



Province of Alberta

PROTECTION OF PRIVACY ACT

PROTECTION OF PRIVACY REGULATION

Alberta Regulation 132/2025

Current as of June 11, 2025

Extract

© Published by Alberta King's Printer

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

Copyright and Permission Statement

The Government of Alberta, through the Alberta King's Printer, holds copyright for all Alberta legislation. Alberta King's Printer permits any person to reproduce Alberta's statutes and regulations without seeking permission and without charge, provided due diligence is exercised to ensure the accuracy of the materials produced, and copyright is acknowledged in the following format:

© Alberta King's Printer, 20__.*

*The year of first publication of the legal materials is to be completed.

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 132/2025

Protection of Privacy Act

PROTECTION OF PRIVACY REGULATION

Table of Contents

- 1** Interpretation
- 2** Consent
- 3** Disclosure for audit purposes
- 4** Researcher agreements
- 5** Expiry
- 6** Coming into force

Interpretation

1(1) For the purposes of the Act,

- (a) “enactment of Alberta” means an Act or a regulation or a portion of an Act or a regulation and includes a directive issued by the Treasury Board;
- (b) “imminent danger” includes a situation in which the head of a public body believes, on reasonable grounds, that
 - (i) there is a significant risk of harm to the health or safety of a person, and
 - (ii) disclosure of personal information is necessary to protect the health or safety of the person;
- (c) “reasonable security arrangements” means administrative safeguards, physical safeguards and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of a public body that
 - (i) are appropriate and proportional with the security classification level of the information or data, and
 - (ii) in the case of non-personal data, ensure, to the extent possible, that the identity of an individual who is the subject of the non-personal data cannot be re-identified from the data.

(2) For the purposes of subsection 1(c),

- (a) “administrative safeguard” means a policy, procedure or practice to manage a public body’s conduct that protects the privacy of personal information, data derived from personal information and non-personal data;
- (b) “physical safeguard” means a measure to protect a public body’s physical assets, including electronic information systems, from natural and environmental hazards and unauthorized intrusion;
- (c) “technical safeguard” means a measure to protect a public body’s electronic information and control access to it.

Consent

2(1) In this section,

- (a) “electronic” includes created, recorded, transmitted or stored in digital form or in another intangible form by electronic, magnetic or optical means or by other means that have similar capabilities for creation, recording, transmission or storage;
- (b) “electronic consent” means a consent provided by electronic means;
- (c) “electronic signature” means electronic information that an individual creates or adopts in order to sign a record and that is in, attached to or associated with the record.

(2) An individual’s consent to a public body using or disclosing any of the individual’s personal information under section 12(1)(b) or 13(1)(c) of the Act

- (a) must meet the requirements of subsection (3), (4) or (5),
- (b) must specify the personal information to which the consent relates,
- (c) must specify to whom the personal information may be disclosed and how the personal information may be used, and
- (d) must specify the date on which the consent is effective and, if applicable, the date on which the consent expires.

(3) For the purposes of this section, a consent in writing is valid if it is signed by the individual who is giving the consent.

(4) For the purposes of this section, an electronic consent is valid if

- (a) the head of the public body has established rules respecting the purposes for which electronic consent is acceptable,
 - (b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),
 - (c) the public body has explicitly communicated that it will accept electronic consent,
 - (d) the electronic consent
 - (i) is accessible by the public body so as to be usable for subsequent reference,
 - (ii) is capable of being retained by the public body,
 - (iii) can be authenticated in a manner that allows the individual giving the consent to be identified, and
 - (iv) meets the information technology standards, if any, established by the public body,
 - (e) the electronic consent includes the electronic signature of the individual giving the consent,
 - (f) the electronic consent is provided in a manner consistent with the electronic signature requirements in section 16(2) of the *Electronic Transactions Act*, and
 - (g) the association of the electronic signature with the consent is reliable for the purpose for which consent is given.
- (5)** For the purposes of this section, a consent that is given orally is valid if
- (a) the head of the public body has established rules respecting the purposes for which consent that is given orally is acceptable,
 - (b) the purpose for which the consent is given falls within one or more of the purposes set out in the rules mentioned in clause (a),
 - (c) the public body has explicitly communicated that it will accept consent that is given orally,
 - (d) the record of the consent
 - (i) is accessible by the public body so as to be usable for subsequent reference, and

- (ii) is capable of being retained by the public body,
 - (e) the public body has authenticated the identity of the individual giving consent, and
 - (f) the method of authentication is reliable for verifying the identity of the individual and for associating the consent with the individual.
- (6) For the purposes of subsection (5)(d), the record of the consent must be
- (a) an audio recording of the consent created by or on behalf of the public body,
 - (b) in the form of documentation of the consent created by an independent third party, or
 - (c) in the form of documentation of the consent created by the public body in accordance with the rules established by the head of the public body.
- (7) Notwithstanding subsections (3) to (5), the consent of a minor is not valid unless the public body has determined, on reasonable grounds, that the minor has the capacity to understand the information relevant to providing consent and appreciates the consequences of providing consent.
- (8) Despite anything to the contrary in this section, a consent under section 12(1)(b) or 13(1)(c) of the Act is no longer valid if an individual provides notice to a public body that the individual withdraws the individual's consent.
- (9) Nothing in this section requires an individual to give consent in an electronic form or orally.

Disclosure for audit purposes

3 Personal information may be disclosed to persons who are employees of a public body, including a person retained under a contract to perform services for the public body, to carry out a financial or other formal and systematic examination or review of a program, portion of a program or activity that includes personal information about individuals, provided such examination or review is sanctioned by statute, regulation or public policy relating to the public body.

Researcher agreements

4 An agreement under section 15 of the Act must include the following information and conditions:

- (a) that the person to whom the information is disclosed may use the personal information only for a research purpose set out in the agreement or for which the person has written authorization from the public body;
- (b) the names of other persons who will be given access to the personal information;
- (c) that, before disclosing personal information to persons referred to in clause (b), the person must enter into an agreement with those other persons to ensure that they will adhere to the same policies and procedures of confidentiality as described in section 15(d) of the Act;
- (d) that the person must keep the personal information in a secure location to which access is given only to the persons referred to in clause (b);
- (e) that the person must remove or destroy all individual identifiers in the personal information by the date and in the manner specified in the agreement;
- (f) that the person must not, without the prior written authority of the public body, contact an individual to whom the personal information relates, directly or indirectly;
- (g) that the person must ensure that, without the written authority of the public body, no personal information will be used or disclosed in a form in which the individual to whom it relates can be identified;
- (h) that the person must ensure that identifiable personal information about an individual is not used for an administrative purpose directly affecting the individual;
- (i) that the person must, immediately and in writing, notify the public body if the person becomes aware that a condition set out in the agreement has been breached;
- (j) that, if a person fails to meet the conditions of the agreement, the agreement may be immediately cancelled and that the person may be guilty of an offence under section 60(1) of the Act.

Expiry

5 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

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



Printed on Recycled Paper 