PART 3 | PRIVACY 101 - OBLIGATIONS UNDER QUÉBEC'S NEW ACT 25: HOW TO ENSURE YOUR BUSINESS' BIOMETRIC DATA COMPLIES WITH THE LAW

Posted on September 15, 2022

Categories: Insights, Podcasts

This podcast series, intended for private sector companies doing business in Québec, dives into the requirements of Act 25 coming into force on September 22, 2022. Candice Hévin and Marie-Eve Jean, from our Privacy & Data Protection Group, lead the discussions on the changes to the private sector regime, namely the amendments to the Act respecting the protection of personal information.

In this episode, discover your responsibilities surrounding biometric data and disclosure obligations to the Québec privacy regulator.

Please note that the following provides only an overview and doesn't constitute legal advice. Listeners are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

Transcript

Marie-Eve Jean: Hello, and welcome to Privacy 101 – Obligations under Act 25, a series of podcasts designed to assist you in preparing to comply with Québec's new privacy legislation.

Candice Hévin: I am Candice Hévin.

Marie-Eve Jean: And I am Marie-Eve Jean.

Candice Hévin: We're both lawyers at McMillan LLP and we work together as a team to help businesses operating in Québec achieve compliance with Québec's privacy legislation.

Marie-Eve Jean: To give you some context, Québec adopted a new law on September 22, 2021. Bill 64 aims to modernize the privacy framework for both private and public sector regimes. This series focuses on the changes to the private sector regime, namely the amendments to the *Act respecting the protection of personal information in the private sector*, we will refer to it as Act 25.

Candice Hévin: In terms of timing, requirements will come into effect in three phases throughout the next three years. Although the majority of the new requirements will take effect as of September 22, 2023, some key requirements will take effect this month, as of September 22, 2022. A few requirements will also take effect as of September 22, 2024.

Marie-Eve Jean: In our previous episodes, we talked about enforcement mechanisms and your obligation to appoint a Privacy Officer and the obligations surrounding breach reporting, coming into force on September 22, 2022. In this episode, we will talk about the measures that impact the use of biometric data and that come into effect on September 22, 2022. So, what exactly is biometric data?

Candice Hévin: These are techniques that are used to analyze one or more physical or morphological characteristics. Physical characteristics can include fingerprints, facial features, the iris or retina of the eye. Biometric data can also include behavioural traits such as a person's gait, or biological characteristics, such as DNA.

Marie-Eve Jean: Biometric data is unique and specific to each person. That is what makes it highly sensitive information. It therefore qualifies as "sensitive personal information" under Act 25. Generally, companies use it to automate identification and authentication processes. Common examples in the every day world include using employees' fingerprints to record their "clock in" and "clock out" times; or using a facial recognition system to authorize access to a facility or room. Biometric data can be very helpful, but as we've said, it is "sensitive personal information" and that means that it involves risk.

Candice Hévin: This information is permanent, distinctive and unique and makes it possible to identify a person. The most significant risk is that it could be used to deduce information other than the identity of a person, such as a disease, or to impersonate or steal a person's identity. Another significant risk from a business perspective is that, if your organization has a biometric database that does not comply with the law, the CAI may consider it an invasion of privacy and can order its permanent destruction.

So what do you need to do to make your biometric database compliant?

Marie-Eve Jean: Here are the three steps you must take. Step 1: Conduct a Privacy Impact Assessment (PIA)

prior to creating a biometric feature or measurement database or biometric system. In your PIA, you will need to question yourself about necessity, purpose, proportionality and alternatives:

- It must be necessary to collect biometric data. And no, the fact that it is much more convenient is not in itself a justification for the need to collect it.
- The purpose must be important, legitimate and real.
- The data collected must be proportional to the use. For example, you will collect one fingerprint rather than the five fingers of the hand because you want to be mindful of proportionality.
- Alternatives are other measures that the company must provide to an individual if they refuse to consent to the collection of their biometric data. For example, an alternative measure can be to provide a personalized password rather than having someone provide their fingerprint or otherwise.

Candice Hévin: Step 2: Disclose the project to the CAI no later than 60 days prior to implementation and notify the CAI prior to using any biometric technologies to verify or confirm an individual's identity:

- This declaration must be made as soon as possible because the CAI may require adjustments to the biometric data system, which could delay its implementation.
- Important clarification: Only biometric databases that are used (i) to identify or authenticate individuals (ii) specifically by technological means are affected. Only these databases must be declared to the CAI. For example, a static photo bank will not need to be declared.
- A small note here, clients often get confused and often ask us who exactly should declare the biometric system - the one creating it or the one using it? As a general rule, the declaration of the biometric system is made by the company that will be using the system. As it is generally the company that holds and uses the personal information and not by the company that designed it, even though the company that designs the system may be required to store the biometric information of its customers.
- Note that this is not an absolute rule, it will sometimes be verified on a case-by-case basis and, in particular, given the context and obligations of Act 25, the CAI could request additional information from the entity that designed the system, if required, after analyzing the declaration of the company that uses the biometric system.

Marie-Eve Jean: Step 3: Fulfill the various obligations under Act 25 during project implementation (i.e., prior to its operation):

- You will need to obtain the express consent of the persons concerned. For this purpose, the CAI provides on its website a model consent form to use. You can always ask us to help you prepare and draft this form.
- Confirm the identity of individuals.

- Assess whether other means of identification are available and propose them, if applicable. This circles back to our "alternatives" which we discussed earlier, like providing a password rather than collecting someone's fingerprint.
- Respect the purpose for which the data is collected.
- Implement appropriate privacy and security measures.
- Ensure the safe and final destruction of the biometric data. When destroying, you must be sure to delete both the image and the encrypted code associated with the image, as they are both considered sensitive personal information.
- Finally, you will have to implement a process for user access and rectification requests.

Candice Hévin: So that concludes our third episode. We have several other tips and tricks relating to handling biometric data and conducting privacy impact assessments so don't hesitate to reach out.

Marie-Eve Jean: Make sure to tune in for the following episodes that will be released in the following months, where we'll dive into your obligations coming into force as of September 2023. This is Marie-Eve Jean.

Candice Hévin: And Candice Hévin.

Marie-Eve Jean: Of McMillan LLP. It's been a pleasure recording for you!