End of clause-by-clause consideration of Bill 64: Where we stand

August 27, 2021

On August 24, the Committee on Institutions of the Québec National Assembly completed its clause-by-clause consideration of Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (Bill 64), which had begun in February 2021. In our previous bulletin, published at the end of the parliamentary proceedings in June, we discussed key changes made to Bill 64 up to this date.

Building on these previous developments, this bulletin highlights the most recent round of amendments passed in the few Committee sessions held in August. We invite you to consult our amended version of the *Act respecting the protection of personal information in the private sector* (Private Sector Act) for the exact wording of these amendments.

When the Committee reconvened, it had moved on to the consideration of section 124 of Bill 64 (of which there are 165 in total), which introduced an amendment to section 46 of the Private Sector Act. However, a few earlier sections of Bill 64 that had been suspended were revisited by the Committee in order to be considered for adoption; our review begins with discussion of these.

Privacy by design / by default

The Committee revisited and ultimately adopted section 100 of Bill 64 in a slightly amended form. This section enshrines the principle of privacy by default in the Private Sector Act by introducing section 9.1, which reads as follows:

> **9.1.** *Any person carrying on an enterprise who collects personal information by offering to the public a technological product or service that has privacy parameters must ensure that, by default, the parameters of the product or service provide the highest level of confidentiality without any intervention by the person concerned.*
>
> *The first paragraph does not include the privacy settings of a cookie.*

The government's amendment clarifies three elements regarding the application of the privacy by default requirement. First, it does not apply to technological products and

services used internally by a business' employees (e.g. intranet, back-to-the-office mobile app). Second, section 9.1 applies only when a technological product or service has privacy settings, such as a social networking account, a search engine or a mobile application. Finally, section 9.1(2) specifies that cookies are outside the scope of the provision. In this regard, the government has indicated that cookies are excluded since they are not “customizable”.

The practical consequences of section 9.1 of the Private Sector Act for businesses operating in Québec are difficult to assess, particularly given the uncertainty surrounding the meaning of the term “highest level of confidentiality”. Moreover, the intent of the legislator with this new section is also difficult to ascertain since the notion of privacy by design and/or by default was used in different ways during the Committee's deliberations, notably in relation to the obligation to conduct privacy impact assessments (PIA) (s. 3.3), the need to obtain express consent for the processing of sensitive personal information (s. 12(1)) and the requirement to disable technological functions that allow a person to be identified, located or profiled (art. 8.1(1)(2)). However, when Bill 64 was introduced, the government viewed this principle as requiring businesses to ensure that the privacy settings of their products and services guarantee that personal information collected will not be shared with an unspecified number of persons (whether organizations or individuals) without the consent of the individual concerned.[1]

Data portability right

The government also adopted an amendment to resolve the ambiguity surrounding the application of the portability right to personal information inferred or derived by a business from other information provided by the individual. Thus, section 27(3) of the Private Sector Act now provides that an individual may request that personal information collected from them, and not created or derived from their personal information, be communicated to them (or to another organization designated by the individual) in a structured, commonly used technological format.

In this regard, the government has clarified that the purpose of the portability right is to allow an individual to be able to retrieve the information they have provided to the business (and nothing more). Thus, the amendment aims to prevent the portability right from being used in such a way as to force a business to share data it has produced using proprietary methods with one of its competitors.

Personal information agents

New provisions regarding personal information agents have been adopted. As a reminder, the Private Sector Act defines this role as including “Any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports bearing on the character, reputation or solvency of the persons to whom the information contained in such files relates is a personal information agent” (s. 70(2)). Businesses in the field of credit or debt collection, or those who carry out private investigations or identity checks on individuals, are generally considered to be personal information agents.

Under the new provisions introduced by Bill 64, personal information agents will be required to:

- File a registration request with the Commission d'accès à l'information (CAI) accompanied with the required fees (s. 72);
- Provide various information to the public, including the fact that it holds personal information about other persons and, if applicable, credit reports, how to exercise access and rectification rights and the contact information of the person in charge of the protection of personal information (s. 79);
- Adopt rules of conduct to allow any person to whom personal information held by an agent relates to have access to the information and to have it rectified (s. 78);
- Destroy personal information after a seven-year retention period (s. 79.1).

It should be noted that the CAI maintains a register of personal information agents that is publicly available. The CAI specifies, however, that registration does not guarantee compliance with the Private Sector Act. Furthermore, it is important to remember that a personal information agent who fails to comply with the requirements prescribed by the Private Sector Act may be subject to monetary administrative penalties and/or penal fines.

Political parties

The Committee also adopted two new sections to the *Election Act*. Section 127.22 provides that the Private Sector Act applies to personal information about electors held by a political party, an independent deputy or independent candidate. As a result, political parties will have to designate a person in charge of the protection of personal information. It should be noted, however, that individuals will not be able to exercise their right of access, rectification or deletion with respect to personal information held by a political party since these provisions have been specifically excluded from the scope of section 127.22.

In addition, section 127.23 states that political parties may collect only electors' personal information that is necessary for election purposes, political financing, or for the purpose of a political activity as defined in section 88 of the Election Act. This provision also requires political parties to obtain the consent of individuals concerned when collecting or using their personal information. Consent may be implied, for example, when an elector responds to a request concerning their intention to vote.

CAI investigation procedure

The procedure for conducting investigations by the CAI's surveillance section has also undergone some changes. From now on, any person, whether qualified as having an interest in the matter or not, will be able to file a complaint with the CAI so that it may investigate any matter relating to a business' information handling practices. This complaint may be made anonymously (s. 81). In order to carry out its investigation, the CAI may require the production of any information or document (s. 81.2 and 83.1). Refusal to cooperate with an investigation or to provide the required documents will be considered a penal offence punishable by a fine.

In addition, a “whistleblower protection” provision prohibiting businesses from taking reprisals (e.g., demotion, suspension, dismissal, transfer or other disciplinary measure) against a person for having filed a bona fide complaint with the CAI or cooperated in an investigation has been introduced (s. 81.1).

It is also worth mentioning the new section 81.3 of the Private Sector Act, which gives the CAI the power to order any person involved in a confidentiality incident to take any measure to protect the rights of the individuals concerned, including an order that the compromised personal information be returned to the business or be destroyed. While it is questionable whether the CAI will be able to actually enforce such orders in many circumstances, such as an order directing a threat actor to surrender or destroy the personal information exfiltrated from a business' network, it is interesting to see the government recognize a more active role for the CAI in managing confidentiality incidents.

Monetary administrative penalties and penal offences

The Committee adopted the controversial regime allowing the CAI to impose monetary administrative penalties (more commonly known as “administrative monetary penalties” or “AMPs”). The maximum amount of penalties is set at $50,000 for an individual and $10,000,000 or 2 per cent of worldwide turnover for a legal entity (s. 90.12). The grounds on which the CAI may impose an AMP are:

- Failure to provide a proper privacy notice to individuals in accordance with sections 7 and 8 of the Private Sector Act;[2]
- Collecting, using, communicating, holding or destroying personal information in contravention with the provisions of the Private Sector Act;
- Failure to report a confidentiality incident to CAI or affected individuals in contravention of section 3.5 of the Private Sector Act;
- Failure to take appropriate security measures to protect personal information in accordance with section 10 of the Private Sector Act;
- Failure to inform the individual concerned by a decision based solely on an automated process of his or her personal information or giving the individual an opportunity to make representations, in contravention of section 12.1 of the Private Sector Act;
- For a personal information agent to contravene sections 70, 70.1, 71, 72, 78, 79 or 79.1 of the Private Sector Act.

It should be noted that section 90.1 of the Private Sector Act provides that AMPs will be imposed by “a person designated by the Commission, but who is not a member of any of its divisions”. The fact that the status of the person in charge of administering and imposing AMPs is left uncertain is concerning, especially considering the significant penalties that can be imposed under this new regime. That said, this issue may be resolved in the general framework for the application of monetary administrative penalties to be developed by the CAI pursuant to section 90.2 of the Private Sector Act, which the government has indicated may be similar to the one developed by the Minister of the Environment and the Fight Against Climate Change (available in French only).

In addition, the Committee adopted an amendment to section 90.1 introducing a mechanism by means of which a business can acknowledge its failure to comply with

applicable legal requirements and enter into an undertaking with the CAI to remedy the contravention or mitigate its consequences. Where such an undertaking is accepted by the CAI, the business cannot be subject to an AMP with respect to the acts or omissions covered by the undertaking (s. 90.1(2) and (3)).

In this regard, it is relevant to note that the government has repeatedly emphasized that the purpose of the AMP regime is to ensure compliance with the Private Sector Act's requirements. Thus, unlike fines that may be imposed following a penal offence, AMPs are not intended to be punitive. The government has also clarified that a business that has received an AMP and continues to violate the law could subsequently be fined under the penal regime. In other words, the two regimes are not mutually exclusive.

The Committee also adopted the amendments made by Bill 64 to the penal provisions of the Private Sector Act. Thus, the offences set out in section 91 encompass the grounds for the imposition of an AMP, with the addition of the following:

- Contravening the prohibition formulated in section 8.4 of the Private Sector Act (introduced by section 108 of the *Credit Assessment Agents Act*) against obtaining communication of personal information that is subject to a security freeze;
- Identifying or attempting to identify a natural person using de-identified information without the authorization of the person holding the information or using anonymized information;
- Obstructing an investigation or inspection by the CAI or the processing of an application by the CAI by, among other things, providing false or inaccurate information or failing to provide required information;
- Taking reprisals against whistleblowers in contravention of section 81.1 of the Private Sector Act;
- Refusing or neglecting to comply, within the specified time, with the CAI's request to produce information or a document as per section 81.2 of the Private Sector Act; or
- Failing to comply with an order from the CAI.

The maximum fine that can be imposed for a penal offence is $100,000 for a natural person and $25,000,000 or 4 per cent of worldwide turnover for a legal entity (s. 91). Moreover, the maximum amount for a natural person has been increased from $50,000 to $100,000 to distinguish the penal regime from the administrative regime and to reflect its dissuasive nature.

The statute of limitations for an AMP is 2 years from the date of the contravention (s. 90.10), whereas it is 5 years for penal offences (s. 92.2). An AMP can be contested before the Court of Québec (s. 90.9) whereas a penal sanction, which is imposed by a judge of the Court of Quebec, is subject to a right of appeal to the Superior Court (s. 270 Code of Penal Procedure).

Private right of action

The Committee also adopted an amendment to replace section 93.1, proposed by section 152 of Bill 64, with the following:

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

The Minister's comments indicate that the goal of the amendment is to ensure that the recourse provided for in this section is subject to the general rules of civil liability. However, section 93.1 is now limited to recognizing the court's authority to sanction an unlawful infringement of a right conferred by the Act or by sections 35 to 40 of the Civil Code with punitive damages where the infringement is intentional or results from gross negligence. The notion of a private right of action, *i.e.* the possibility for an individual to bring a civil claim against a business for compensation for an injury caused by a breach of the Private Sector Act, seems to have been set aside. However, given the lack of clear legislative intent in this regard, it is advisable to await clarification either during the final adoption debate or from the CAI before jumping to conclusions.

Next steps

There are only two steps left in the legislative process of Bill 64 in the National Assembly, namely the consideration of the Committee's report and the final passage debate. These two sessions will allow the Committee's members to present to their fellow members of Parliament the changes that were made to the Bill during its clause-by-clause consideration. However, it is unlikely that any further changes will be made to Bill 64 between now and its final passage. Given that the National Assembly officially resumes on September 14, it is reasonable to expect that Bill 64 will be passed by the end of October 2021.

Coming into force

The Committee adopted an amendment to section 165 of Bill 64 to provide for the coming into force of the *Act to modernize legislative provisions as regards the protection of personal information* in several phases. As a result, most of the new provisions introduced to the Private Sector Act will come into force two years after the Act receives its assent, except for certain specific provisions that will come into force one year after the Act receives its assent, including:

- The requirement to designate a person in charge of the protection of personal information (s. 3.1);
- The obligation to report a confidentiality incident (s. 3.5 to 3.8);
- The exception for disclosure of personal information in the course of a commercial transaction (s. 18.4); and
- The exception to disclosure of personal information for study or research purposes (s. 21 to 21.0.2).

In addition, the period for the right to portability of personal information (s. 27) has been maintained at three years from the date of the Act's assent.

Conclusion

There is no doubt that the work of the Committee on Institutions, which was spread out over 19 meetings over more than six months, has resulted in significant improvements to the initial version of Bill 64. Indeed, it is clear that by adopting this reform, Québec is taking an important step forward to ensure better protection of its citizens' personal information in the context of the digital economy.

However, it is unfortunate that members of Parliament were not more sensitive to the recommendations made by various stakeholders from the business community. Indeed, many of the new requirements that Bill 64 introduces in the Private Sector Act will be difficult for businesses to implement. These include the requirement to inform individuals of the names of third parties (including service providers) to whom the business may disclose personal information, the requirement to have technologies that identify, locate or profile an individual be deactivated by default and the requirement to ensure that the privacy settings of a product or service provide the highest level of confidentiality without any input from the individual.

Finally, the CAI will have a major role to play between now and the coming into force of the new provisions, as Bill 64 entrusts it with the responsibility of developing guidelines to facilitate the application of the *Private Sector Act* (new section 123(9) of the *Act respecting Access to documents held by public bodies and the Protection of personal information*) as well as a general framework for the application of AMPs (section 90.2).

Stay tuned, as we will soon publish a comprehensive guide to help businesses comply with the new privacy requirements introduced by Bill 64. In the meantime, please do not hesitate to contact BLG's Cybersecurity, Privacy & Data Protection team with any questions you may have about recent developments regarding the legal framework governing data protection in Québec.

1 See page 11 of the Mémoire au Conseil des ministres (French only).

2 These sections provide that the business must inform the individual, when collecting personal information, of the purposes for which the information is collected, the means by which the information is collected, the rights of access and rectification provided by law, and the right to withdraw consent to the disclosure or use of the information. Where applicable, the business must also inform the individual of the name of the third party for whom the information is being collected, the names of the third parties to whom it is necessary to communicate the information and the possibility that the information may be communicated outside Quebec. At the individual's request, the business must also indicate the specific personal information collected, the categories of persons who have access to this information within the business, the retention period of this information, the source of the information when it was collected from a third party, and the contact information of the person in charge of the protection of personal information.

By

Elisa Henry, Max Jarvie, Simon Du Perron, Andy Nagy

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.