dissemination of the information causes the person concerned serious injury in relation to his right to the respect of his reputation or privacy;

(2) the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and

(3) the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury.

In assessing the criteria set out in the second paragraph, the following, in particular, must be taken into account:

(1) the fact that the person concerned is a public figure;

(2) the fact that the information concerns the person at the time the person is a minor;

(3) the fact that the information is up to date and accurate;

(4) the sensitivity of the information;

(5) the context in which the information is disseminated;

(6) the time elapsed between the dissemination of the information and the request made under this section; and

(7) where the information concerns a criminal or penal procedure, the obtaining of a pardon or the application of a restriction on the accessibility of records of the courts of justice.

Sections 30, 32 and 34 apply, with the necessary modifications, to a request made under this section. When granting such a request, the person in charge of the protection of personal information shall attest, in his written reply under section 32, to the cessation of the dissemination of the personal information or to the de-indexation or the re-indexation of the hyperlink.

(…)

**DIVISION V**

**RECOURSE**

(…)

*§ 1. — Examination of disagreements*

**42**. Any interested person may submit an application to the Commission d’accès à l’information for the examination of a disagreement relating to the application of a legislative provision concerning access to or the rectification of personal information, or concerning the application of section 28.1.

(…)

**DIVISION VII**

**APPLICATION OF THIS ACT**

(…)

*§ 2. — Inquiry*

**81**. The Commission may, on its own initiative or following a complaint by a person, inquire into or entrust a person with inquiring into any matter relating to the protection of personal information as well as into the practices of a person who carries on an enterprise and who collects, holds, uses or communicates such information to third persons. A complaint may be filed anonymously.

**81.1**. It is forbidden to take a reprisal against a person on the ground that the person has, in good faith, filed a complaint with the Commission or cooperated in an investigation.

It is also forbidden to threaten to take a reprisal against a person to dissuade him from filing a complaint or cooperating in an investigation.

(…)

**83**. The inquiries of the Commission are non-adversary investigations.

Following an inquiry relating to the collection, retention or communication of personal information by a person carrying on an enterprise, the Commission may, after giving the person an opportunity to present his observations, recommend or order the application of such remedial measures as are appropriate to ensure the protection of the personal information within the reasonable time limit the Commission specifies.

**83.1**. Every person carrying on an enterprise must, at the request of the Commission, provide it with any information it requires on the carrying out of this Act.

(…)

*§ 4.1. — Monetary administrative penalties*

**90.1**. A monetary administrative penalty may be imposed by a person designated by the Commission, but who is not a member of any of its divisions, on anyone who

(1) does not inform the persons concerned in accordance with sections 7 and 8;

(2) collects, uses, communicates, keeps or destroys personal information in contravention of the law;

(3) does not report, where required to do so, a confidentiality incident to the Commission or to the persons concerned;

(4) does not take the security measures necessary to ensure the protection of the personal information in accordance with section 10;

(5) does not inform the person concerned by a decision based exclusively on an automated process or does not give the person an opportunity to submit observations, in contravention of section 12.1; or

(6) is a personal information agent and contravenes any of sections 70, 70.1, 71, 72, 78, 79 and 79.1.

Following a failure referred to in the first paragraph, a person may, at any time, enter into an undertaking with the Commission to take the measures necessary to remedy the failure or mitigate its consequences. The undertaking must identify the acts or omissions constituting a failure and the provisions involved. It may also include the conditions the Commission considers necessary and contain a requirement to pay a sum of money.

If the undertaking is accepted by the Commission and is complied with, no monetary administrative penalty may be imposed on the person carrying on an enterprise with regard to the acts or omissions mentioned in the undertaking.

(...)

**90.5**. A monetary administrative penalty is imposed on the person in default by notification of a notice of claim setting out the amount of the claim, the reasons for it, the time from which it bears interest, the right to apply for a review of the decision, the right to contest the review decision before the Court of Québec and the time limit for bringing such proceedings.

The notice of claim must also include information on the procedure for recovery of the amount owing, in particular with regard to the issue of a recovery certificate under section 90.14 and its effects. The person must also be advised that the facts on which the claim is founded may result in penal proceedings.

The amount owing bears interest at the rate determined under the first paragraph of section 28 of the Tax Administration Act (chapter A-6.002), from the 31st day after notification of the notice.

The notification of a notice of claim interrupts the prescription provided for in the Civil Code with regard to the recovery of the amount owing.

**90.6**. The person in default may apply to the Commission in writing for a review of the decision to impose a monetary administrative penalty, within 30 days after notification of the notice of claim.

A member assigned to the Commission’s oversight division is responsible for reviewing the decision.

(…)

**90.11**. No monetary administrative penalty may be imposed on a person for a failure to comply with this Act if a statement of offence has already been served on the person for a failure to comply with the same provision on the same day, based on the same facts.

**90.12**. The maximum amount of the monetary administrative penalty is $50,000 in the case of a natural person and, in all other cases, $10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.

**90.13**. The debtor and the Commission may enter into a payment agreement with regard to the amount owing. Such an agreement, or the payment of the amount owing, does not constitute, for the purposes of penal proceedings or any other administrative penalty under this Act, an acknowledgement of the facts giving rise to it.

(…)

*§ 5. — Penal provisions*

**91**. Anyone who

(1) collects, uses, communicates, keeps or destroys personal information in contravention of the law,

(2) fails to report, where required to do so, a confidentiality incident to the Commission or to the persons concerned,

(3) contravenes the prohibition set out in section 8.4,

(4) does not take the security measures necessary to ensure the protection of the personal information in accordance with section 10,

(5) identifies or attempts to identify a natural person using de-identified information without the authorization of the person holding the information or using anonymized information,

(6) is a personal information agent and contravenes any of sections 70, 70.1, 71, 72, 78, 79 and 79.1,

(7) impedes the progress of an inquiry or inspection of the Commission or the hearing of an application by the Commission by providing it with false or inaccurate information, by omitting to provide information it requires or otherwise,

(8) contravenes section 81.1,

(9) refuses or neglects to comply, within the specified time, with a demand made under section 81.3, or

(10) fails to comply with an order of the Commission

commits an offence and is liable to a fine of $5,000 to $100,000 in the case of a natural person and, in all other cases, of $15,000 to $25,000,000, or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year.

**92**. The Commission may, in accordance with article 10 of the Code of Penal Procedure (chapter C-25.1), institute penal proceedings for an offence under this division.

**92.1**. In the case of a subsequent offence, the fines under this division are doubled.

**92.2**. All penal proceedings must be instituted within five years of the commission of the offence.

**92.3**. In determining the penalty, the judge takes into account the following factors, among others:

(1) the nature, seriousness, repetitiveness and duration of the offence;

(2) the sensitivity of the personal information concerned by the offence;

(3) whether the offender acted intentionally or was negligent or reckless;

(4) the foreseeable character of the offence or the failure to follow recommendations or warnings to prevent it;

(5) the offender’s attempts to cover up the offence or failure to try to mitigate its consequences;

(6) whether the offender failed to take reasonable measures to prevent the commission of the offence;

(7) whether the offender obtained or intended to obtain an increase in revenues or a decrease in expenses by committing the offence or by omitting to take measures to prevent it; and

(8) the number of persons concerned by the offence and the risk of injury to which they are exposed.

**93**. Where an offence under this Act is committed by a legal person, the administrator, director or representative of the legal person who ordered or authorized the act or omission constituting the offence, or who consented thereto, is a party to the offence and is liable to the prescribed penalty.

*§ 6. — Damages*

**93.1**. Where the unlawful infringement of a right conferred by this Act or by articles 35 to 40 of the Civil Code causes an injury and the infringement is intentional or results from a gross fault, the court shall award punitive damages of not less than $1,000.