BSP Bureau de la Sécurité privée

Governance rules regarding personal information

Translation of the French version adopted by the Board of Directors

Resolution no RBSP/142/2026-06-11/1

June 11, 2026

BSP Bureau de la Sécurité privée

TABLE DES MATIÈRES

OBJECT

The Act respecting Access to documents held by public bodies and the Protection of personal information (CQLR, c. A-2.1) (the "**Access Act**") governs access to documents and the protection of personal information held by public bodies. Pursuant to Section 36 of the Private Security Act (CQLR, c. S-3.5) (the "**PSA**"), the Bureau de la sécurité privée (the "**BSP**") is subject to the Access Act.

In the course of its activities, the BSP is responsible for protecting and preserving the confidentiality of the personal information it collects and holds, as well as for complying with its obligations under the applicable laws.

PERSONAL INFORMATION MANAGEMENT

1. Objectives

These *Governance rules regarding personal information* (the "**Rules**") are established in accordance with Section 63.3 of the Access Act and aim to achieve the following objectives:

- Regulating the BSP's practices regarding the collection, use, disclosure, retention and destruction (the "**life cycle**") of personal information it holds, ensuring their protection and to comply with the applicable legislation.
- Providing information regarding the process for complaints regarding the protection of personal information.
- Describing the training and awareness activities offered to the BSP's personnel regarding the protection of personal information.
- Identifying the protective measures to be taken in respect to personal information collected, namely as part of a survey.
- Defining the roles and responsibilities of the members of the BSP's personnel regarding personal information.

2. Scope

The Rules apply to all members of the BSP's personnel as well as to any natural or legal person who, by contractual commitment or otherwise, within the framework of exchanges authorized by law, collects, uses, retains, discloses or destroys personal information on behalf of the BSP.

The Rules apply to all personal information that directly or indirectly allows to identify a natural person and that is collected, used, disclosed, retained or destroyed in the course of the BSP's activities, including personal information held by a third party, regardless of the medium on which it is stored.

3. Legal Context

The Rules established by the BSP regarding personal information is based on the following acts and regulations, among other:

- *Private Security Act* (CQLR, c. S-3.5) (PSA);
  - *Regulation under the Private Security Act* (CQLR, c. S-3.5, r.1);
  - *Regulation respecting the training required to obtain an agent licence to carry on private security activities* (CQLR, c. S-3.5, r.2);
  - *Regulation respecting standards of conduct of agent licence holders carrying on a private security activity* (CQLR, c. S-3.5, r.3);

- *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, c. A-2.1) (Access Act);
  - *Regulation respecting the distribution of information and the protection of personal information* (CQLR, c. A-2.1, r. 2);
  - *Regulation respecting confidentiality incidents* (CQLR, c. A-2.1, r. 3.1);
  - *Regulation respecting the confidentiality policies of public bodies that collect personal information through technological means* (CQLR, c. A-2.1, r. 4.1);

- *Act to establish legal framework for information technology* (CQLR, c. C-1.1).

It is also based on recognized practices in information governance, including those published by the Commission d'accès à l'information.

4. Guiding Principles

In addition to the legal framework, the Rules are based on the following guiding principles:

- **Responsibility**: The BSP is responsible for the personal information it holds and ensures its integrity and confidentiality.
- **Necessity**: Collection and retention limited to personal information necessary for the performance of the BPS's duties or for the implementation of programs under its responsibility. The use of personal information by the BSP'S personnel is limited to what is required to perform their duties.
- **Informed Consent**: Obtaining valid consent for personal information when required by law.
- **Accuracy**: Keeping personal information up to date, accurate and complete for the purposes for which it is collected.

- **Confidentiality**: Protection of the confidentiality of personal information held by the BSP during its life cycle, including physical, technological and administrative security measures necessary to prevent any unauthorized access, use or disclosure.
- **Transparency** : Clear communication of personal information management practices, namely through the disclosure of these Rules, and its *Privacy Policy*.

5. Governance Rules

Personal information held by the BSP is generally confidential and subject to the protection rules of the Access Act throughout its life cycle.

However, some personal information being public by the law is therefore not confidential. This is namely the case for information published in the Register of licence holders, pursuant to Sections 76 to 81 of the PSA, as well as any personal information declared public by the Access Act, subject to exceptions under the PSA.

As part of its management of personal information, throughout its life cycle, the BSP puts in place the necessary tools to comply with the applicable legal framework and guiding principles.

5.1 Collection

The BSP collects personal information that is necessary to fulfill its mission and to hire and manage its personnel.

Except in cases provided for by law, at the time of collection or at its request, the BSP informs the person concerned of the objectives for the collect of its personal information, the use that will be made of it and shares the following information:

- the name of the public body on whose behalf the information is collected;
- the purposes for which the information is collected;
- how the information is collected;
- the mandatory or optional nature of the request;
- the consequences for the person concerned or for the third party, as the case may be, for refusing to reply to the request or, if applicable, for withdrawing consent to the disclosure or use of the information collected pursuant to an optional request;
- the rights of access and correction provided for by law.

With respect to the collection of personal information, the BSP publishes on its website an *Inventaire des fichiers de renseignements personnel* (in French only) and a *Privacy Policy*.

In accordance with Section 63.4 of the Access Act and the *Regulation respecting the confidentiality policies of public bodies that collect personal information through technological means*, the BSP's *Privacy Policy* provides, among other things:

- The types of information that are collected and by what means;
- The purposes for which they are collected;
- The persons to whom they are disclosed;
- The way they are protected;
- The rights of individuals with respect to their personal information, such as the right of access, the right to rectification, the right of refusal and withdrawal, and the procedure.

5.2 Use

The BSP ensures that the personal information it retains is up to date, accurate and complete to serve the purposes for which it was collected or used.

Any use for purposes other than those originally intended, or for any other reason provided by law, must be previously authorized by the person in charge of access to documents and the protection of personal information at the BSP, who ensures that such new use is either legally permitted or that consent from the person concerned is obtained.

The BSP's personnel who use personal information in the performance of their duties must:

- limit their use strictly to purposes relating to their duties;
- respect the access rights granted to them;
- ensure confidentiality is maintained under all circumstances;
- promptly inform their immediate supervisor and the person in charge of protection of personal information of any situation where personal information confidentiality may have been compromised;
- participate in privacy awareness activities prescribed by the BSP.

5.3 Disclosure

The BSP may not disclose confidential personal information to a third party without the consent of the person concerned, given in accordance with the Access Act.

The Access Act does, however, provide for certain exceptions, including:

- In the event of an emergency threatening the life, health or safety of the person concerned (Section 59 (4) of the Access Act). In accordance with Section 59.1 of the Access Act, the terms and conditions according to which the personal information held by the BSP may be disclosed for the purpose of preventing an act of violence, including suicide attempt, are determined by internal directives.
- To the BSP attorney, or to the Attorney General, the Director of Criminal and Penal Prosecutions, if the information is necessary for the purposes of judicial proceedings or to prosecute an offence under the law (Section 59 (1) and (2) of the Access Act).
- To a person or body responsible for the prevention, detection or repression of a crime or statutory offences, if the information is necessary to prosecute an offence under a law (Section 59 (3) of the Access Act). Namely, in accordance with paragraph 2 of Section 73 of the PSA, if it appears to the Bureau's investigators, after a preliminary analysis of a complaint, that a criminal offence may have been committed, the BSP must refer the complaint to the competent police force without delay for the purpose of a criminal investigation.
- To a person or body if such disclosure is necessary for the enforcement of a law in Québec, whether or not it is explicitly provided for by law (Section 67 of the Access Act). The BSP may make such a disclosure on its own initiative, in accordance with the guidelines it has adopted for reporting an offence under a law applicable in Québec.
- To a third party, when such disclosure is necessary for carrying out a mandate or performing a contract for work or services. Any mandate or contract that requires the disclosure of personal information to a third party must be in writing and specify the provisions for the protection of personal information in accordance with Section 67.2 of the Access Act.

Except in cases specifically provided for in the policies or directives adopted by the BSP, any disclosure of personal information to a third party, without the consent of the person concerned by the information, must be previously authorized by the person in charge of access to documents and the protection of personal information at the BSP.

In accordance with Section 67.3 of the Access Act, the BSP publishes on its website a *Registre des communications de renseignements personnels* (in French only) concerning disclosures of personal information made without the consent of the concerned individual and authorized by law.

5.4 Retention

To ensure the proper retention of the personal information it holds, and solely for the necessary duration, the BSP establishes retention rules upon expiration of which the information must be destroyed.

The BSP retains personal information recorded on a physical media in premises protected by appropriate physical security measures, including an access control system.

In addition, the BSP retains personal information recorded on a technological media within environments protected by effective and evolving technological security measures appropriate to the sensitivity of some information, to reduce the risks of security incidents.

Each employee is responsible, in the performance of their duties, for managing, protecting, and judiciously classifying information according to its nature, characteristics, and value.

5.5 Destruction

The BSP ensures the secure destruction of the personal information it holds in accordance with the retention rules it establishes.

5.6 Confidentiality Incidents

All BSP personnel must promptly inform their immediate supervisor, as well as the person in charge of access to documents and the protection of personal information, of any situation they become aware of that could jeopardize the security or confidentiality of the personal information.

The management of confidentiality incidents is conducted in accordance with internal guidelines established to comply with the Regulation respecting confidentiality incidents.

5.7 Use of video surveillance

The BSP is responsible for ensuring the protection of its personnel, property and assets, including the personal information it holds. To this end, the use of surveillance cameras has been deemed essential and complementary to the other components of the integrated physical security system.

It should be noted that an individual's image is considered personal information under the Access Act as it enables their identification. Therefore, the BSP has

adopted directives on the use of video surveillance within its premises to regulate the use of this technology in a manner that balances, on one hand, employees' and visitors' rights, and on the other hand, the BSP's right to protect its organization, its assets and the information it holds, as well as its obligation to ensure the safety of its personnel and visitors.

5.8 Complaint Process Regarding the Protection of Personal Information

In the event of dissatisfaction regarding the processing of their personal information or in the exercise of their rights thereto, as described in the BSP *Privacy Policy*, any individual may address a complaint to the person in charge of protection of personal information at the BSP, whose contact information is indicated in the *Access to Information section* of the website as well as on the last page of these Rules. Any complaint will be responded to promptly.

For a complaint to be admissible, it must meet the following conditions:

- Filed by a natural person;
- Related to dissatisfaction with a practice, action or inaction of the BSP with respect to the management or protection of the personal information it holds regarding the complainant;
- Contain the surname, first name and contact information of the complainant, a sufficiently precise description of the problematic situation and the desired corrective measures.

A complaint is inadmissible if it is anonymous, abusive, frivolous, made in bad faith, contains hateful or defamatory language, is incomplete or does not relate to dissatisfaction with the protection of personal information.

If a complaint is deemed inadmissible by the person in charge of access to documents and the protection of personal information, they will inform the complainant in writing of the reasons for their decision.

If a complaint is deemed admissible, the person in charge of access to documents and the protection of personal information will acknowledge receipt of the complaint in writing and will ensure that the appropriate action is taken. Namely, they will collect all the relevant facts, analyze the complaint, determine if it is founded or not and, if so, decide on the measures to be taken.

If the complainant believes that the BSP is not fulfilling its obligations under the Access Act, they may also file a written complaint with the Commission d'accès à l'information du Québec, an administrative body whose duties include overseeing

the application of the Access Act. To do so, a complaint form is available on the website of the Commission d'accès à l'information du Québec.

5.9 Awareness and Training of the Personnel

In addition to the security measures set out in relation to the use and retention of personal information as well as the management of confidentiality incidents, the BSP provides training and awareness in the areas of private life, protection of personal information and cybersecurity, to each of its employees who may have access to personal information.

Namely, a mandatory virtual training on the protection of personal information is offered to its personnel. This training must be taken at the time of hiring and thereafter, annually. Basic cybersecurity training must be taken regularly by all personnel.

5.10 Privacy Impact Assessment

The BSP has developed tools to conduct any Privacy Impact Assessment ("**PIA**") when required by the Access Act, to identify and mitigate privacy risks, namely:

- From the start of any project to acquire, develop and overhaul an information system or electronic service delivery system involving the collection, use, disclosure, retention or destruction of personal information (Section 63.5 of the Access Act);
- Before collecting personal information necessary for the exercise of its rights and powers or for the implementation of a program of the public body with which it cooperates to provide services or to pursue a common mission, within the framework of a written agreement sent to the Commission d'accès à l'information (Section 64 of the Access Act);
- Before disclosing personal information without the consent of the persons concerned to a person or body that wishes to use the information for study or research purposes or for the production of statistics (Section of the Access Act);
- Prior to the disclosure of personal information that is necessary for the provision of a service to the person concerned (the disclosure is made pursuant to a written agreement) (Section 68 of the Access Act);
- Before disclosing personal information outside Québec (Section 70.1 of the Access Act).

5.11 Protective Measures Specific to Survey

Before collecting personal information as part of a survey, the BSP must conduct an assessment of the need to use it in light of its mission as well as an evaluation of the ethical aspect of the survey, taking into account, in particular, the nature of the survey and the persons concerned, the sensitivity of the personal information collected and the purposes for which it is to be used.

6. Roles and Responsibilities

To ensure the protection of personal information within the BSP, namely compliance with the Rules, the following stakeholders are assigned the following roles and responsibilities:

6.1 Executive Director

As the highest authority within the BSP, the Executive Director ensures compliance and implementation of the provisions of the Access Act within the BSP. More specifically, they:

- Ensure to facilitate the performance of the duties provided under the Access Act delegated to the person in charge of access to documents and the protection of personal information;
- Preside on the Committee on Access to Information and the Protection of Personal Information ("**AIPPI Committee**");
- Allocate resources and ensures that budgets and the material and technological tools are sufficient to protect personal information;
- Determine, in collaboration with the AIPPI Committee, in the event of a data leak or unauthorized access, whether the incident poses a "risk of significant harm" to the individuals involved;
- Endorse or reject the recommendations made by the AIPPI Committee regarding any proposed addition or modification of video surveillance systems for the BSP premises.

At the BSP, the Executive Director's duties relating to access to documents and protection of personal information are delegated to the person holding the title of Director of Legal Affairs.

6.2 Committee on Access to Information and the Protection of Personal Information

The AIPPI Committee reports to the Executive Director and is composed, in addition to the latter, of the person in charge of access to documents and the protection of personal information, the person responsible for information security, the person responsible for the premises physical security, the person responsible for document management and the person responsible for licence treatment and information. Depending on the needs, the AIPPI Committee may be joined by other collaborating members.

This committee is responsible for supporting the person in charge of access to documents and the protection of personal information in carrying out their responsibilities and fulfilling their obligations under the Access Act. Its members collaborate in the implementation of measures to ensure proper protection of personal information. More specifically, the AIPPI Committee:

- Performs the duties assigned by the Access Act;
- Approves and publishes these Rules;
- Evaluates the internal process for managing confidentiality incidents, conduct post-mortem and makes recommendations in this matter;
- Ensures the awareness and training of the personnel regarding the access to documents and the protection of personal information;
- Ensures that PIAs are carried out for any project for which it is required by the Access Act and suggests, if necessary, specific protection measures;
- Analyzes any request for the installation or modification of a video surveillance system for the BSP's premises;
- Publishes on the BSP's website, the documents and information covered by the *Regulation respecting the distribution of information and the protection of personal information*, and includes a report attesting to the distribution of the documents in the BSP's annual report;
- Proactively distributes the information of interest to the public (open data).

6.3 Person in Charge of Access to Documents and the Protection of Personal Information

Under the powers and duties delegated to them by the Executive Director, the persons in charge of access to documents and the protection of personal information shall:

- Ensure compliance with the BSP's rights and obligations regarding the collection, use, retention, disclosure and destruction of personal and confidential information;
- Advise the Executive Director, namely with respect to the governance framework related to the protection of personal information within the BSP;
- Oversee the application of these Rules and the governance framework related to the protection of personal information within the BSP;
- Sit on the AIPPI Committee;
- Support the work of the AIPPI Committee, ensuring the implementation of its orientations and the execution of its decisions;
- Process requests for access to administrative documents and personal information or to correction of personal information, in accordance with the requirements of the Access Act and other applicable legislation;
- Make decisions on access to documents and personal information or correction of personal information;
- Manage confidentiality incidents;
- Record in the BSP annual report, with the approval of the Executive Director, relevant statistics on requests for access to documents and personal information and on requests for rectification of personal information, in addition to reporting on the activities carried out in this regard;
- Receive complaints of dissatisfaction with the handling of personal information.

6.4 Managers

Managers are responsible for the protection of personal information held by the personnel in their departmental. As such, they:

- Ensure compliance with these Rules within their respective departments;
- Ensure that personnel under their responsibility use secure means to collect, use, disclose, retain or destroy personal information;
- Take appropriate measures in the event of a breach of these Rules by a personnel member under their responsibility;
- Raise awareness of the importance of protecting personal information, in collaboration with the person in charge of access to documents and the protection of personal information;
- Collaborate with the person in charge of access to documents and the protection of personal information in managing any request or complaint, or

any confidentiality incident, concerning personal information that directly or indirectly involves their department.

6.5 Person responsible for document management

The person responsible for document management ensures the organization and management of information within the BSP, whether in paper or digital format. As part of their duties, they:

- Manage documents from their creation, or receipt, to their final archiving or destruction;
- Organize the filing of documents, namely the establishment and administration of an electronic document management system;
- Ensure that documents are accessible only to authorized persons, namely by implementing restricted and secure access rights;
- Identify documents containing personal information, in collaboration with the person in charge of access to documents and the protection of personal information;
- Ensure, in collaboration with the person in charge of access to documents and the protection of personal information, the secure destruction or irreversible anonymization of documents containing personal information in accordance with the retention rules that the BSP establishes.

6.6 Members of the personnel

The BSP's personnel must ensure compliance with the Rules and any administrative tools adopted by the BSP or its management related to the protection of personal information.

In addition, they must immediately forward any request or complaint they receive related to the Access Act to the person in charge of access to documents and the protection of personal information.

Moreover, they must report any confidentiality incident that they may have become aware of in the course of their duties.

7. Coming Into Force

These Rules, duly approved by the AIPPI Committee on May 20, 2026, come into force on the day of their adoption by the Board of Directors on June 11, 2026.

In accordance with Section 63.3 of the Access Act, they are published on the BSP website.

For any questions about the Governance Rules Regarding Personal Information, please contact:

Me Isabelle F. LeBlanc,

Person in charge of access to documents and the protection of personal information

Bureau de la sécurité privée

1611 Crémazie Boulevard East, suite 500

Montréal (Québec) H2M 2P2

Toll free: 1 877 748-7483

Email: **aiprp@bspquebec.ca**