ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DU QUÉBEC

Submission to the Committee on Institutions on Bill 64, An Act to modernize legislative provisions as regards the protection of personal information

October 2020

Table of Contents

Preamble

Mega-data, artificial intelligence, cloud computing, blockchains: these technologies are at the origin of what is now called the digital revolution, a recent phenomenon characterized by the multiplication of digital data, accessible everywhere and at all times.

Faced with the exponential growth of data, some will see new opportunities or vulnerabilities to exploit. Others will be resistant to innovative projects due to lack of knowledge or appetite for risk. Against a backdrop of uneven digital maturity, one factor is essential if Québec is to innovate and prosper: trust.

- Trust that an individual's data is collected ethically and used appropriately
- Trust that innovative data exploitation projects are based on accurate and verifiable information
- Trust that all players play by the same rules

Without trust, Québec will not be able to become a leader in the new data-driven economy.

Recent incidents in Québec have demonstrated the importance of a framework that can protect personal information adequately, as well as the fragility of public trust. In addition to the risk of data theft, Canadian and Québec businesses are increasingly vulnerable to cyber attacks, whether they are SMEs, non-profits or multinationals.

Not only is it essential to effectively protect the personal data of Québecers against malicious appropriation or alteration, but public and private organizations must also be able to trust the quality and accuracy of the data they use for their daily activities and decisions. This trust must extend to citizens, who are entitled to transparent customer experience in their interactions with institutions and businesses.

CPAs have always played a crucial role in public trust by vouching for the credibility and transparency of both financial and non-financial information. They make sure data is managed soundly, from the initial capture to archiving and destruction, including security, availability and validity. In sum, given their extensive expertise in certification, standardization and data management, CPAs are well positioned to contribute to the design, creation and implementation of data governance initiatives. Following a national reflection on its future, the accounting profession has undertaken to actively collaborate in defining a data governance model.[1]

[1] https://www.cpacanada.ca/en/foresignt-initiative/data-governance

The potential value of a data certification process was also discussed during Innovation, Science and Economic Development Canada's public consultations on digital and data.[2] Such a system would reassure citizens and organizations that certified individuals or organizations meet a specific standard for managing the data entrusted to or produced by them. Québec should also consider setting standards and creating a data certification process.

As we said earlier, the world is changing, and fast. The nature and volume of the data and information collected, the use made of it and the desire to use it call for resolute and agile action to reassure citizens about governance and the protection of personal data.

At this point in time the Ordre des CPA welcomes the introduction of a bill covering the protection of personal information. A reform of the ecosystem for protecting such information is long overdue, since the original legislative framework established in the early 1980s was not designed to keep pace with technological development in the 21st century.

Bill 64 is an important milestone in this reform. Setting out basic principles for the protection of personal data is the first step in a culture shift for businesses that have been slow to plunge into the digital age. Bill 53, the *Credit Assessment Agents Act* which is currently being studied, is another one. Bills to create a citizen digital identity and reform the rules on access to information will complete the picture.

Bill 64 raises many questions about its underlying approach and the principles it sets out. Some concerns are: how Québec's legislation aligns with laws in other jurisdictions, particularly within the North American economic space; the resources that businesses will have to mobilize to comply with it; the pace at which the legislation will be implemented; and the penalties in the event of default. Some of the definitions in the bill will also need to be clarified.

That said, it would be unfortunate if the proposals under consideration quickly became obsolete, because the legislator did not take the opportunity to update them further and truly upgrade the protection of Québecers' personal information.

The Ordre des CPA submits its comments and recommendations in a constructive spirit and out of a desire to contribute its expertise to the debate.

[2] CPA Canada, Roundtable report: Positioning Canada to lead in a digital and data-driven economy
.

Clearly defined concepts

The detailed study of the bill by parliamentarians is an excellent opportunity to clarify and truly update the terminology used in the protection of personal information. The Ordre des CPA du Québec cannot overemphasize the need for the proposed legislative and regulatory provisions to be written in clear terms to ensure compliance with the rules, making them easy for consumers and organizations to understand so that the greatest number of people will abide by them. The tightening of penalties in the bill also argues for clarity so that there is no room for interpretation. At the present time, many of the terms and concepts referred to in the bill seem to be self-evident to the legislator, although they really deserve more special attention.

Personal information

Personal information, the very subject of the bill, remains as broadly and vaguely defined as it was originally in the two main laws governing its protection.

> ***An Act respecting the protection of personal information in the private sector***
>
> **2.** *Personal information is any information which relates to a natural person and allows that person to be identified.*
>
> ***An Act respecting access to documents held by public bodies and the protection of personal information***
>
> **54.** *In any document, information concerning a natural person which allows the person to be identified is personal information.*

We suggest that the definition of personal information be updated in both Acts and that it be identical throughout the Québec legislative corpus. The European definition could be a model:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,* ***location data****, an* ***online identifier*** *or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*[3]

This definition is of interest to us for several reasons. Resolutely modern, it refers to an online identifier, location data and other personal characteristics. It is a good illustration of the diversity of elements that can constitute personal information or data. Financial data thus becomes just as personal as an element of a person's identity, such as sexual orientation or social insurance number.

[3] *General Data Protection Regulation (GDPR)*, Article 4(1)

Determining the sensitivity of information

Leaving the determination of sensitivity to each organization or company leads to significant, avoidable risks. The bill should provide objective assessment criteria. The current wording of sections 12 and 102 of the bill states that "*personal information is sensitive if, due to its nature or the context of its use or release/communication, it entails a high level of reasonable expectation of privacy*." We understand the legislator's desire to make the definition adaptable to circumstances and have it evolve over time. However, it is our view that such a generic definition has more potential disadvantages than advantages.

The lack of objective criteria for determining what constitutes a high expectation of privacy may lead to conflicting decisions from one organization to another and, therefore, significant enforcement difficulties, since there is also a need to obtain "consent given expressly" for any secondary use of the information, such as for commercial or philanthropic prospecting or for forwarding to a third party.

Given the importance of the sanctions that may be imposed on organizations that misinterpret "reasonable expectations of privacy," it is important that the concept of "high level of reasonable expectation of privacy" be clarified. We also believe that this definition cannot be limited to the prohibited grounds of discrimination alone. It might be appropriate here to draw inspiration from the General Data Protection Regulation (GDPR), which provides a very specific framework similar to that in the bill, forbidding the "*[P]rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation[…]*"

Clarification of the consent required

It is difficult to reconcile the possibility that sections 12 and 13 of the bill seem to open up for obtaining implied consent when the use or disclosure does not involve sensitive information with the definition of "consent" in section 9, which refers in **all cases** to consent that is "clear, free, informed and given for specific purposes":

> *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 and separately from any other information provided to the person concerned.*

If the legislator wishes to define only the concept of "consent given expressly" in sections 12 and 13 in this way, that should be specified, otherwise any possibility of implied consent is eliminated.

Moreover, the notion of consent "given for specific purposes" and "sought for each of those purposes" is already giving privacy officers in organizations headaches. Should the consent forms be revised to obtain a separate consent for each proposed use, or will a single consent on a form describing all such uses be sufficient? It would therefore be highly desirable to make guidelines with examples of "specific consent" tailored to different situations available to organizations to help them define their obligations.

Harmonizing terminology

We cannot stress enough the importance of harmonizing and updating the terminology of the legislative corpus. Section 14 of the bill, which introduces section 63.7 into the *Act respecting access to documents held by public bodies and the protection of personal information*, is a good illustration of the problem According to the proposed wording, when a security incident occurs the person responsible for the protection of personal information who communicates personal information without having obtained the prior authorization of the person concerned must "record the release of the information." However, section 18.1 of the *Act respecting the protection of personal information in the private sector* stipulates that the person who communicates personal information for such purposes must "make an entry of the communication." We believe that the concept of "entry" is unclear and refers to an outdated approach.

Inter-jurisdictional transfers: impracticable obligations

The free flow of data is a very important issue right now. So much so that it has become the fifth freedom of the Single Market, enshrined in European law, subject to the protection of personal information under the *General Data Protection Regulation.*[4] Since data has become a value in itself, the European Union deems it essential to harmonize national laws so as to allow it free movement, while at the same time protecting personal data.

Section 103 of the bill, amending section 17 of the *Act respecting the protection of personal information in the private sector,* provides that personal information may be disclosed outside Québec only after a privacy impact assessment has concluded that the information will be protected the same way under the applicable legal regime as if it were kept in Québec.

This is a very restrictive requirement in a context where the activities of businesses and professionals have no borders; it could act as a brake on economic exchanges and place Québec businesses in an untenable situation.

A privacy impact assessment requires a study of comparative law and the intervention of lawyers who may have to invest considerable time on it. In other words, a costly and complex operation that may be impossible for SMEs.

The proposed section 17.1 does stipulate that the Minister must "*publish a list of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec*." But it is not known whether this list will be published at the same time as the Act comes into effect. Nor is the government likely to make an exhaustive study of all the legal regimes of all States.

Further, a list of States (i.e. countries) is insufficient to define equivalent legal regimes outside Québec. The term "jurisdictions" should be used here, not States, since laws are likely to vary within confederated States such as Canada and the United States.

It is also curious that this obligation is imposed for data transmitted outside Québec, which is not a State, and that they talk about a State when assessing legal regimes outside Québec. Treating other Canadian provinces as foreign jurisdictions poses a fundamental problem for Québec companies doing business elsewhere in Canada. Unless the Minister publishes a decree recognizing all of Canada as a State with an equivalent legal regime when the Act comes into effect, companies will be required to assess the legal regime in each province where their data may be located or used.

[4] MOURON, Philippe, « La libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'Union européenne », La revue européenne des médias et du numérique, no 49 Hiver 2018-2019.

Accounting firms that are part of a Canadian and international network are an example of this type of business. Does this mean they will have to assess the applicable legal regime in order to go on billing in another Canadian province? The Government of Québec must work with all the other provinces and territories and the federal government to harmonize the laws applicable to the protection of personal information.

Internationally, this requirement could considerably slow down or even curtail Québec's trade exchanges. We find it absurd to ask each company to individually assess the legal regime of the same State. The assessment should be made just once by the Government, with a uniform result all companies can rely on. For States that are not on the list published by decree under section 17.1 of the bill, the Government could offer a service to assess a State's legal regime at the request of companies. If gaps are found, the assessment report should specifically identify the terms and conditions to be included in an agreement "for the purpose of mitigating the risks identified in this assessment." Once again, we believe that the bill will add to the regulatory and administrative burden on Québec businesses, particularly those that do business with emerging economies.

The real long-term solution is to adopt international standards for the governance of data and personal information. The Standards Council of Canada has created the Canadian Data Governance Standards Collaborative to determine needs and make suggestions for standards for data assessment, collection, classification and sharing. That involves studying what is being done elsewhere in the world and adopting a harmonized framework to establish minimum rules for businesses to follow so that data can be exchanged and shared in different jurisdictions. The Ordre des CPA is willing to participate in that kind of reflection at the provincial level and promote dialogue at the national and international levels.

Sanctions: the need for a modulated approach

Several briefs submitted to the Committee on Institutions stressed the severity of the administrative and penal sanctions provided for in the bill. We acknowledge that the most effective way to hold people accountable is by imposing dissuasive sanctions, and that administrative sanctions are a good way of ensuring compliance with the proposed measures, but several elements of the sanctions in the bill raise questions and should be discussed further.

First, it should be noted that organizations that use service providers have limited control over the data they collect, produce or use, and that such control cannot be compared with that of large corporations. Large corporations rely on risk management teams, develop their own computer and artificial intelligence systems, and data processing is a routine operation with significant market value for them. We find it logical that companies that provide IT and data storage services be subject to more severe penalties than the SMEs that use their services. We therefore propose that sanctions be tailored to the sophistication and scope of companies' activities in the collection, production and use of data.

Second, when copying the penalties provided for in the European GDMP, which are based on companies' worldwide sales, the legislator should give some consideration to the risk of discouraging certain companies outside Québec--particularly North American companies--from offering their products and services on the Québec market, which is not significant in terms of the risks of non-compliance and the severity of the penalties. Québecers will not be better served.

Lastly, the scope of the law should be clarified. The scope of both penal and administrative sanctions based on a company's worldwide sales suggests that the intention is to subject foreign companies offering services in Québec to such penalties, even if they do not have a physical establishment here. If that is the legislator's intention, it should be in the form of an express provision.

If, on the other hand, the *Act respecting the protection of personal information in the private sector* applies only to businesses with an establishment in Québec, the legislator should seriously consider the competitive harm that Québec businesses could suffer, particularly those in the artificial intelligence sector, a cutting-edge sector in which Québec is a world leader attracting the best minds in the field.

Staggered implementation

SMEs account for almost all Québec businesses. In 2019, according to the Institut de la statistique du Québec, 99.8% of businesses were SMEs, 53% had fewer than 5 employees and 32.6% had between 5 and 19 employees.[5] Under Québec law, a professional practising alone and offering services to third parties is a business. An artisan who uses a service provider to host his or her website in order to sell jewelry would therefore also be a business and would be subject to the amendments made by the bill.

It is important not to lose sight of this reality. While it is essential to update the laws governing personal information, that will require Québec businesses to upgrade considerably and, consequently, make major investments of money, time and staff mobilization.

For example, companies that deal with service providers to host their data or websites have hardly more bargaining power with these providers than mere consumers. Yet the bill forces the same risk assessment obligations with respect to personal data on them, and they must ensure that their contracts with the service provider set out the measures the service provider must take to protect their customers' personal data. But in such cases it is the service provider that has the expertise in data security. Businesses will therefore have to assess the scope of the standard contract with the service provider and switch to another provider if the contract does not meet the requirements of the Act. That is a very heavy burden for a very small company.

It is utopian to think that all companies have internal resources with the expertise to conduct a Privacy Impact Assessment (PIA) or draw up a data governance policy. Almost all of them will have to call in external resources to guide them through the various implementation steps of the bill. Will they have the financial capacity? Just the requirement to publish the data governance policy on the company's website and keep it up to date will be a major challenge for many SMEs.

The Ordre des CPA believes that it could take over two years to implement the new rules, even though it has in-house expertise in this area and is highly aware of the importance of its confidentiality obligations. This time frame is due to the need to revise policies, processes and all existing contracts in the light of the final text of the Act, develop new information systems and update the website. It is therefore easy to imagine what this will mean for less seasoned private companies, which do not have employees with expertise in risk management or data management, or whose limited financial resources do not allow them to call in the specific expertise required. It seems essential to us that the implementation of the Act and the achievement of the laudable objectives sought by the legislator not be compromised by a regulatory and administrative burden that would curtail the productivity of organizations and countermand the relief objectives of the Ministère de l'Économie et de l'Innovation.

[5] NIKUZE, Pascasie, Les entreprises québécoises de moins de 5 employés - Portrait et contribution à la dynamique des entreprises et de l'emploi, July 13, 2020, Institut de la statistique du Québec.

The bill should therefore provide for transitional measures staggering its entry into effect and deferring the implementation of administrative and penal sanctions, in order to allow organizations to comply with the new requirements of the law, inform and train all their employees and internalize their personal data management policies. To be effective, privacy protections should not be the sole responsibility of senior management. They are the responsibility of all employees.

These transitional measures could differ depending on the size of the company and the nature of its activities, as is the case in some bills that adapt the deadlines to large, medium and small businesses. That would take into account the reality of businesses, which do not all have the same expertise and financial resources for complying with the new obligations prescribed by this bill.

Support for organizations and the public

The best personal data management policy will only be effective if it is understood and applied by the organization and by each of its staff members. Unlike other types of information, personal data is collected and used at all levels of the organization. It is therefore imperative to quickly set up a guidance system that will generate support for the changes proposed by the bill.

That is why the Ordre believes that the implementation of the law should be preceded by a mandatory coaching and training program, set up and managed by the Commission d'accès à l'information (CAI). Training should be provided to all target organizations and their employees.

The CAI should also create and produce explanatory guides to help organizations understand the various concepts and obligations introduced by the bill and give practical demonstrations of how they will work in their respective sectors.

At the same time, a digital literacy program should be developed to help the general public take ownership of the notions of personal data protection and develop sound digital practices. Organizations' informed consent obligations will only fully achieve their purpose if the public is aware of the concepts referred to in the consent forms and understands the language used. The same applies to the requirement for organizations to publish their data governance and confidentiality policies on their websites. For its part, the accounting profession will be able to bolster its financial literacy program to include a digital component in order to contribute to civic education efforts.

Record keeping and storage for professionals in the digital age

Bill 64 raises some concerns about the legislative framework for professionals who access a multitude of confidential information in the course of their practice--including personal information and information about businesses--which must be protected under professional secrecy. However, case law recognizes that expectations of privacy protection are highest in the relationship between professionals and clients.[6]

New technologies have become an integral part of professionals' daily lives, especially CPAs, and have revolutionized their practices. Everything has changed rapidly in recent years: teleconsultations, work and research tools, communication with the clients and especially the protection of confidential information. Paper files stored in vaults have been replaced by virtual files stored in the cloud. It is therefore imperative that the professional system keep pace and demonstrate flexibility and agility. Unfortunately, that is not happening.

The *Professional Code* empowers the professional orders to determine the standards relating to the keeping, holding and maintenance of professionals' records (s. 91 *Professional Code*). However, it is clear from the regulations adopted by the various professional orders that the rules for keeping professional records are outdated and need to be reviewed. In the interest of consistency with the objectives of the bill, we therefore feel it is imperative that the Office des professions draw up guidelines for the drafting of regulations on the keeping, holding, and maintenance by professionals of information protected by professional secrecy.

The *Professional Code* also provides that the Office des professions must adopt a framework regulation on the holding and keeping by the orders of documents for overseeing the profession. If the Office wishes to adopt such a regulation, this would be a good time to adopt a regulatory framework that is harmonized with the requirements of Bill 64.

[6] *(Attorney General)* v. *Chambre des notaires du Québec*, 2016 SCC 20 [2016] 1 S.C.R. 336 para 35. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/15989/index.do

Reporting of security incidents by professionals

The use of technology for the collection, storage and use of data carries risks. No one is safe from theft or cyber attacks. In the light of recent security incidents that may have compromised the personal information of millions of people, the Ordre welcomes the imposition of an obligation on public bodies and people operating businesses to inform anyone whose personal information may have been compromised by a security incident. By having a complete picture of the incidents that may have affected the confidentiality of their personal information, citizens will be able to better assess their risks and take the measures they deem necessary to protect themselves, particularly against identity theft.

Professionals governed by the *Professional Code* hold a great deal of confidential information obtained during the course of a privileged and trusting relationship. The explicit obligation to notify any person whose personal information is at risk of being compromised by a security incident is perfectly in line with the spirit of existing professional obligations such as professional secrecy, objectivity and integrity, and the duty of loyalty to the client.

However, the confidential information held by professionals is not limited to personal information governed by the *Act respecting access to documents held by public bodies and the protection of personal information* and the *Act respecting the protection of personal information in the private sector*, which apply only to the personal information of natural persons and do not in any way protect the confidential information of businesses. Yet the clientele of many professionals, including CPAs, includes both businesses and individuals, and the professionals become the trustees of extremely sensitive information for the businesses they serve. The Ordre believes that all clients of professionals should benefit from the same reporting guarantees and thus enjoy better protection under professional secrecy.

Security incidents are two-pronged breaches of professional secrecy, involving both the obligation not to disclose confidential client information and the obligation to protect such information. The right to respect for professional secrecy is enshrined in section 9 of the *Charter of Human Rights and Freedoms* and section 60.4 of the *Professional Code*.

It would therefore be appropriate to include in the *Professional Code* the obligation for all professionals to notify their clients about breaches of confidentiality in relation to any confidential information; that obligation will be in addition to the obligation to disclose incidents involving personal information.

The lifting of professional secrecy

If the incident presents a risk of serious harm, sections 14 and 95 of the bill provide for the possibility of notifying any person or body that may be able to reduce that risk, disclosing only the personal information necessary for that purpose without the consent of the person concerned.

According to the *Professional Code*, a professional may be released from the obligation of professional secrecy "*only with the authorization of his client or where so ordered or expressly authorized by law*." However, the wording of sections 14 and 95 does not contain any express provision allowing for the lifting of professional secrecy, a gap that the legislator would be well advised to fill.

Conclusion

The reform proposed by the Government in Bill 64 is a major one. It will require a culture shift within organizations plus the allocation of significant resources and, for many, the development of in-house expertise.

Most organizations will not be able to do it alone. They will have to be guided, equipped and coached. This calls for the Commission d'accès à l'information to play its role fully and, in particular, take on some of the obligations currently assigned to organizations by the bill. It must also help citizens understand their new rights and organizations perform their new obligations.

To do so, the CAI must be provided with the financial, human and material resources it needs to bring the Government's objectives to fruition. That is an essential condition for the success of this reform.

It is imperative that the laudable objectives of the bill not be compromised by regulatory and administrative red tape that could undermine the productivity of organizations and businesses. We therefore call on parliamentarians to adopt a clear text using up-to-date terminology and concepts, a modulated implementation schedule and simplified obligations.

The framework will have to reassure the various stakeholders, including citizens, that their information will be collected and used according to sound governance practices. Without trust, innovation will be slow.

The companies that stand out in the new economy will be those that take advantage of all the data available. To do this, in a world where fake news is common and trust in traditional institutions is eroding, society as a whole needs to know which information or organization is reliable, especially as technology is increasingly being trusted over people.[7] This does not only apply to personal data, but to all information generated.

Establishing basic principles for the protection of personal data is a necessary milestone to guide businesses that have been slow to plunge into the digital age. However, if Québec wants to become the spearhead of a connected and innovative society, all digital information will one day have to be regulated.

[7] CPA Canada, « La voie à suivre », Projet voir demain 2018, p. 18, en ligne : https://www.cpacanada.ca/foresight-report/fr/index.html?sc_camp=2B1B40A7F54A4CCDB896A7AF16B79E21#page=1

Recommendations

The Ordre des CPA makes the following recommendations, based on protection and the public interest:

Recommendation 1

Review and update the definition of what constitutes personal information.

Recommendation 2

Establish objective criteria for determining what constitutes sensitive information with a high level of reasonable expectation of privacy.

Recommendation 3

Amend section 14 to clarify the distinction between the concepts of "consent" and "consent given expressly" and create explanatory guides and guidelines for organizations to clarify the concepts underlying the bill and illustrate its application with concrete examples.

Recommendation 4

Harmonize the terminology of all the different laws governing the use and protection of data and personal information.

Recommendation 5

Clarify the scope of application of the *Act respecting the protection of personal information in the private sector* with regard to foreign companies doing business in Québec.

Recommendation 6

Replace the word "State" with "jurisdiction" in the proposed amendment of section 17.1 of the *Act respecting the protection of personal information in the private sector*.

Recommendation 7

Recognize the equivalence of legal regimes elsewhere in Canada, while working to harmonize them.

Recommendation 8

Create a service to assess the legal regimes of states and jurisdictions outside Canada with regard to the protection of personal information.

Recommendation 9

Adjust the system of administrative penalties that may be imposed by the Commission d'accès à l'information according to the size and nature of the activities of the organization in question.

Recommendation 10

Provide for transitional measures staggering the coming into effect of the bill and postponing the implementation of administrative and penal sanctions to allow organizations of different sizes to comply with the new requirements of the Act.

Recommendation 11

Set up a support and training program, developed and managed by the Commission d'accès à l'information, for organizations subject to the Act.

Recommendation 12

Deploy a digital literacy program, developed and managed by the Commission d'accès à l'information, to help the public take ownership of concepts and notions with regard to the protection of personal information.

Recommendation 13

That the Office des professions develop guidelines for the drafting of regulations relating to the keeping, holding and maintenance by professionals of information protected by professional secrecy.

Recommendation 14

That the Office des professions quickly adopt a framework regulation on the holding and storing of documents held by the professional orders as part of its mission to oversee the profession.

Recommendation 15

Amend section 60.4 of the *Professional Code* to require all professionals to notify their clients in the event of an incident that has caused a breach of confidentiality with regard to confidential information.

Recommendation 16

Add a provision to sections 14 and 95 of the bill expressly authorizing the lifting of professional secrecy.

Recommendation 17

Provide the Commission d'accès à l'information with the financial, human and material resources it needs to play its role fully and help the public and organizations understand the new legal framework.

ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DU QUÉBEC

5, Place Ville Marie, bureau 800, Montréal (Québec) H3B 2G2
T. 514 288-3256 1 800 363-4688 Fax 514 843-8375
www.cpaquebec.ca