The CAI rules on the interpretation of new AI requirements

December 22, 2022

The Commission d'accès à l'information (CAI) recently published a decision regarding the use of an artificial intelligence (AI) system. This decision refers to some new provisions introduced by the *Act to modernize legislative provisions as regards the protection of personal information* (Bill 64),[1] coming into force on September 22, 2023, and offers insight into the analytical framework the CAI might develop in connection with these provisions.

Background

The CAI issued its decision following an investigation into the use of an AI system by the Centre de services scolaire du Val-des-Cerfs (the School Board), following the publication of a news article.

The School Board retained the services of an accounting firm's data analysis specialists to develop an AI system capable of identifying students at significant risk of dropping out. To this end, the School Board granted its service provider temporary access to a database containing de-identified information of students, including grades and statistics on financial assistance, absenteeism, discipline and frequent address changes. This partnership led to the development of a machine-learning algorithm capable of generating a set of indicators to predict the risk of dropping out of Grade 6 students.

In its decision, the CAI assesses whether the School Board's development and use of this AI system are compliant with the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the Public Sector Act).

In this bulletin, we go over the CAI's main conclusions and their impact on how Québec's data protection laws are applied to AI systems. Given the similarities between the Public Sector Act and the *Act respecting the protection of personal information in the private sector* (the Private Sector Act), and the fact that Bill 64 brings similar amendments to both laws, private sector organizations can also learn from this decision.

1. Anonymization vs De-identification

The CAI found that the data sent by the organization to its service provider for the purpose of developing the algorithm was de-identified rather than anonymized. Let us recall that Bill 64 sets out that personal information is de-identified if it no longer allows the individual to be **directly** identified, and anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the individual to be identified **directly or indirectly**. This is a crucial distinction, since de-identified information remains subject to the legislation, unlike anonymized information.

In this case, the organization had removed 80 categories of sensitive data (*e.g.*, names, mailing and email addresses, phone numbers, usernames, etc.) from the training database before granting access to its service provider in order to reduce the risk of students and parents being identified. However, the CAI found that these measures were not “irreversible” in accordance with the terms of Bill 64. The CAI's analysis is fairly brief in this regard: it simply states that the organization is able to identify students from the training database by using other data collected over the course of their studies. This interpretation confirms the very high standard for anonymization under Québec privacy framework. Organizations that assert their project only involves the processing of anonymized data must be prepared to provide a detailed explanation of their anonymization methodology in order to convince the CAI that they comply with the statutory requirement and with generally accepted best practices. They could for instance submit a re-identification risk analysis conducted by a specialized firm and/or demonstrate how their practices comply with the recommendations of the Canadian Anonymization Network (CANON).

2. Consistent Purposes

The Public Sector Act provides that a public body may only use personal information for the purposes for which it was collected, unless it has obtained consent from the individual (s. 65.1). However, the Public Sector Act provides certain exceptions, including when information is used for purposes that are consistent with the purposes for which it was collected, that is to say when there is a relevant and direct link between the new purpose and the initial purpose.

In this case, the CAI found that the development of an AI system for the early detection of students at risk of dropping out is consistent with the pursuit of academic success, which was one of the School Board’s overarching aims when it first collected the students’ personal information. Accordingly, the CAI found that the School Board was not required to obtain additional parental consent to use the students’ information for this purpose. This conclusion supports a rather broad interpretation of the notion of “consistent purpose” which, incidentally, will be introduced in the Private Sector Act next September.

Moreover, the CAI held that the exception allowing personal information to be used without consent for consistent purposes applies **even when the use is made a service provider** (*i.e.*, the accounting firm) on behalf of the organization. Note that in this case, the processing of of personal information was governed by a written agreement in accordance with section 67.2 of the Public Sector Act (which is very similar to the new section 18.3 of the Private Sector Act coming into force on September 22).

3. Inferred Data

The CAI found that the data generated by the AI system, namely the indicators that predict students' risk of dropping out, is itself personal information as it helps build a profile of the students and is likely to affect the decisions made in their regard.

The CAI goes further by stating that the production of these indicators by the algorithm amounts to a "new collection" of personal information. Accordingly, the School Board must ensure that this collection complies with the requirements of the Public Sector Act, namely the necessity test under section 64[2] (ss. 4 and 5 in the Private Sector Act) and the notice requirement under section 65[3] (s. 8 of the Private Sector Act). Having found a breach of this duty to notice, the CAI ordered the School Board to inform the parents of students whose information was used to develop the system of:

- the project and its purpose;
- the fact that personal information collected during registration and throughout the studies was used in this project;
- the fact that an analysis of this personal information by the algorithm allowed for the creation of new personal information regarding the students; and
- the purposes for which the information was collected, the categories of persons who had access to the information and their rights of access and correction.

This conclusion highlights the importance of transparency when using AI systems, particularly when processing the personal information of minors. Note that the CAI recently published a report with several recommendations to ensure better protection for minors' personal information.

4. Data Retention

The CAI specified that when native data is sent to a third party for developing an AI system, this data must be deleted from the third party's servers once the mandate is complete.

The CAI also challenged the School Board's argument that the data generated while the AI system was in development, including a spreadsheet listing de-identified identifiers associated with risk factors, could be retained for a three-year period based on its retention schedule for documents related to studies, research, surveys and statistics. On this question, we note that Bill 64 introduces a requirement to make available, upon request from the individuals, the retention period applicable to their personal information (s. 65 para. 3 of the Public Sector Act and s. 8 para. 3 of the Private Sector Act). Thus, organizations must ensure they have a comprehensive and up-to-date retention policy in order to comply with these upcoming requirements.

5. Privacy Impact Assessment (PIA)

Although this obligation is not yet in force, the CAI has recommended that the School Board conduct a PIA before deploying the AI system, and ensure a periodic review of this PIA. It should be noted that Bill 64 makes it mandatory to conduct a PIA in three specific cases:

- for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the processing of personal information;
- before transferring personal information outside Québec or entrusting someone outside Québec with the task of processing personal information; and
- before disclosing personal information without consent to a person or body wishing to use the information for study or research purposes or for the production of statistics.

Organizations must therefore develop a procedure for conducting PIAs when required by law or when a project might have a high impact on individuals' privacy. The CAI has published a PIA guide (in French only) (which will be amended in light of Bill 64) which advise organizations to conduct a PIA when a project involves the processing of personal information by an AI system.

***

The *Centre de services scolaire du Val-des-Cerfs* decision sheds new light on how some of the new Bill 64's provisions will be interpreted

For any questions concerning recent developments affecting Québec's personal information protection framework, please contact a member of BLG's Cybersecurity, Privacy & Data Protection Team.

[1] Also known as "Bill 25".

<[2] A public body may only collect personal information if it is necessary for the exercise of its rights and powers or for the implementation of a program it administers. This standard was construed as requiring that the organization prove it has a legitimate, important and real objective that is proportional to the invasion of privacy (see *Laval (Ville)* c. *X.,* 2003 CanLII 44085 (C.Q.).

[3] Section 65 sets out that an organization must inform individuals of the following before or during the collection of personal information:

- the name and address of the public body on whose behalf the information is collected;
- the purposes for which the information is collected;
- the categories of persons who will have access to the information;
- whether the request is mandatory or optional;
- the consequences for the person concerned or for the third person, as the case may be, for refusing to reply to the request;
- the rights of access and correction provided by law.

By

Simon Du Perron

Expertise

Cybersecurity, Privacy & Data Protection, Artificial Intelligence (AI)

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.