

PROVINCE OF QUÉBEC

MUNICIPALITY OF KAZABAZUA

MRC DE LA VALLÉE DE LA GATINEAU

ADMINISTRATIVE POLICY CONCERNING THE RULES OF GOVERNANCE FOR THE PROTECTION OF PERSONAL INFORMATION OF THE MUNICIPALITY OF KAZABAZUA

WHEREAS the Municipality of Kazabazua (hereinafter the "Municipality") is a public body subject to the Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR c. A-2.1 (hereinafter the "Access Act");

WHEREAS the Municipality undertakes to protect the personal information it collects and processes in the course of its activities in compliance with applicable laws and regulations;

WHEREAS in 2022, the Municipality employed, on average, 50 employees or less, and that it is therefore not subject to the obligation to establish a committee on access to information and the protection of personal information in accordance with the Regulation excluding certain public bodies from the obligation to form a committee on access to information and the protection of personal information;

WHEREAS in order to fulfil the obligations set out in the access act, this administrative policy on privacy governance rules is hereby established.

THEREFORE, IT IS PROPOSED by Damien Lafrenière, **SECONDED** by Paul Chamberlain and resolved that the council decreets as follows:

CHAPITRE I — APPLICATION AND INTERPRETATION

1. DEFINITIONS

For the purposes of this policy, the following expressions or terms have the following meanings:

CAI: Refers to the Commission d'accès à l'information established under the Access Act;

Council: Refers to the municipal council of the Municipality of Kazabazua;

Life cycle: Refers to all stages of existence of information held by the Municipality and more specifically its creation, modification, transfer, consultation, transmission, conservation, archiving, anonymization or destruction;

Access Act: Refers to the Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR v. A -2.1;

Concerned person: Refers to any natural person for whom the Municipality collects, holds, communicates to a third party, destroys or anonymizes, one or more personal information;

Stakeholder: Refers to a natural person in relation to the Municipality in the context of its activities and, without limiting the generality of the foregoing, an employee or supplier;

PRP Governance Policy: Refers to the administrative policy concerning the Municipality's privacy governance rules;

PRP: Refers to the protection of personal information;

Personal information (or PI): Refers to any information that relates to a natural person and that allows him to be directly or indirectly identified, such as: postal address, telephone number, email or bank account number, whether personal or professional data of the individual;

Sensitive Personal Information (or PI): Means any personal information that gives rise to a reasonable expectation of privacy for any individual, including because of the potential harm to the individual in the event of a privacy incident, such as financial information, medical information, biometrics, social insurance number, driver's licence number or sexual orientation;

Responsible for access to documents (or RAD): Refers to the person who, in accordance with the Access Act, exercises this function and responds to requests for access to documents from the Municipality;

Privacy Officer (or RPRP): Refers to the person who, in accordance with the Access Act, exercises this function ensures the protection of personal information held by the Municipality.

2. OBJECTIVES

The objectives of the PRP Governance Policy are to:

- State guidelines and guiding principles for effective PRP;
- Protéger les RP recueillis par la Municipalité tout au long de leur cycle de vie ;
- Ensure compliance with legal requirements applicable to the PRP, including the Access Act, and best practices in this area;
- Ensure public confidence in the Municipality, be transparent about the processing of PRI and PRP measures applied by the Municipality and provide access to them when required.

CHAPITRE II — MEASURES TO PROTECT PERSONAL INFORMATION

3. COLLECTION OF PERSONAL INFORMATION

- 3.1. The Municipality only collects the PI necessary for the purposes of its activities.
- 3.2. Subject to the exceptions provided for in the Access Act, the Municipality does not collect PI without first obtaining the consent of the person concerned.
- 3.3. It is understood that consent must be given for **specific purposes**, for a **period necessary** to achieve the purposes for which it is requested. The consent of the data subject must be:
 - a) **Manifesto**: which means that it is obvious and certain;
 - b) **Free**: which means that it must be free of constraints;
 - c) **Enlightened**: which means that he is taken with full knowledge of the facts.
- 3.4. At the time of collection of any PI, the Municipality makes sure to expressly obtain the free and informed consent of the person concerned. In particular, the Municipality must indicate:
 - The purposes for which any PI is required;
 - The mandatory or optional nature of the request to collect PI;
 - The consequences for the data subject of a refusal to respond to the request;

- The consequences for the data subject of withdrawing consent to the disclosure or use of PI following an optional request;
- The rights of access and rectification to the PI collected;
- The means by which any PI is collected;
- The necessary details relating to (1) the use by the Municipality of a technology to collect any PI, including functions that allow the identification, location or profiling of the person concerned and (2) the means offered to the person concerned, to activate or deactivate the functions;
- Details of the retention period of any PI;
- Contact information of the person responsible for the PRP within the Municipality.

4. CONSERVATION AND UTILISATION OF PERSONNEL INFORMATIONS

- 4.1. The Municipality restricts the use of any PI to the purposes for which it was collected and for which the Municipality has obtained the express consent of the person concerned, subject to the exceptions provided for in the Access Act.
- 4.2. The Municipality limits access to any PI held only to persons for whom such access is required for the exercise of their functions within the Municipality.
- 4.3. The Municipality applies equivalent security measures, regardless of the sensitivity of the PI detainees to prevent breaches of their confidentiality and integrity subject to the exceptions provided for in the Access Act.
- 4.4. The Municipality retains data and documents containing PI:
 - a) for the time necessary for the use for which they were obtained
 - or**
 - b) in accordance with the deadlines set out in its retention schedule.
- 4.5. When using any PI, the Municipality ensures the accuracy of the PI. To do this, it validates its accuracy with the person concerned on a regular basis and, if necessary, at the time of its use.
- 4.6. The Municipality places the same reasonable high expectation of protection, confidentiality and integrity with respect to any PI it collects, retains and uses whether the PI is sensitive or not.

5. PERSONAL INFORMATION FILE

The Municipality establishes and maintains an inventory of its personal information banks.

This inventory must contain the following information:

- a) the identification of each bank, the categories of information it contains, the purposes for which the information is retained and how each bank is managed;
- b) the source of the information contained in each bank;
- c) the categories of persons to whom the information in each bank relates;
- d) the categories of persons who have access to each file in the performance of their duties;

- e) the security measures taken to ensure the protection of personal information.

Any person who so requests is entitled to access the inventory, except in respect of information whose existence may be refused under the provisions of the Access Act.

6. DISCLOSURE TO THIRD PARTIES

- 6.1. The Municipality may not communicate to third parties any PI without the express consent of the person concerned, except as provided for in the Access Act.
- 6.2. The Municipality indicates, in the registers required by the Access Act, all information relating to the transmission of any PI to a third party for any purpose whatsoever.

7. DESTRUCTION OR ANONYMIZATION

- 7.1. When PI is no longer necessary for the purposes for which it was collected and when the period provided for in the retention schedule has expired, the Municipality must irreversibly destroy it or make it anonymous.
- 7.2. *The destruction procedure must be approved by the clerk-treasurer and the RPPR to ensure compliance with article 199 of the Municipal Code.*
- 7.3. Anonymization has a serious and legitimate end and the procedure is irreversible.
- 7.4. *On the recommendation of the RPPR, any anonymization procedure must be approved by the Clerk-Treasurer.*

CHAPTER III — ROLES AND RESPONSIBILITIES WITH REGARD TO THE PROTECTION OF PERSONAL INFORMATION

8. COUNCIL

The Council approves this Policy and ensures its implementation, including ensuring:

- a) To make the necessary decisions within its jurisdiction to see to the implementation and compliance with this Policy;
- b) That the Municipality's general management and department heads promote an organizational culture based on the protection of PI and the necessary behaviours to avoid any confidentiality incidents;
- c) That the RPP and the FDR be able to exercise their powers and responsibilities autonomously.

9. GENERAL DIRECTION

The general management is responsible for the quality of the management of the PRP and the use of any technological infrastructure of the Municipality for this purpose.

In accordance with the Regulation excluding certain public bodies from the obligation to form a committee on access to information and the protection of personal information (Decree 744-2023, May 3, 2023), the General Management assumes the tasks devolved to the Committee on Access to Information and the Protection of Personal Information:

- a) Define and approve the rules of governance for the protection of personal information (PRP) within the Municipality;

- b) Define and approve the orientations for PRP within the Municipality;
- c) Formulate opinions on initiatives to acquire, deploy and redesign information systems or any new electronic delivery of services by the Municipality requiring the collection, use, retention, communication to third parties or destruction of PI, both at the time of the implementation of these initiatives and at the time of any modification to them. »

In this regard, it shall implement this Policy by:

- a) Ensuring that the RPP and FSC can autonomously exercise their powers and responsibilities;
- b) Ensuring that PRP values and orientations are shared and conveyed by all managers and employees of the Municipality;
- c) Providing the necessary financial and logistical support for the implementation and compliance with this policy;
- d) Exercising its investigative power and applying sanctions appropriate to the circumstances for non-compliance with this Policy;

10. RESPONSIBLE PROTECTION OF PERSONNEL INFORMATIONS

The Privacy Officer (PIO), in collaboration with the FDR, contributes to the sound management of PRP within the Municipality. It supports Council, General Management and all Municipality staff in the implementation of this Policy.

In particular, the RPRP ensures that:

- a) Define, in collaboration with the general management, the orientations for PRP within the Municipality;
- b) Determine the nature of the personal information (PI) to be collected by the various departments of the Municipality, its retention, its communication to third parties and its destruction;
- c) Suggest the necessary adaptations in the event of amendments to the Access Act, its related regulations or the interpretation of the courts, if applicable;
- d) Plan and ensure, in collaboration with the General Management, the implementation of training activities for the Municipality's employees in the area of PRP;
- e) Provide advice to the Executive Director on initiatives for the acquisition, deployment and redesign of information systems or any new electronic delivery of services by the Municipality requiring the collection, use, retention, communication to third parties or destruction of PI, both at the time of the implementation of these initiatives and at the time of any modification to them;
- f) Advise on specific measures to be taken with respect to surveys that collect or use PI, or with respect to video surveillance;
- g) Ensure that the Municipality is aware of the orientations, directives and decisions made by the Commission d'accès à l'information (CAI) with respect to PRP;
- h) Assess, in collaboration with the General Manager, the level of PRP within the Municipality;
- i) Recommend to the Clerk-Treasurer to proceed with the anonymization of PI instead of the destruction of PI that is no longer useful to the Municipality;
- j) Report to the Board and Executive Management, on an annual basis, on the application of this policy.

11. PERSON RESPONSIBLE FOR ACCESS TO DOCUMENTS

As part of this function, the compliance officer must:

- a) Receive all requests that are of the nature of a request for access to documents within the meaning of the Access Act, including requests for information;
- b) Responding to applicants for access to records based on the requirements of the Access Act.

12. SERVICE DIRECTOR

Each department head is responsible for ensuring the PRP within the department he or she directs as well as the technological infrastructure necessary for this purpose to which he and the department's employees have access as part of their duties at the Municipality.

As such, each department head must:

- a) Make this PRP policy known to employees in your department and ensure its application and compliance by them;
- b) Ensure that the security measures determined and put in place are systematically applied during his employment and that of the employees he directs in the department for which he is responsible;
- c) Participate in raising awareness among each employee on their team about PRP issues;
- d) Designate, within its department, the employee(s) whose task specifically includes the functions of ensuring the collection, holding, retention or destruction of PI and its protection;
- e) Where no employee is designated, the department head shall assume the tasks and responsibilities provided for in section 13.

13. PERSON IN CHARGE OF PRP IN THE VARIOUS MUNICIPAL DEPARTMENTS

Each department head of the Municipality must identify the person responsible for PRP within his or her RPRP department. The employees of each department of the Municipality so designated are responsible within their department for certain stage of the life of PI, that is, collection and detention.

Each head within a unit mentioned above works closely with the RPRP to identify the various categories of PI collected, held, communicated to third parties, if applicable, destroyed or anonymized and to maintain this inventory. The person in charge must also ensure that employees of the service obtain any consent required from any individual for the purpose of collecting, holding or transferring to third parties as appropriate. The person in charge must see to the retention and classification of the consents collected in such a way that they can be easily traced.

14. EMPLOYEES

Each employee must:

- a) Take all necessary measures to protect PI;
- b) Make every effort to comply with the applicable legal framework and the measures provided for in the various policies and directives of the Municipality in relation to the protection of PI;

- c) Access only the PI necessary in the performance of his/her duties;
- d) Report any confidentiality incidents or improper handling of PI to the PRP;
- e) Actively participate in any awareness or training activities given on PRP;
- f) Working with RPRP and RAD.

15. PRIVACY TRAINING FOR MUNICIPAL STAFF

The RPP establishes the content and selection of training offered to all employees of the Municipality and determines the frequency with which employees must take any established training.

Training or awareness-raising activities include, in particular:

- Hiring training on the importance of PRP and the actions to take in your work;
- Training to all employees on the implementation of this policy;
- Training for employees using a new IT tool involving PI;
- Training on updates to this policy or PI security measures, if applicable;

CHAPTER IV — ADMINISTRATIVES MEASURES

16. SURVEYS

Before conducting, or allowing a third party to conduct a survey of affected persons for whom the Municipality holds, collects or uses PI, the RPP must first make an assessment of the following points:

- the need for the use of the survey;
- the ethical aspect of the survey, taking into account, in particular, the sensitivity of the personal information collected and the purpose for which it was used.

Based on this assessment, the RPP will be required to make recommendations to the Board and Branch.

17. ACQUISITION, DEVELOPMENT OR OVERHAUL OF AN INFORMATION OR ELECTRONIC DELIVERY SYSTEM

17.1. Before acquiring, developing or redesigning PI management systems, the Municipality must conduct a Privacy Impact Assessment.

For the purposes of this assessment, the Municipality must consult, at the beginning of the project, its PRP.

17.2. As part of the implementation of the project provided for in section 17.1, general administration may, at any stage, suggest measures to protect PI, including, but not limited to:

- a) the appointment of a person responsible for the implementation of PRP measures;
- b) PRP measures in any project document, such as specifications or contracts;
- c) a description of the PRP responsibilities of project participants;
- d) conducting PRP training activities for project participants.

- 17.3. The Municipality must also ensure that, as part of the project provided for in section 17.1, the personal information management system allows a computerized PI collected from the person concerned to be communicated to the latter in a structured and commonly used technological format.
- 17.4. The conduct of a Privacy Impact Assessment must be proportionate to the sensitivity of the information concerned, the purpose of its use, its quantity, its distribution and its medium.

18. CONFIDENTIALITY INCIDENTS

Unauthorized access, use or disclosure of any PI or its loss constitutes a confidentiality incident within the meaning of the Access Act.

The Municipality shall manage any confidentiality incident in accordance with the confidentiality incident management procedure, which includes the following rules:

- Any actual or potential privacy incident must be reported to the RPP as soon as possible by anyone who becomes aware of it;
- The RPP must review the reported information to determine if it is a confidentiality incident and if so:
 - Enter relevant information in the Municipality's Privacy Incident Registry;
 - Notify the CAI and any person concerned by the confidentiality incident;
 - Identify and recommend the application of appropriate mitigation measures, if necessary.

19. COMPLAINTS HANDLING

Any natural person who believes that the Municipality does not ensure the protection of PI in a manner consistent with the Access Act may file a complaint as follows:

- 19.1. A complaint can only be considered if it is made in writing by a natural person who identifies himself.
- 19.2. Such request is addressed to the RPRP of the Municipality.
- 19.3. The RPRP notifies the applicant in writing of the date of receipt of the complaint and indicates the time limits for its response.
- 19.4. The RPRP responds to a complaint promptly and no later than twenty days from the date of receipt.
- 19.5. If the processing of the complaint within the time limit set out in section 19.4 of this Policy seems impossible to comply with without interfering with the normal conduct of the Municipality's activities, the RPRP may, before the expiry of this period, extend it by a reasonable period and give notice to the applicant, by any means of communication allowing the applicant to be contacted.
- 19.6. As part of the complaint process, the RPRP may contact the complainant and conduct an internal investigation.
- 19.7. At the end of the examination of the complaint, the RPRP sends the complainant a final written and reasoned response.
- 19.8. If the complainant is not satisfied with the response received or the handling of his complaint, he may contact the CAI in writing.


20. SANCTIONS

Any employee of the Municipality who contravenes this Policy or the laws and regulations in force applicable to RPP is liable, in addition to the penalties provided for in the laws, to disciplinary action that may lead to disciplinary action and up to and including dismissal. The Director-General, together with the Human Resources Department, is responsible for deciding whether to apply the appropriate sanction, if necessary. The Municipality may also transmit to any judicial authority the information collected on any employee, which suggests that an offence under any of the laws or regulations in force regarding PRP has been committed.

21. FINAL DISPOSITION

This policy is effective immediately upon adoption by the Council.

Robert Bergeron
Mayor



Pierre Vaillancourt
Directeur general and clerk-treasurer

Adoption of the policy: October 3, 2023

Modificationn of the policy: November 7, 2023 Resolution number 2023-11-222