Privacy Management Program

1. Purpose

The Automobile Insurance Rate Board ("AIRB") has established this Privacy Management Program ("PMP") in accordance with the *Protection of Privacy Act* (the "Act). This PMP sets out AIRB's policies and procedures which promote its compliance with and duties under the Act. These policies and procedures have been established to ensure privacy is protected and to ensure alignment of the same with the requirements of the Act.

This PMP is available on AIRB's public-facing websites and will be provided within thirty (30) business days following receipt of a written request therefor in accordance with the Act.

2. Scope

This plan applies to all Employees of AIRB respecting its collection, use, disclosure, storage, creation and retention of Personal Information and Non-Personal Data in the course of its operations.

3. Definitions

"Employees" include a person who performs a service for AIRB as an appointee, volunteer or student or under a contract or agency relationship with AIRB.

"Non-Personal Data" means data, including data derived from Personal Information, that has been generated, modified or anonymized so that it does not identify any individual, and includes synthetic data and any other type of Non-Personal Data identified in the Act and its regulations.

"Personal Information" means recorded information about an identifiable individual, including

a. the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent,
b. the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
c. the individual's age, gender identity, sex, sexual orientation, marital status or family status,
d. an identifying number, symbol or other particular assigned to the individual,
e. the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
f. information about the individual's health and health care history, including information about the individual's physical or mental health,
g. information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
h. anyone else's opinions about the individual; and
i. the individual's personal views or opinions, except if they are about someone else.

4. Privacy Officer

The AIRB has a designated Privacy Officer: Heather Mack, Policy and Communications Advisor. The Privacy Officer can be contacted by email at airb@gov.ab.ca or by phone at 780-427-5428.

The Privacy Officer is responsible for ensuring compliance with the Act, including but not limited to:

a. establishing and implementing privacy controls,
b. overseeing the ongoing assessment and revision of program controls,
c. representing the AIRB in the event of a complaint investigation by the privacy commissioner's office, and
d. advocating privacy within the AIRB.

5. Collection of Personal Information

The AIRB was established through the Insurance Act as an independent, quasi-judicial regulator. The AIRB is responsible for regulating automobile insurance premiums in Alberta. The AIRB serves all Albertans – the public, industry, and government – through its functions and statutory duties and responsibilities. AIRB decisions are made independently of the government and pursuant to the AIRB's enabling legislation.

The AIRB only gathers Personal Information from individuals to the extent necessary to perform the services associated with its operations, programs and activities. AIRB shall not request or collect Personal Information unless it is reasonably necessary or directly related the AIRB's operations, programs and activities.

6. Use and Disclosure

Personal Information collected by AIRB shall only be used and disclosed:

a. to provide consumer support services including to facilitate the resolution of issues between an individual policyholder and its insurer,
b. to communicate with the individual,
c. to third parties to provide the services requested by the individual (for example, contacting an insurer on behalf of an individual in conjunction with providing consumer support services), or
d. in accordance with the Act.

If AIRB contacts an insurance company on behalf of an individual in the delivery of consumer support services, AIRB will direct the insurance company to contact its policyholder directly to resolve the inquiry or complaint raised by the policyholder with the AIRB and only to confirm resolution thereof to the AIRB.

7. Non-Personal Data

The AIRB creates Non-Personal Data for the purpose of generating reports identifying the services it provides which includes statistic on inquiries and complaints received by it. This information is used for planning, administering, delivering, managing and monitoring or evaluating the delivery of its programs, systems and services.

The AIRB shall ensure that reports containing Non-Personal Data which it intends to use or disclose in accordance with this PMP are reviewed and assessed by an Employee other than the Employee who created the report to:

a. ensure, 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.

The Privacy Officer shall from time to time:

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,
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 service.

8. Safeguards and Retention

AIRB shall categorize Personal Information and Non-Personal Data as either "Class A" or "Class B" based on the sensitivity of the information. Data which is highly sensitive will be classified as Class A with the remainder being Class B. More stringent security mechanism shall be implemented for Class A data. Access to data contained in each Class shall be limited to those Employees who need such information to perform their roles with the AIRB.

AIRB implements a combination of physical, administrative, and technical safeguards to safeguard Personal Information and Non-Personal Data as follows:

a. Physical Safeguards: Secure office spaces, locked filing cabinets, and controlled access to facilities, with access being given to only those required to access such data to perform their roles with the AIRB,
b. Administrative Safeguards: Privacy training for Employees, role-based access controls having regard to the Class of data to which an Employee requires access to perform their role with the AIRB and regular audits of privacy practices, and
c. Technical Safeguards: Encryption of data in transit and at rest, secure user authentication, firewalls, and intrusion detection systems.

All safeguards are reviewed regularly to ensure they remain effective and are updated in response to best practices, emerging threats and changes in technology.

The AIRB shall comply with the Government of Alberta's records retention and disposal guidance and schedules proposed or established by the Records and Information Management Branch. Personal Information and Non-Personal Data is retained only for as long as necessary to fulfill the purposes for which it was collected or created, as the case may be, or as may be required in accordance with legal and regulatory requirements.

9. Consent Management

The AIRB shall provide individuals with clear information about why the individual's Personal Information is being collected, how it will be used, and to whom it may be disclosed prior to the collection thereof.

10. Employee Training and Education

All Employees of AIRB are required to complete a privacy training course provided by the Government of Alberta within twelve months of the date of this PMP. Thereafter, Employees are required to complete a retraining course provided by the Government of Alberta at least one time per calendar year.

AIRB may require additional training for certain Employees if it determines such training is necessary having regard to the Employee's need to collect, use or disclose Personal Information in conjunction with the Employee's duties to AIRB.

11. Privacy Impact Assessments (PIA)

Privacy Impact Assessments (PIA's) will be conducted by AIRB when it implements a new program, system or service or substantially changes an existing program, system or service to the extent such program, system or service requires the collection, use or disclosure of Personal Information.

PIA's will be submitted to the Information and Privacy Commissioner in accordance with the Act.

12. Access and Correction

Individuals have the right to request a correction to the individual's Personal Information held by the AIRB. Upon receipt of such request, the AIRB shall as soon as reasonably possible:

a. attempt to confirm the identity of the requester, and
b. request any supporting documentation or evidence necessary for AIRB to make the requested correction.

In no event shall the AIRB correct an opinion, including a professional or expert opinion.

The AIRB shall, within a reasonable period of time following receipt of the request to correct, or if supporting documentation or evidence has been requested by the AIRB, receipt of such supporting documentation or evidence, determine whether the correction should be made. A correction shall not be made if the AIRB is unable to confirm the identify of the requester.

If no correction is made, or if no correction can be made in accordance with this PMP, the head of the AIRB shall annotate or link the Personal Information with that part of the requested correction that is relevant and material to the record in question.

On correcting the Personal Information or annotating or linkage of the same as provided in the previous paragraph, the head of the AIRB shall notify any other public body or any third party to

whom that information has been disclosed during the one year before the correction was requested that a correction, annotation or linkage has been made. Notwithstanding the foregoing, the AIRB shall not be required to issue such notification if:

a. in the opinion of the head of the AIRB, the correction, annotation or linkage is not material, and
b. the individual who requested the correction is advised and agrees in writing that notification is not necessary.

Upon receipt of a notification of a correction, annotation or linkage of Personal Information, from another public body, the AIRB shall make the correction, annotation or linkage on any record of that information in its custody or under its control.

Within thirty (30) business days after the request for correction, or any longer period allowed by the Information and Privacy Commissioner appointed under the Access to Information Act, the head of the AIRB shall give written notice to the individual that

a. the correction has been made, or
b. an annotation or linkage has been made as provided herein.

13. Complaints

An individual may make a complaint that the individual's Personal Information has been collected, used or disclosed in contravention of the Act. If the AIRB receives such complaint, the following process shall be followed:

1. The complaint shall be forwarded to the Privacy Officer.
2. The AIRB shall as soon as reasonably possible, acknowledge to the complainant, receipt of the complaint.
3. The Privacy Officer shall attempt to confirm the identity of the complainant. If the AIRB is unable to confirm the identity of the complainant, no further action shall be taken.
4. Once the identity of the complainant has been confirmed, the Privacy Officer shall review the complaint and make request to the complainant for such additional information or supporting documentation as may be reasonably required by the Privacy Officer to respond to the complaint.
5. The Privacy Officer shall use reasonable efforts to make a determination with respect to the complaint within thirty (30) days of the later of: (i) the date of the identify of the complainant has been determined; and (ii) the date the Privacy Officer is in receipt of all requested additional information and supporting documentation, if such request is made.
6. The Privacy Officer shall provide a response to the complainant in writing setting out the Privacy Officer's determination and next steps.

14. Breach Management

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure, or destruction of Personal Information. Examples include but are not limited to:

a. Lost or stolen devices containing personal information,
b. Misdirected emails or faxes,
c. Unauthorized access by employees, or
d. Cyberattacks or malware incidents.

The AIRB's Privacy Officer leads the breach response process and coordinates with:

a. IT Security,
b. Communications,
c. Legal Counsel (if required), or
d. Affected program area(s).

Breach Response Steps

Step 1: Contain the Breach

a. Immediately stop the unauthorized practice or access,
b. Secure physical or digital records,

c. Disable compromised accounts or systems, or
d. Retrieve misdirected information if possible.

Step 2: Assess the Risk

Evaluate:

(i) the type, sensitivity and Class of the Personal Information affected,
(ii) the number of individuals affected,
(iii) whether the information was encrypted or otherwise protected,
(iv) the likelihood of misuse, and
(v) the potential harm (identity theft, financial loss, reputational damage).

Step 3: Notification

If the AIRB determines that there is a real risk of significant harm to an individual as a result of the loss, unauthorized access or unauthorized disclosure, the AIRB shall give notice of the incident, without unreasonable delay, to the affected individual(s), the Information and Privacy Commissioner appointed under the Access to Information Act and the Minister responsible for the Act under Section 16 of the Government Organization Act.

The notice to the affected individual(s) shall be in writing and shall include:

a. a statement that AIRB is giving the notice,
b. a description of the circumstances of the loss of, unauthorized access to or unauthorized disclosure of the Personal Information,
c. the date on which or period during which the loss or the unauthorized access or disclosure occurred or is thought to have occurred,
d. the date on which the loss or the unauthorized access or disclosure was discovered,
e. a general description of the type of Personal Information that was lost or that was the subject of the unauthorized access or disclosure,
f. 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,
g. contact information for the Privacy Officer 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,
h. notice of the individual's right to request a review by the Commissioner under section 37 of the Act, and
i. other information the AIRB considers relevant.

The notice to the Information and Privacy Commissioner shall be in writing and shall include:

a. a statement that AIRB is giving the notice,
b. a description of the circumstances of the loss of, unauthorized access to or unauthorized disclosure of the Personal Information,
c. the date on which or period during which the loss or the unauthorized access or disclosure occurred or is thought to have occurred,
d. the date on which the loss or the unauthorized access or disclosure was discovered,
e. 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,
f. the date on which or period during which the loss or the unauthorized access or disclosure ended or is thought to have ended,
g. a general description of the type of Personal Information that was lost or that was the subject of the unauthorized access or disclosure,
h. a general description of the AIRB's assessment of the risk of harm to individuals resulting from the loss of, unauthorized access to or unauthorized disclosure of Personal Information,
i. 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,

j. a description of the steps the AIRB 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,
k. a description of measures the AIRB has taken to prevent a subsequent similar loss or similar unauthorized access to or unauthorized disclosure of Personal Information,
l. an example of the notice provided to the affected individual(s) for whom there exists a real risk of significant harm,
m. contact information for the Privacy Officer of the AIRB 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
n. other information the AIRB considers relevant.

The notice to the Minister shall be in writing and shall include:

a. a statement that AIRB is giving the notice,
b. a description of the circumstances of the loss of, unauthorized access to or unauthorized disclosure of the Personal Information,
c. the date on which or period during which the loss or the unauthorized access or disclosure occurred or is thought to have occurred,
d. the date on which the loss or the unauthorized access or disclosure was discovered,
e. a general description of the type of Personal Information that was lost or that was the subject of the unauthorized access or disclosure,
f. 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
g. other information the AIRB considers relevant.

Step 4: Investigate and Prevent Future Breaches

a. Conduct a root cause analysis,
b. Review and revise policies, procedures, and training,
c. Implement additional safeguards if needed,
d. Document lessons learned and corrective actions.

Step 5: Documentation and Reporting

All breaches, regardless of severity, must be documented in the AIRB's Privacy Breach Log, including:

a. Date and time of breach,
b. Description of incident,
c. Individuals involved,
d. Actions taken,
e. Notifications made, and
f. Follow-up measures

15. Monitoring and Review

This PMP shall be reviewed every twelve (12) months unless prior to expiry of such twelve (12) months period:

a. there is a substantial change to or replacement of the Act including any associated regulations, or
b. there is a significant change in AIRB's operations, or
c. AIRB determines that there is an increased risk surrounding its collection, use or disclosure of Personal Information,

in which event this PMP shall be reviewed at such time.

Compliance audits and privacy risk assessments shall be conducted if determined necessary by the Privacy Officer.