CONFIDENTIALITY OF THE MUNICIPAL LIST OF ELECTORS

Guide for candidates, authorized political parties and recognized tickets

DGE-1004.2-VA (21-08)

élections Québec

TABLE OF CONTENTS

INTRODUCTION

Persons who receive information contained in a municipal list of electors[1] must take the necessary measures to ensure the confidentiality and security of that information.

This document aims to inform candidates, authorized political parties and recognized tickets about the provisions of the *Act respecting elections and referendums in municipalities* (CQLR, c. E-2.2 [AERM]) governing the use and disclosure of information contained in lists of electors, as well as to raise awareness of good practices related to confidentiality. Representatives of qualified voters who obtain a copy of the referendum list may also use this document.

This document is available on the Élections Québec website (electionsquebec.qc.ca).

The general information and measures presented in this guide do not take precedence over the provisions of the AERM. When interpreting or applying the AERM, you should always refer to the text published by the Éditeur officiel du Québec, which is available at the following address : legisquebec.gouv.qc.ca.

If you have questions or comments about this document or the recommended measures for protecting the confidentiality of information relating to electors contained in lists of electors, please contact the returning officer, the clerk or the secretary-treasurer of the municipality.

1. In this document, “list of electors” refers to the list of electors or the referendum list of a municipality, as well as the list of qualified voters entitled to have their names entered on a referendum list.

CONFIDENTIALITY OF THE INFORMATION CONTAINED IN THE LIST OF ELECTORS

The list of electors contains personal information relating to electors. This information is confidential, under the AERM. It includes :

- Each elector's surname and given name;
- His or her domiciliary address;
- His or her date of birth;
- His or her sex.

Any other information relating to an elector on a list of electors is also confidential. This includes :

- The line number corresponding to an elector;
- The fact that an elector's name has been struck off;
- The fact that an elector voted and the voting method he or she used.

Furthermore, the list of electors may indirectly reveal additional information relating to electors. For example, it can be used to identify older women or women living alone, same-sex couples and young adults still living with their parents, along with other details regarding the lifestyles or personal choices of electors.

SENDING OF THE LIST OF ELECTORS TO CANDIDATES, AUTHORIZED POLITICAL PARTIES AND RECOGNIZED TICKETS

The AERM provides that candidates, authorized political parties and tickets may obtain a copy of the list of electors in the situations described below.

Candidate for the seat of mayor

Every candidate for the seat of mayor is entitled to obtain, on request, up to five copies of the list of electors of the municipality (s. 106).

Where a person has previously requested the list of electors, the returning officer will also provide the same number of copies of the revised list or of the abstract of changes made to the list as a result of the revision process (s. 139).

Candidate for the seat of councillor

Every candidate for the seat of councillor for an electoral district or a ward is entitled to obtain, on request, up to five copies of the list of electors of the district or ward (s. 106).

Every candidate for the seat of councillor of a municipality whose territory is not divided for election purposes is entitled to obtain, on request, up to two copies of the list of electors of the municipality (s. 106).

Where a person has previously requested the list of electors, the returning officer will also provide the same number of copies of the revised list or of the abstract of changes made to the list as a result of the revision process (s. 139).

Authorized political party or recognized ticket

Not later than the 23rd day before polling day, the returning officer must send a copy of the list of electors to each authorized political party or recognized ticket (s. 109).

The returning officer will also provide them with a copy of the revised list or of the abstract of changes made to the list as a result of the revision process (s. 139).

List of electors registered to vote at a mobile polling station

The returning officer must send a copy of the list of electors having applied to vote at a mobile polling station to each authorized political party or recognized ticket that requests it and to each independent candidate who requests it (s. 175).

List of electors having voted in an advance poll

Not later than the third day before polling day, the returning officer must send a copy of the list of electors who have voted in an advance poll to each authorized political party or recognized ticket that requests it and to each independent candidate who requests it (s. 184).

USE AND DISCLOSURE OF INFORMATION CONTAINED IN THE LIST OF ELECTORS

The AERM (s. 659.1) prohibits any person from using information contained in a list of electors for any purpose other than those set out in the legislation.

The AERM also prohibits any person from disclosing or allowing the disclosure of such information for any purpose not provided for in the legislation. Furthermore, it also prohibits any person from disclosing or allowing the disclosure of such information to anyone not legally entitled to it.

The AERM (ss. 631 and 639) provides that a natural person is liable to a fine of between $500 and $4,000 if he or she uses, discloses or allows the disclosure of information contained in a list of electors in contravention of the legislation. Fines for legal persons range from $1,500 to $12,000.

The following table aims to help candidates, political parties and tickets better understand the scope of these restrictions. It outlines the purposes for which they may use information contained in the list of electors.

Use of Information Relating to Electors

Authorized recipients	Permitted use
Authorized political parties	• Communicating with electors • Recruiting members • Soliciting support • Promoting voter turnout • Recruiting volunteers or campaign staff • Soliciting political contributions*
Recognized tickets (during the election period)	• Communicating with electors • Soliciting support • Promoting voter turnout • Recruiting volunteers or campaign staff
Candidates (during the election period)	• Communicating with electors • Soliciting support • Promoting voter turnout • Recruiting volunteers or campaign staff • Soliciting political contributions*

** Contributions may only be solicited by the official representative or a person designated by the official representative for that purpose. Solicitation may continue until the candidate's authorization expires.*

Candidates, political parties and tickets may share information relating to electors with volunteers and staff members, as well as with service providers. The latter must use such information for the purposes set out in the AERM while acting as a mandatary of the candidate, political party or ticket.

Volunteers and staff members

Before entrusting volunteers or staff members with information relating to electors, candidates, political parties and tickets must ensure that the information will only be shared with persons who require it to carry out their duties. Limiting the number of people with access to information relating to electors reduces the risk of a confidentiality breach.

Furthermore, persons receiving information relating to electors must be informed of the confidential nature of the information, the limitations on its use and the penalties applicable in the case of a confidentiality breach.

More specifically, such persons should be aware that :

- They may not access or use information relating to electors for personal reasons or purposes not provided for in the AERM;
- They may not disclose information relating to electors to anyone, unless instructed to do so by the candidate, political party or ticket, in accordance with the AERM;
- They must ensure the security of information relating to electors at all times;
- They must return any documents containing information relating to electors once they have finished using the information. They may also securely destroy the information, under the guidance of the candidate, political party or ticket.

Any person provided with information relating to electors should sign a confidentiality undertaking form (Appendix 2).

Sharing the list of electors with service providers

Prior to entrusting a service provider with information relating to electors, especially by electronic means, candidates, authorized political parties and tickets should have the service provider sign a confidentiality undertaking form. The confidentiality undertaking form provided in Appendix 3 may be used for this purpose.

The form aims to inform service providers regarding the confidential nature of information relating to electors, the restrictions on its use and the applicable provisions of the AERM.

The service provider should limit the disclosure and use of information relating to electors to the mandate given by the candidate or by the leader of the party or ticket. The latter should take appropriate measures to ensure that the service provider complies with the terms of the undertaking, where applicable; in particular, the service provider should not retain any information relating to electors beyond the term of the mandate. The service provider’s mandate must comply with the purposes set out in the AERM.

Withdrawal of nomination, authorization or recognition

A candidate who withdraws his or her nomination, a political party whose authorization is withdrawn or a ticket whose recognition is withdrawn must provide the returning officer with any copies of the list of electors that the candidate, the party or the ticket has received (ss. 108 and 109).

Any natural person who fails to return these documents is liable to a fine of between $ 500 and $ 4,000 (ss. 632 and 639).

RECOMMENDED SAFEGUARDS

Candidates, political parties and tickets must implement safeguards to ensure the protection and confidentiality of any information relating to electors that is entrusted to them.

Élections Québec recommends adopting the following measures. Candidates, political parties and tickets may adapt or implement additional safeguards to ensure the protection and confidentiality of the information for which they are responsible.

Officer responsible for the protection of personal information

Élections Québec recommends that candidates, political parties and tickets designate an officer responsible for ensuring the protection of information relating to electors. This person should oversee the implementation of the recommended safeguards. Candidates and the leaders of parties or tickets may choose to personally assume this responsibility.

In particular, the officer should be responsible for authorizing volunteers and staff members to receive and use information relating to electors, as well as for drawing their attention to the confidential nature of such information.

Policy on the protection of personal information

Élections Québec recommends that candidates, political parties and tickets using information relating to electors adopt a policy on the protection of personal information. Such a policy constitutes a commitment to electors regarding the protection of personal information. It should be available to electors upon request and inform them of the measures implemented to ensure the confidentiality of their personal information.

Candidates may choose to be subject to the policy adopted by their party or ticket, where applicable.

A policy template for the use of candidates is provided in Appendix 4. A policy template for the use of political parties and tickets is provided in Appendix 5.

Disclosure log

Élections Québec recommends that candidates, political parties and tickets maintain a disclosure log for information relating to electors, in addition to signing a confidentiality undertaking. Such a log should record the name of the person receiving the information, the date of disclosure and the means of communication. It should also provide confirmation that the documents were returned or securely destroyed, or that electronic access rights were revoked, where applicable.

Élections Québec provides candidates, political parties and tickets with a disclosure log template they can use for this purpose (Appendix 6).

Information security in a mobile environment

Candidates, political parties and tickets may handle information relating to electors using mobile technology or applications. In addition, they may handle such information in public places. They therefore need to exercise caution in order to reduce the risk of a confidentiality breach involving information relating to electors. That is why Élections Québec recommends implementing the following security measures. These measures will help ensure confidentiality, regardless of the format used to store the information.

Retaining paper documents

- Limit the number of full or partial copies of a document in circulation.
- Do not leave confidential documents unattended.
- When documents are not in use, store them in a secure location with restricted access, such as a locked filing cabinet.

Removing documents from the office

- Documents containing information relating to electors should not be removed from the office, unless absolutely necessary.
- Volunteers and staff members should always obtain approval from the officer responsible for the protection of personal information before removing such documents.

Public transportation and public places

- Information relating to electors, whether stored in paper or electronic format, should never be handled in public places or on public transit.
- Likewise, documents or computer equipment containing information relating to electors should never be left unattended in a car or in a carrier bag.

Retaining electronic documents

- Electronic records containing information relating to electors should be encrypted when kept on storage devices.
- Likewise, data stored on removable media should be encrypted.
- At all times, removable media should be in the possession of a volunteer or staff member, or kept in a secure location.
- It is important to always limit the number of copies of an electronic document in circulation.

Laptops and personal computers

- Laptops or personal computers containing information relating to electors should be password-protected. All data stored on a hard drive should be encrypted. Antivirus software should be installed on such computers. Laptops should be kept in a secure location when not in use.
- If a hard drive cannot be encrypted, the data stored on it should be encrypted using software designed for this purpose.

Wireless technology

- When using a smartphone or tablet connected to a public wireless network, it is important not to run mobile applications that use or share information relating to electors, or that access such information. It is better to share such data over a cellular network.
- Any mobile device used to store information relating to electors must be protected with a secure password.
- When away from the office, volunteers and staff members should always have their mobile devices in their possession to prevent loss or theft.

Communication by e-mail or fax

- Never send information relating to electors via e-mail.
- Avoid sending information relating to electors by fax or confirm that the recipient will be on hand to receive the documents as they arrive. Also, ensure that the fax number has been dialled correctly.

Information systems

- Internet-connected information systems (such as a website a party uses to help manage its election campaign) that use information relating to electors must be protected by a strong (or two-factor) authentication mechanism.
- Penetration tests should be conducted annually to confirm the strength of the system and its safeguards.

Destruction

When it is no longer necessary to retain information relating to electors, the information must be securely destroyed in a manner that protects its confidentiality.

We recommend that paper documents be destroyed using a cross-cut shredder or the services of a specialized firm.

Electronic documents should be destroyed using specialized software or the services of a specialized firm. Any backup copies also need to be securely destroyed..

REPORTING CONFIDENTIALITY-RELATED INCIDENTS AND POTENTIAL OFFENCES

Candidates, political parties and tickets should immediately inform the returning officer of any act likely to cause an actual or potential confidentiality breach involving electors' private information, such as the loss or theft of paper or electronic documents containing information relating to electors; the penetration of a network or an information system; the misuse or malicious use of information; fraud; the unauthorized disclosure of information; identity theft; or unauthorized data access.

APPENDIX 1

Frequently Asked Questions

Can a candidate in a municipal election, a political party or a ticket…

1. **… use the list of electors to visit voters at home, promote their platforms or solicit political contributions?**

   Yes, those are legitimate uses of information relating to electors under the AERM.

2. **… use the list of electors to send birthday greetings to electors?**

   Non, la liste électorale n'est pas transmise dans ce but, mais seulement pour les fins prévues à la LERM. Une personne qui utiliserait les renseignements relatifs aux électeurs de cette façon est susceptible de commettre une infraction à la LERM.

3. **… tell a person whether his or her contact information appears on the list of electors?**

   No. Such a person should be directed to contact the returning officer of his or her municipality or to appear before the board of revisors.

4. **… tell a person whether a relative or friend is entered on the list of electors?**

   No. The AERM prohibits anyone from sharing information contained in the list of electors to any person who is not legally entitled to receive it. All information related to entries on the list of electors is confidential.

5. **… sell or give the list of electors to anyone wishing to use it as a mailing list or for solicitation purposes?**

   No, the list of electors may not be used for any purpose other than those set out in the AERM.

   Furthermore, any natural person who discloses or allows the disclosure of the list of electors in violation of the AERM is liable to a fine of between $500 and $2,000 for a first offence.

6. **… keep a copy of the list of electors once the election is over?**

   Since the AERM prohibits the use of the list of electors for any purpose other than those set out in the legislation, we recommend securely destroying all copies of the list of electors once the election period is over.

   However, a political party may, if it deems necessary, retain a copy of the list of electors after the election period for the purpose of contacting electors. This could involve recruiting new members or soliciting political contributions.

7. **… share the list of electors with volunteers or members of the campaign staff so they can track support or encourage electors to go vote on polling day?**

   Volunteers or staff members may be provided with a copy of the list of electors for the purpose of campaigning on behalf of a candidate, political party or ticket.

   We recommend assigning such a mandate in writing, while specifying the scope of the mandate as well as the relevant confidentiality requirements. Any person who receives a copy of the list of electors should sign a confidentiality undertaking.

   Candidates, political parties and tickets must take the necessary measures to ensure that all persons who receive the list of electors comply with the conditions of their mandate and with the provisions of the AERM.

8. **... share the list of electors with MNAs, political parties or candidates for a different level of government?**

   No, the AERM prohibits anyone from sharing the list of electors for any purpose other than those set out in the legislation or with anyone who is not legally entitled to receive it.

9. **... personally use the list of electors for genealogical research or allow volunteers to retain a copy for that purpose?**

   No, the list of electors may not be used or shared for any purpose other than those set out in the AERM.

   Furthermore, any natural person who uses or shares the list of electors, or who allows it to be shared in violation of the AERM is liable to a fine of between $500 and $2,000 for a first offence.

10. **... provide the list of electors to a firm supplying election campaign management software?**

    After receiving the list of electors from the returning officer, a candidate, political party or ticket may entrust it to a service provider mandated to manage or host the list of electors, for its exclusive use, on an IT platform.

    We recommend assigning such a mandate in writing, while specifying the scope of the mandate as well as the relevant confidentiality requirements.

    Candidates, political parties and tickets must take the necessary measures to ensure that the service provider complies with the conditions of its mandate and with the provisions of the AERM.

APPENDIX 2

Confidentiality Undertaking for Persons Receiving the List of Electors

Confidentiality undertaking form for persons receiving the list of electors

In view of the following:

- The *Act respecting elections and referendums in municipalities* (CQLR, c. E-2.2 [AERM]) provides that personal information relating to electors – including an elector's name, address, date of birth and sex – is confidential;
- Section 659.1 of the AERM states that, "No person may use, communicate or allow to be communicated, for purposes other than those provided for in [the AERM], or communicate or allow to be communicated to a person not legally entitled thereto, any information contained in a list of electors or referendum list or in a list of qualified voters entitled to have their names entered on a referendum list";
- Under section 639 of the AERM, persons guilty of an offence described in section 659.1 are liable to a fine of between $500 and $4,000, in the case of a natural person, and between $1,500 and $12,000, in the case of a legal person.

I,

_____

Name of the person

having received the list of electors sent to

_____

Name of the candidate, political party or ticket (hereinafter "the entity"),

hereby agree to :

- Maintain the confidentiality of all information relating to electors entrusted to me by the entity;
- Use such information exclusively for the purposes set out in the AERM, subject to the instructions given to me by the entity;
- Not communicate this personal information to anyone, unless instructed to do so by the entity;
- Take all appropriate security measures to protect the confidentiality of such information;
- Upon the completion of my duties, not retain any personal information relating to electors, regardless of the format used to store it, by returning any relevant documents to the entity or by seeing to their secure destruction, according to the instructions provided by the entity;
- Immediately inform the entity of any failures to comply with the provisions described above or of any incidents that could lead to a security or confidentiality breach involving this personal information.

_____

Signature

Signed in _____ On _____

City/town Date

APPENDIX 3

Confidentiality Undertaking for Service Providers

Confidentiality and protection of personal information undertaking form for service providers

In view of the following :

- The *Act respecting elections and referendums in municipalities* (CQLR, c. E-2.2 [AERM]) provides that personal information relating to electors – including an elector's name, address, date of birth and sex – is confidential;
- Section 659.1 of the AERM states that, "No person may use, communicate or allow to be communicated, for purposes other than those provided for in [the AERM], or communicate or allow to be communicated to a person not legally entitled thereto, any information contained in a list of electors or referendum list or in a list of qualified voters entitled to have their names entered on a referendum list";
- Under section 639 of the AERM, persons guilty of an offence described in section 659.1 are liable to a fine of between $500 and $4,000, in the case of a natural person, and between $1,500 and $12,000, in the case of a legal person.

I,

_____

Name of the person,

acting as a representative of the service provider mandated by

_____

Name of the candidate, political party or ticket (hereinafter "the entity"),

hereby agree to :

- Maintain the confidentiality of all information relating to electors entrusted to me by the entity;
- Use such information exclusively for the purposes set out in the AERM, subject to the instructions given to me by the entity;
- Not communicate this personal information to anyone, unless instructed to do so by the entity;
- Take all appropriate security measures to protect the confidentiality of such information;
- Inform the relevant staff members of the security requirements relating to the confidentiality of this information, as well as of the obligations provided for in the provisions mentioned above;
- Upon the expiry of the mandate, not retain any personal information relating to electors, regardless of the format used to store it, by returning any relevant documents to the entity or by seeing to their secure destruction, according to the instructions provided by the entity;
- Immediately inform the entity of any failures to comply with the provisions described above or of any incidents that could lead to a security or confidentiality breach involving this personal information.

I acknowledge that I have read and understood the terms of this agreement.

_____ _____

Signature Name of service provider

Signed in _____ On _____

Location Date

APPENDIX 4

Personal information protection policy template for candidates

1. Scope

This policy applies to [name of the person], [candidate] in the municipality of [name of the municipality], and to any person who receives information relating to electors while acting as a volunteer for the candidate or as a member of the latter's staff.

It applies to all information relating to electors provided by the returning officer or by one of the latter's representatives, in accordance with the *Act respecting elections and referendums in municipalities* (CQLR, c. E-2.2).

In accordance with the *Act respecting elections and referendums in municipalities*, the returning officer must provide the candidate with a copy of the list of electors, as well as other documents that contain information including the name, address, date of birth and gender of each elector.

2. Responsibility

The candidate is responsible for the protection of personal information. He or she must ensure compliance with the policy by any person who receives information relating to electors.

More specifically, the candidate is responsible for:

- Ensuring compliance with restrictions on the use and disclosure of information relating to electors as set out in the Act respecting elections and referendums in municipalities and in this policy;
- Obtaining a confidentiality undertaking from any person who receives information relating to electors, and maintaining a disclosure log;
- Notifying the returning officer of any incidents involving the theft or loss of information relating to electors, or that could otherwise lead to a confidentiality breach;
- Ensuring the secure destruction of information relating to electors;
- Receiving and processing complaints from electors regarding the protection of personal information.

Where applicable, the candidate delegates this responsibility to the following person:

[Name and contact information of the officer responsible for the protection of personal information]

3. Restrictions on use

In accordance with section 659.1 of the Act respecting elections and referendums in municipalities, the candidate and his or her representatives should only use information relating to electors for the purposes set out in the Act respecting elections and referendums in municipalities.

The candidate and his or her representatives are forbidden from using any information relating to electors in their possession for commercial purposes or for profit.

4. Disclosure of information

The candidate may disclose information relating to electors to members of his or her staff or to his or her volunteers, where such disclosure is necessary for these staff members or volunteers to carry out the duties or mandate assigned to them by the candidate, subject to the restrictions set out in section 659.1 of the Act respecting elections and referendums in municipalities.

The candidate may also disclose information relating to electors to a third party, where such disclosure is necessary to fulfil a mandate or service contract assigned by the candidate under the Act respecting elections and referendums in municipalities.

5. Confidentiality undertaking and disclosure log

Before disclosing any information relating to electors, the candidate should obtain a written undertaking from the person receiving the information. The undertaking should commit the person to respecting the confidential nature of the information as well as the restrictions on its use set out in section 659.1 of the Act respecting elections and referendums in municipalities.

The officer responsible for the protection of personal information should maintain a disclosure log that records:

- The date of the disclosure;
- The name of the person receiving the information;
- A description of the storage medium used for sharing or consulting the information;
- A confirmation that the confidentiality undertaking has been signed;
- The date on which the information was returned or on which its secure destruction was confirmed.

6. Security measures

The candidate agrees to implement the security measures required to protect the information relating to electors he or she collects, uses, discloses, retains and destroys.

7. Retention and destruction of information

The candidate may retain information relating to electors for as long as he or she requires it for election purposes. He or she is responsible for ensuring that all documents are securely destroyed, regardless of the medium used to store the confidential information, once the documents are no longer in use or once their retention is no longer authorized.

The officer responsible for the protection of personal information is responsible for taking the necessary measures to ensure that all disclosed information is returned to the candidate or securely destroyed once the persons who received the information are no longer authorized to use it.

The candidate is responsible for destroying all information relating to electors when he or she no longer requires the information for election purposes or, at the latest, when his or her authorization expires.

8. Loss or theft of information

In cases where information relating to electors is lost or stolen, the candidate is responsible for:

- Determining the cause of the incident and limiting its impact;
- Documenting the circumstances leading up to the incident;
- Reviewing internal policies, processes and procedures with an eye to preventing similar incidents;
- Notifying the returning officer of the loss or theft.

9. Access to information

Any person may contact the officer responsible for the protection of personal information to learn what pieces of his or her personal information have been collected or to submit a question or complaint regarding how the candidate manages information relating to electors.

APPENDIX 5

Personal information protection policy template for political parties and tickets

1. Scope

This policy applies to the [name of the political party or ticket], to its candidates and to any other person who receives information relating to electors, who represents the party or who works for the latter, whether in a paid capacity, in exchange for some other benefit or as a volunteer.

It applies to all information relating to electors provided by the returning officer or by one of the latter's representatives, in accordance with the Act respecting elections and referendums in municipalities (CQLR, c. E-2.2).

In accordance with the Act respecting elections and referendums in municipalities, the returning officer must provide the [name of the political party or ticket] with copies of the list of electors, which contains the name, address, date of birth and gender of each elector.

2. Responsibility

The [name of the political party or ticket]'s officer responsible for the protection of personal information, identified below, is responsible for ensuring compliance with the policy by any person who receives information relating to electors.

[Name and contact information of the officer responsible for the protection of personal information]

More specifically, this person is responsible for:

- Ensuring compliance with restrictions on the use and disclosure of information relating to electors as set out in the Act respecting elections and referendums in municipalities and in this policy;
- Obtaining a confidentiality undertaking from any person who receives information relating to electors, and maintaining a disclosure log;
- Notifying the returning officer of any incidents involving the theft or loss of information relating to electors, or that could otherwise lead to a confidentiality breach;
- Ensuring the secure destruction of information relating to electors;
- Receiving and processing complaints from electors regarding the protection of personal information.

3. Restrictions on use

In accordance with section 659.1 of the Act respecting elections and referendums, the [name of political party or ticket] and its representatives can only use information relating to electors for the purposes set out in the Act respecting elections and referendums in municipalities.

The candidate and his or her representatives are forbidden from using any information relating to electors in their possession for commercial purposes or for profit.

4. Disclosure of information

The [name of the political party or ticket] may disclose information relating to electors to members of its staff, to its volunteers or to its candidates, where such disclosure is necessary for these staff members, volunteers or candidates to carry out the duties or mandate assigned to them by the [name of the political party or ticket], subject to the restrictions set out in section 659.1 of the Act respecting elections and referendums in municipalities.

The [name of the political party or ticket] may also disclose information relating to electors to a third party, where such disclosure is necessary to fulfil a mandate or service contract assigned by the [name of the political party or ticket] under the Act respecting elections and referendums in municipalities.

5. Confidentiality undertaking and disclosure log

Before disclosing any information relating to electors, the [name of the political party or ticket] should obtain a written undertaking from the person receiving the information. The undertaking should commit the person to respecting the confidential nature of the information as well as the restrictions on its use set out in section 659.1 of the Act respecting elections and referendums in municipalities.

6. Security measures

The [name of the political party or ticket] agrees to implement the security measures required to protect the information relating to electors it collects, uses, discloses, retains and destroys.

Furthermore, the [name of the political party or ticket] agrees to have its information systems tested annually for resistance to cyberattacks (e.g., by conducting a penetration test).

7. Retention and destruction of information

The [name of the political party or ticket] may retain information relating to electors for as long as it requires such information for election purposes. It is responsible for ensuring that all documents are securely destroyed, regardless of the medium used to store the confidential information, once the documents are no longer in use or once their retention is no longer authorized.

The officer responsible for the protection of personal information is responsible for taking the necessary measures to ensure that all disclosed information is returned to the party or ticket, or that it is securely destroyed once the persons who received the information are no longer authorized to use it.

8. Loss or theft of information

In cases where information relating to electors is lost or stolen, the [name of the political party or ticket] is responsible for:

- Determining the cause of the incident and limiting its impact;
- Documenting the circumstances leading up to the incident;
- Reviewing internal policies, processes and procedures with an eye to preventing similar incidents;
- Notifying the returning officer of the loss or theft.

9. Access to information

Any person may contact the [name of the political party or ticket]'s officer responsible for the protection of personal information to learn what pieces of his or her personal information have been collected or to submit a question or complaint regarding how the [name of political party or ticket] manages information relating to electors.

APPENDIX 6

Disclosure log for information relating to electors

Recipient's name	Disclosure date	Confidentiality undertaking signed (yes/no)	Description of the storage medium used or of the information disclosed	Date of return, access revocation or destruction