

Introduction Of Bill 33 And Bill 34 To Replace The Freedom Of Information And Protection Of Privacy Act (FOIP)



On November 6, 2024, the provincial government proposed legislative changes designed to replace Alberta's existing public sector access to information and privacy legislation, the *Freedom of Information and Protection of Privacy Act* ("FOIP"). These changes involved the introduction of two separate pieces of legislation: Bill 33 – the *Protection of Privacy Act* ("Bill 33"), and Bill 34 – the *Access to Information Act* ("Bill 34"). The Bills passed third reading on December 4, 2024, and were given Royal Assent on December 5, 2024. The legislation will come into force upon the proclamation of Bill 34 (*Access to Information Act*).

The proposed division of FOIP marks the first changes to Alberta's public sector privacy laws in two decades, and seeks to distinctly legislate privacy protections and access to information. It is expected that Bill 34 will be proclaimed some time in spring 2025.

Bill 33 – *Protection of Privacy Act*

Bill 33 will introduce the "strongest protections in the country and the strictest penalties", and will establish rules for how public bodies can create and use personal information and data, including:

- Mandating public bodies to have documented privacy management programs and privacy impact assessments in prescribed circumstances
- Requiring privacy breach notifications and reporting by public bodies where the privacy breach poses a real risk of significant harm. Public bodies will be required to promptly notice affected individuals, the Office of the Information and Privacy Commissioner (the "**OIPC**"), and the responsible Minister
- Requiring public bodies to notify individuals when the public body intends to input personal information into an automated system to generate content or make decisions, recommendations, or predictions
- Prohibiting public bodies from selling personal information for any purpose
- Prohibiting public bodies from data matching to produce derived personal information about an identifiable individual. Data matching will only be permitted for "research and analysis" and "planning, administering, delivering, managing, mentoring or evaluating a program or service"
- Establishing rules for the creation, disclosure and use of non-personal or de-

identified data.

- Requiring individuals to first attempt to resolve complaints with the relevant public body before going to the OIPC
- Introducing the following, significant penalties for the misuse of personal information:
 - For breaches involving personal information, individuals may be fined up to \$125,000, and organizations up to \$750,000; and
 - For breaches involving non-personal information and data matching violations, individuals may be fined up to \$200,000, and organizations up to \$1 million

The requirements of privacy management programs and privacy impact assessments are expected to be set out in Bill 33's supporting regulations. Further, many terms – including “predictions”, “automated system”, and “research and analysis” – are not defined in Bill 33, and it is unknown if definitions or further clarification will be provided in the regulations. The supporting regulations are not expected to be published until spring 2025.

Bill 34 – Access to Information Act

Bill 34 aims to modernize *FOIP*'s rules regarding access to information requests by recognizing electronic records, which the bill defines broadly as “a record that exists at the time a request for access is made or that is routinely generated by a public body that can be any combination of texts, graphics, data, audio, pictorial or other information represented in a digital form that is created, maintained, archived, retrieved or distributed by a computer system”.

Key changes under Bill 34 will include:

- Extending timelines to respond to requests both during emergencies and by specifying that timelines for responses are based on “business days” rather than calendar days
- Providing public bodies with additional powers to unilaterally extend timelines, subject to review by the Information and Privacy Commissioner
- Further clarification on what records can be withheld from disclosure, including:
 - Communications solely among political staff or between political staff and members of the Executive Council; and
 - Workplace investigation materials if the disclosure could interfere with, prejudice, or harm a workplace investigation, or cause harm to a witness or third party of the investigation
- Provide public bodies with the power to disregard access requests if the request is abusive, threatening, frivolous, or vexatious, or is made in an abusive or threatening manner (currently, only the Information and Privacy Commissioner had the power to allow a public body to disregard a request)
- Prohibit public bodies from submitting access requests to another public body
- Enable public bodies to identify information that is publicly available outside the formal access to information process

As with Bill 33, the supporting regulations are not expected to be published until spring 2025. Further, a special committee of the Legislative Assembly will be required to perform a comprehensive review of the Act every six years to provide recommendations for proposed amendments and regulations.

What does this mean for public bodies?

The replacement of *FOIP* with the proposed Bill 33 and Bill 34 will naturally come

with shifts in the privacy landscape. New access procedures will likely affect litigation involving public bodies, while new protection provisions may raise new grounds for claims. It remains to be seen the effect that extended time limits will have on access request wait times.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Authors: [Jennifer Davis](#), [Katherine Hagan](#), [Tom Ndekezi](#)

McLennan Ross LLP