Alberta overhauls its public sector access and privacy regime

January 21, 2025

I. Background

In December of last year, the Alberta legislature passed a major overhaul of Alberta's access and privacy legislation. Upon proclamation, Bill 33 and Bill 34 will split the *Freedom of Information and Protection of Privacy Act* (FOIP Act) into the new *Access to Information Act* (AIA)[1] and *Protection of Privacy Act* (PPA).[2]

The AIA will come into force at a time when public bodies in Alberta and across Canada are bearing a heavy burden of responding to access requests, in part due to challenges relating to retrieving and processing large sets of responsive e-mails and other electronic records. The AIA can be viewed as a strong response to this trend and overall will limit the right of access.

The PPA will bring breach notification and reporting based on the "real risk of significant harm" standard to the Alberta public sector. The PPA also features modernization provisions relating to de-identification and automated decision-making that are novel in public and private sector Canadian privacy legislation.

The new acts will govern "public bodies," including most provincial and local government entities. Private sector organizations are subject to the *Personal Information Protection Act* (PIPA). PIPA is also currently undergoing a legislative review, anticipated to conclude in June 2025.

II. Bill 34: the Access to Information Act

The AIA will replace the part of the FOIP Act that provides the public with a right of access to records in the custody or control of public bodies. The stated goal of the replacement is to align the access to information regime in Alberta with the realities of the modern digital world.[3]

To do so, the AIA will feature several important definitional changes that will affect its scope:

- The AIA will define "electronic record" as a "a record that exists at the time a request for access is made or that is routinely generated by a public body," excluding an obligation to produce unique reports from stored data.[4]
- "Information" will be defined as "content in a record," which suggests an exclusion of record metadata (*i.e.*, data about a record's creation and handling).[5]

The AIA preserves many of the "exclusions" that remove certain records from the access to information regime. For example, the research and teaching records exclusions meant to preserve academic freedom at post-secondary institutions will be preserved in the same form.[6] The AIA will also bring in new exclusions, including an exclusion for communications with "political staff" – a term to be defined by regulation.[7]

The AIA will also expand the exemptions from the right of access. Most significantly:

- The AIA will introduce a new exemption for information that could reasonably be expected to interfere with, prejudice or harm a workplace investigation or cause harm to a witness or third party, or prevent a witness from coming forward as a witness.[8]
- The AIA will implement a new and broad exemption for "information about the labour relations of a public body."[9]
- The exemption for advice, proposals, recommendations, analyses or policy options will be broadened to include "background factual information and information provided for informational purposes only."[10]
- The AIA will expand the mandatory exemption for cabinet confidences to include any record submitted to or prepared for the Executive Council, or any record created by or on behalf of the Executive Council;[11]

The AIA's treatment of information relating to Cabinet deliberations and decision-making is notable. The FOIP Act formerly protected Cabinet records only where they "would reveal the substance of deliberations." This meant that when assessing claims of Cabinet confidence under the FOIP Act, the Privacy Commissioner would look for evidence that Cabinet deliberated over the record in question.[12] The AIA removes this requirement.

Regarding procedural changes, public bodies will be provided with a new power to disregard requests unilaterally, and without Commissioner authorization.[13] The criteria for disregarding requests will also expand significantly under the AIA, allowing a public body to disregard requests that:

- are abusive or threatening (even if not frivolous or vexatious);
- are not sufficiently clear to enable the public body to locate and identify the record within a reasonable time with reasonable effort (after a clarification attempt has been made); and
- are overly broad or incomprehensible.[14]

The Commissioner will continue to review access decisions, but will not be permitted to compel production of some types of disputed records, including records claimed to be exempt based on any legal privilege.[15] Such claims will be determined based on attestations.

Lastly, the AIA will increase penalties for stipulated offences to a maximum of $50,000.[16]

III. Bill 33: the Protection of Privacy Act

The PPA contains several provisions addressing contemporary privacy protection challenges, including data breaches and the sale of personal information.

- The PPA will require breach notification and reporting based on the "real risk of significant harm" standard, a standard that has now become the Canadian norm. This standard has been interpreted by the Commissioner to set a relatively low threshold for notification and reporting.[17] Significant harms include harms such as identity fraud, embarrassment, and harm to reputation. A "real risk" is one that is not speculative. If notification and reporting is required, the PPA requires that reports be made "without unreasonable delay" to both the Office of the Information and Privacy Commissioner and the Minister responsible for the Act.[18] Requiring reports to the regulator and government is novel.
- The PPA will prohibit the sale of personal information "in any circumstances or for any purpose."[19] Sale is not defined.
- The PPA will allow the disclosure of personal information if the disclosure would not constitute an unreasonable invasion of personal privacy.[20] This flexible allowance, which contemplates balancing interests, does not typically apply outside of the access request context.

The PPA also features new provisions addressing modern privacy issues, including automated decision-making, data-matching, de-identification, and artificial data.

- The PPA will require public bodies to give pre-collection notice of an intent to input directly collected personal information into an "automated system to generate content or make decisions, recommendations or predications."[21] The duty is only triggered if there is an intention to use the personal information for this purpose at the time of collection. The duty to ensure personal information is accurate and complete for its purposes will apply to this novel use of personal information.[22]
- The PPA will have a prohibition on data matching to produce data derived from personal information about an identifiable individual.[23] This matching will only be permitted for "research and analysis" and "planning, administering, delivering, managing, mentoring or evaluating a program or service" unless additional allowances are implemented by regulation.[24] "Research and analysis" is not defined.
- The PPA will establish rules regarding de-identified or "non-personal data," which expressly includes "synthetic data" – "artificial data created to maintain the structure and patterns of real data without being linked to any individual in the original data set.[25] The rules will limit the creation of non-personal data to stipulated purposes, including "research and analysis" and "planning, administering, delivering, managing, monitoring or evaluating a program or service" and will require non-personal data to be created in accordance with "generally accepted best practise."[26] They will permit disclosure of non-personal data to another public body without restriction, but disclosures of non-personal data to others (including commercial entities) will be limited to specified purposes and subject to requirements that render downstream users accountable to the

disclosing public body.[27] Public bodies will also have a duty to secure non-personal data.[28]

More broadly, the PPA will require public bodies to establish and implement privacy management programs consisting of documented policies and procedures that must be made available to the Commissioner upon request.[29] It will also mandate privacy impact assessments in circumstances and in a form that will be prescribed by regulation, with submission to the Office of the Information and Privacy Commissioner also to be prescribed in some circumstances.[30]

The PPA will also create new privacy offences. Importantly, it will be an offence to re-identify or attempt to re-identify non-personal information, an offence that will enable and reduce the risks of secure de-identification.[31] Offences will carry sanctions of up to $125,000 (individuals) and $750,000 (organizations), or $200,000 (individuals) and $1 million (organizations) for certain contraventions of the data-matching, data-derived from personal information, and non-personal data regime.[32]

Conclusion

The changes to be brought in by Bills 33 and 34 are of manifest importance to the Alberta public sector. Public bodies should analyze the bills and make appropriate adjustments to their access to information and privacy protection programs. BLG provides informed advice in this area, and has a leading team of counsel with deep experience in supporting public sector entities with security incident and privacy breach management, freedom of information decision-making, appeals and judicial review applications, and all aspects of privacy management, data protection, and artificial intelligence compliance and risk management. For more information, please contact the individuals below.

Footnotes

[1] Bill 34, *Access to Information Act*, 1st Sess, 31st Leg, Alberta, 2024 (first reading 6 November 2024) [AIA].

[2] Bill 33, *Protection of Privacy Act*, 1st Sess, 31st Leg, Alberta, 2024 (first reading 6 November 2024) [PPA].

[3] Government of Alberta, "Modernizing access to information for Alberta's digital age", online: https://www.alberta.ca/modernizing-access-to-information-for-albertas-digital-age.

[4] AIA, section 1(f).

[5] AIA, section 1(k).

[6] AIA, sections 4(1)(i) and 4(1)(j).

[7] AIA, sections 4(1)(w).

[8] AIA, section 24.

[9] AIA, section 30(1)(e).

[10] AIA, section 29(1)(1).

[11] AIA, section 27(1)-(2).

[12] See for example, *Re Office of the Premier/Alberta Executive Council*, 2024 CanLII 58484, Order F2024-16, at para. 37 or *Re Alberta Environment and Protected Areas*, 2022 CanLII 122541, Order F2022-62.

[13] AIA, section 9.

[14] Ibid.

[15] AIA, section 50(6).

[16] AIA, section 95.

[17] PPA, section 10(2).

[18] Ibid.

[19] PPA, section 11.

[20] PPA, section 13(1).

[21] PPA, section 5(2).

[22] PPA, section 6.

[23] PPA, section 17.

[24] Ibid.

[25] PPA, section 1(w).

[26] PPA, section 21.

[27] PPA, section 23.

[28] PPA, section 24.

[29] PPA, section 25.

[30] PPA, section 26.

[31] PPA, section 60.

[32] PPA, section 60.

By

Daniel J. Michaluk, Matthew Schneider, Christian Halt, Sebastian Pazdan, Richard Kelba

Expertise

Cybersecurity, Privacy & Data Protection, Government & Public Sector

---

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.