Province of Alberta

PROTECTION OF PRIVACY ACT

PROTECTION OF PRIVACY (MINISTERIAL) REGULATION

Alberta Regulation 143/2025

Current as of June 11, 2025

Extract

Alberta King's Printer
Suite 700, Park Plaza
10611 - 98 Avenue
Edmonton, AB T5K 2P7
Phone: 780-427-4952

E-mail: kings-printer@gov.ab.ca
Shop on-line at kings-printer.alberta.ca

Note

All persons making use of this document are reminded that it has no legislative sanction. The official Statutes and Regulations should be consulted for all purposes of interpreting and applying the law.

(no amdt)

ALBERTA REGULATION 143/2025

Protection of Privacy Act

PROTECTION OF PRIVACY (MINISTERIAL) REGULATION

Table of Contents

High-sensitivity information

1 For the purposes of this Regulation, the following shall be deemed to be of high sensitivity:

(a) biometric information about an individual;

(b) financial information about an individual;

(c) personal information respecting a minor, senior or vulnerable individual.

Security classification levels

2(1) A public body must assign a security classification level to all personal information, data derived from personal information and non-personal data in the custody or under the control of the public body, based on an internal classification system established by the public body.

(2) The security classification level assigned to personal information must reflect the sensitivity of the personal information.

Security arrangements and validation measures

3(1) The reasonable security arrangements that a public body must make to protect personal information, data derived from personal

information and non-personal data against such risks as unauthorized access, collection, use, disclosure or destruction must be appropriate and proportional with the security classification level of that information or data.

(2) A public body must implement human oversight, auditing and validation measures for systems used for creating data derived from personal information or non-personal data to ensure the accuracy and reliability of the data.

Real risk of significant harm

4(1) In assessing under section 10(2) of the Act whether there exists a real risk of significant harm to an individual as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information, a public body must consider each of the following factors, in addition to any other relevant factors:

(a) whether there is a reasonable basis to believe that the personal information has been misused or will be misused;

(b) whether the loss of, unauthorized access to or unauthorized disclosure of the personal information occurred as a result of malicious intent;

(c) the sensitivity of the personal information that was lost or accessed or disclosed without authorization;

(d) mitigating measures taken or other factors that reduce the risk of significant harm.

(2) For the purposes of subsection (1), "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

(3) For the purposes of section 10(2)(a) of the Act, a notice to the individual for whom there exists a real risk of significant harm must

(a) be in writing, and

(b) include

(i) the name of the public body giving the notice,

(ii) a description of the circumstances of the loss of, unauthorized access to or unauthorized disclosure of the personal information,

(iii) the date on which or period during which the loss or the unauthorized access or disclosure occurred or is thought to have occurred,

(iv) the date on which the loss or the unauthorized access or disclosure was discovered,

(v) a general description of the type of personal information that was lost or that was the subject of the unauthorized access or disclosure,

(vi) a description of the steps the public body has taken to reduce the risk of harm to the individual as a result of the loss, unauthorized access to or unauthorized disclosure of the personal information,

(vii) contact information for a person at the public body who can respond, on behalf of the public body, to questions about the loss of, unauthorized access to or unauthorized disclosure of the personal information,

(viii) notice of the individual's right to request a review by the Commissioner under section 37 of the Act, and

(ix) other information the public body considers relevant.

(4) For the purposes of section 10(2)(b) of the Act, a notice to the Commissioner must

(a) be in writing, and

(b) include

(i) the name of the public body giving the notice,

(ii) a description of the circumstances of the loss of, unauthorized access to or unauthorized disclosure of the personal information,

(iii) the date on which or period during which the loss or the unauthorized access or disclosure occurred or is thought to have occurred,

(iv) the date on which the loss or the unauthorized access or disclosure was discovered,

(v) the manner in which the loss or the unauthorized access or disclosure was discovered and, if

applicable, the physical location of the loss or the unauthorized access or disclosure,

(vi) the date on which or period during which the loss or the unauthorized access or disclosure ended or is thought to have ended,

(vii) a general description of the type of personal information that was lost or that was the subject of the unauthorized access or disclosure,

(viii) a general description of the public body's assessment of the risk of harm to individuals resulting from the loss of, unauthorized access to or unauthorized disclosure of personal information,

(ix) the number of or an estimate of the number of individuals for whom there is a real risk of significant harm as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information,

(x) a description of the steps the public body has taken to reduce the risk of harm to individuals as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information,

(xi) a description of measures the public body has taken to prevent a subsequent similar loss or similar unauthorized access to or unauthorized disclosure of personal information,

(xii) an example of the notice provided under subsection (3) to an individual for whom there exists a real risk of significant harm,

(xiii) contact information for a person at the public body who can respond, on behalf of the public body, to questions from the Commissioner about the loss of, unauthorized access to or unauthorized disclosure of the personal information, and

(xiv) other information the public body considers relevant.

(5) For the purposes of section 10(2)(c) of the Act, a notice to the Minister must

(a) be in writing, and

(b) include

(i) the name of the public body giving the notice,

(ii) a description of the circumstances of the loss of, unauthorized access to or unauthorized disclosure of the personal information,

(iii) the date on which or period during which the loss or the unauthorized access or disclosure occurred or is thought to have occurred,

(iv) the date on which the loss or the unauthorized access or disclosure was discovered,

(v) a general description of the type of personal information that was lost or that was the subject of the unauthorized access or disclosure,

(vi) the number of or an estimate of the number of individuals for whom there is a real risk of significant harm as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information, and

(vii) other information the public body considers relevant.

Creation of non-personal data

5(1) When creating non-personal data under section 21(1) of the Act, a public body must establish a data quality assurance process to

(a) verify and review the effectiveness of any methods used to create the non-personal data,

(b) ensure methods used to create the non-personal data can be replicated for auditing purposes,

(c) identify and account for potential bias in the non-personal data, and

(d) ensure the accuracy and completeness of the non-personal data if the non-personal data will be used to inform decisions about programs or services.

(2) Before a public body uses or discloses non-personal data, a public body must conduct an assessment that

(a) ensures, to the extent possible, that the identity of any individual who is the subject of the non-personal data cannot be identified or re-identified from the data,

(b) identifies the security classification level of the created non-personal data, and

(c) identifies the level of risk of re-identification and security measures taken to reduce the risk.

(3) The record required by section 21(4)(d) of the Act of the assessment done to ensure that the identity of the individual who is the subject of the non-personal data cannot be identified or re-identified from the data must include the information described in subsection (2).

Privacy management programs

6(1) A privacy management program established by a public body under section 25 of the Act must include

(a) the designation or identification of a privacy officer within the public body who is responsible for ensuring the public body's compliance with the Act,

(b) internal policies and procedures to address the public body's duties under the Act, including policies and procedures for

(i) responding to

(A) requests for the correction of an individual's personal information under section 7 of the Act,

(B) incidents described in section 10(2) of the Act, and

(C) complaints made under section 38(2) of the Act,

(ii) the creation, use and disclosure of non-personal data, if the public body will create, use or disclose non-personal data, and

(iii) how automated systems will use personal information, including any security or technical safeguards that will be implemented to protect personal information, if the public body will use personal information in an automated system to generate content or make decisions, recommendations or predictions,

(c) the establishment of a security classification system for personal information, data derived from personal information and non-personal data in the custody or under the control of the public body,

(d) mandatory training for employees of the public body about the obligations of those employees under the Act,

with specified expiry periods after which retraining is required, and

(e) timelines for the periodic review, assessment and update of the privacy management program.

(2) If a public body has custody or control of a high volume of personal information or highly sensitive personal information, the public body's privacy management program must also include the following:

(a) documentation of the public body's internal privacy management structure and internal policies and procedures to address the public body's duties under the Act, which must address

(i) the roles, responsibilities and accountabilities of employees of the public body in relation to the public body's obligations under the Act,

(ii) the public body's process for completing and submitting privacy impact assessments,

(iii) the public body's policies and procedures for proactive monitoring of information systems that hold personal information, data derived from personal information or non-personal data, to assess security measures and mitigate risks,

(iv) the public body's policies and procedures related to oral, electronic and written consent, and

(v) the public body's policies related to the use of personal information in artificial intelligence systems, the creation of data derived from personal information and the creation of non-personal data, if the public body is using personal information in artificial intelligence systems, the creation of non-personal data or data matching activities;

(b) written administrative, technical and physical safeguards for managing personal information, data derived from personal information and non-personal data.

(3) Each public body must establish a process for making the public body's privacy management program available to the public on request or must make the public body's privacy management program publicly available on the public body's website.

(4) When making a public body's privacy management program available to the public, a public body may withhold technical

information, security-related information and other information that could compromise the security of personal information in the custody or under the control of the public body.

Privacy impact assessments

7(1) A public body must prepare a privacy impact assessment under section 26 of the Act with respect to a new, or a substantial change to an existing, administrative practice, program, project or service that will involve the collection, use or disclosure of personal information if one or more of the following apply:

(a) the loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm as determined in accordance with section 4;

(b) one or more of the factors requiring the submission of a privacy impact assessment to the Commissioner established by subsection (5) apply.

(2) A privacy impact assessment must

(a) include a summary of the purpose of the collection, use or disclosure of personal information for the new, or a substantial change to an existing, administrative practice, program, project or service,

(b) identify the types of personal information that will be collected, used or disclosed and reasonable security arrangements in place to protect that personal information,

(c) identify the legal authority for the collection, use or disclosure of the personal information,

(d) identify any privacy risks and mitigation strategies respecting the personal information,

(e) identify any administrative, physical or technical safeguards in place to protect the personal information, including how the personal information will be securely transmitted, matched or linked by the public body, if applicable,

(f) describe accuracy, correction and retention procedures that will be implemented to ensure the personal information is accurate and complete, and

(g) establish a clear governance structure respecting the responsibilities and accountability of each public body if 2 or more public bodies are engaging in a common or

integrated program or service or if a public body is collecting personal information from another public body under section 17(3) of the Act for the purpose of carrying out data matching.

(3) A privacy impact assessment must provide a level of detail commensurate with the complexity of the practice, program, project or service the privacy impact assessment relates to.

(4) Despite subsection (1),

(a) in the case of a substantial change to an existing administrative practice, program, project or service, if a public body has previously completed a privacy impact assessment relating to the practice, program, project or service, the existing privacy impact assessment may be amended to account for the change to the practice, program, project or service provided that the amended privacy impact assessment complies with the Act and this regulation, and

(b) in the case of a common or integrated program or service or data matching between 2 or more public bodies, the public bodies involved in the common or integrated program or service may prepare a joint privacy impact assessment and each public body must prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.

(5) A privacy impact assessment must be submitted to the Commissioner if one or more of the following factors apply:

(a) a practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity;

(b) a practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves;

(c) a practice, program, project or service will involve data matching between 2 or more public bodies;

(d) a practice, program, project or service is part of a common or integrated program or service;

(e) a practice, program, project or service involves the development or use of innovative technology;

(f) the Commissioner requests a copy of a privacy impact assessment under section 27(1)(j) of the Act.

(6) If a public body is required to submit a privacy impact assessment under subsection (5) and the Act or this Regulation requires the public body to enter into an agreement relating to the practice, program, project or service the privacy impact assessment relates to, the portions of the agreement relating to the protection of privacy must be submitted to the Commissioner together with the privacy impact assessment.

Expiry

8 For the purpose of ensuring that this Regulation is reviewed for ongoing relevancy and necessity, with the option that it may be repassed in its present or an amended form following a review, this Regulation expires on June 10, 2035.

Coming into force

9 This Regulation comes into force on the coming into force of the *Protection of Privacy Act*.

Printed on Recycled Paper