SUMMARY
Political Parties and Protection of Personal Information

Introduction
Since 2013, Québec's Chief Electoral Officer has expressed concerns about the protection of personal information held by political parties and has called for an in-depth review of the Election Act in this regard.

This document aims to foster reflection on this question and to shed light on the issues raised by political parties' use of voters' personal information. It also examines the oversight mechanisms applicable to political parties and the practices associated with the transmission of the electoral list.
Considerations for the digital era

Nowadays, professional life, social life and privacy are organized around digital tools. As a result, individuals reveal information on their personal preferences and leave other traces on the websites they visit. With social media, the types of personal information in circulation have broadened and expanded considerably. Internet exposure — partly voluntary, partly involuntary — can have unexpected repercussions. In the digital era, mechanisms designed to uphold privacy seem increasingly fragile.

Against that backdrop, opportunities for mass collection of personal information, as well as for data reconciliation and use, have grown. Indeed, they have laid the foundations of the digital economy.

Digital technologies have also changed the ways in which individuals contribute to democratic life and exercise their citizenship. More and more, political parties rely on voters' personal information to implement their electoral strategies and engage in political communications.
Principles of personal information protection

Personal information protection is defined by a series of principles applicable to public and private organizations of all kinds. Outside Québec, the following principles are enshrined in privacy protection legislation:

- Assigning responsibility.
- Determining why information is being collected.
- Obtaining consent.
- Limiting the information collected.
- Limiting how information is used, communicated and conserved.
- Ensuring accuracy.
- Implementing security measures.
- Achieving transparency.
- Providing access to personal information.
- Challenging the information collection process.

In Québec, these principles are enshrined in the Act respecting access to documents held by public bodies and the protection of personal information, adopted in 1982, as well as in the Act respecting the protection of personal information in the private sector, adopted in 1993.
Overview of political parties' digital practices in Québec

Digital technologies have led to new ways of campaigning, prompting political parties to change how they rally supporters and communicate with voters.

Québec's main political parties use electoral databases that now play a central role in election campaigns. The social networks also play an important part, primarily as a means of reaching out to voters.

Québec's main political parties have reportedly invested in the acquisition, development and adaptation of IT tools so they can gather and use voters' personal information.

Electoral databases give political parties an opportunity to cross-reference the voter information they collect, including data from electoral lists communicated by the Chief Electoral Officer. These lists contain each elector's name, address, gender and birth date, as well as addresses outside Québec if individuals vote outside the province. The parties use cross-referencing to identify voter concerns, adjust their persuasion strategies and personalize the messages they deliver to voters. Because they are recognized as being faster and more effective, databases are replacing more traditional ways of targeting voters and persuading them to support a candidate.

Since political parties can consult these databases from Web applications and, in some cases, mobile devices, volunteers now have easy access to voter information when campaigning door-to-door and can even collect it in real time.

Using algorithms, political parties can segment the electorate and draw up voter profiles. Voter databases are used as a campaign management tool, particularly for assigning volunteers, generating telephone call lists, organizing door-to-door operations and sending text messages.

Amid limited resources, databases can optimize the time and resources allocated to identifying supporters, engaging in communications and mobilizing voters. Databases are all the more useful amid dwindling political engagement, as reflected in lower voter turnout.

Political parties also reportedly keep personal information on candidates, contributors and staffers, as well as on volunteers recruited during electoral periods.

Less costly than traditional media, social media serve as a complement to traditional communication techniques because political parties can deliver targeted messages to a larger audience. Parties can also buy advertising and conduct surveys on topics of interest on Facebook in order to reach voters.
Protecting the personal information of Québec's voters

Over the past 75 years, various changes have been made to the electoral laws aimed at ensuring better protection of information derived from electoral lists. Previously public, this information is now regarded as confidential and is only accessible by the Chief Electoral Officer and his/her staff, as well as by political parties, MNAs and, during electoral periods, candidates. Since 1989, Québec's Election Act has upheld the confidentiality of this information.

In 1995, Québec drew up a permanent list of electors so the Chief Electoral Officer can continuously monitor the accuracy of the list, thus reducing the need for public oversight. This led to various legislative amendments aimed at limiting access to voter information and the purposes for which it can be used or communicated.

Political parties in Québec are not subject to a general law governing the protection of personal information. Only the Election Act regulates the use and communication of voter information. This legislative framework, however, only applies to information on lists communicated by the Chief Electoral Officer.

In particular, the Election Act prohibits the following:

- Using voter information for purposes other than those set out in the Act.
- Communicating or facilitating the communication of this information for purposes other than those set out in the Act.
- Communicating or facilitating the communication of this information to anyone not legally entitled to access it.

Other personal information held by a political party is not governed by the Election Act, including data on party volunteers, candidates, members and staffers, as well as personal information collected directly by political parties, either from voters or from intermediaries.

The Chief Electoral Officer's audit and investigation powers are limited to the requirements and violations set out in the Election Act. For example, the Chief Electoral Officer cannot conduct an audit on the collection of personal information by political parties because no provisions in the Act regulate those activities.

Moreover, the Act stipulates that political parties and MNAs can receive the list of registered voters (i.e. the permanent list of electors) three times a year. During electoral periods, candidates have access to the same information and can receive lists of individuals registered to vote in residential facilities or at home. They can also obtain lists of individuals who voted in the advance poll or on Election Day.

To receive lists of electors, MNAs and party-designated individuals must submit a written undertaking in which they pledge to take all necessary steps to protect the confidentiality of voter information and to limit its use to the purposes set out in the Election Act.
**Legislative framework in Canada**

With the exception of British Columbia, where all political parties are subject to a general privacy protection law, the legislative framework governing political parties at the federal and provincial levels is similar to that in effect in Québec.

Canada's electoral laws prohibit the use of information recorded on electoral lists for any purposes not set out in the federal *Election Act* and limit its use to communications with voters.

Outside of electoral periods, lists are transmitted to political parties less frequently than they are in Québec. In addition, they do not include birthdates; only New Brunswick's electoral list includes gender information.

Laws in Canada include relatively few measures aimed at verifying the confidentiality of information derived from electoral lists. However, recent legislative amendments have tightened voter information protection in B.C. and Ontario. In both cases, the amendments included requirements to develop and comply with a privacy policy, in addition to instituting stricter controls over access to electoral lists.

In recent years, Canadian supervisory authorities have issued a number of recommendations on personal information protection. In September 2018, the federal, provincial and territorial information and privacy commissioners, including the chair of Québec's Commission d'accès à l'information (access to information commission), called for Canadian laws to include provisions requiring political parties to protect personal information.
Legislative framework outside Canada

A review of the electoral legislation and regulatory systems governing personal information protection in various countries shows that the approaches are varied and wide-ranging. Governance mechanisms range from responsible to flexible use of voters' personal information. In this regard, all these countries have begun to reflect on the oversight of political parties and how to make them more accountable.

In New Zealand, France, Belgium, Luxembourg, Switzerland and the United Kingdom, political parties and election candidates — like any other public or private organizations that collect and use data — are fully responsible and are required to protect the personal information they keep.

In the U.S. and Australia, in contrast, political parties are not required to comply with the same principles, regulations and practices that private and public organizations are subject to.

Within the European Union, the General Data Protection Regulation (GDPR) applies to all private organizations, government bodies, "associative movements" (e.g. community groups) and political parties. The GDPR strengthens requirements on data collection and processing, in addition to instituting governance mechanisms. It also reaffirms existing individual rights and adds a number of new rights aimed at ensuring effective citizen action. In addition, it sets out a series of graduated penalties in the event that regulatory requirements are not met.

When we compare the requirements imposed on political parties under the GDPR and those in Québec and the rest of Canada, we note that the personal information on registered voters on electoral lists in Europe is wide-ranging and detailed; in addition, these lists are more widely accessible. In Europe, however, oversight mechanisms are stricter, e.g. electoral lists must be destroyed after elections and voters have more control over how their data is processed.
**Issues and recommendations**

In relation to the issues raised by personal information protection and concerns over its use by political parties, the Chief Electoral Officer is issuing nine recommendations.

Subjecting political parties to a general legislative framework governing personal information protection would ensure that all personal information held by political parties is covered by a protection regime equivalent to that governing information held by public and private organizations in Québec.

Given that municipal political parties receive lists during electoral periods, municipal parties should be subject to the same oversight mechanisms as provincial parties.

**For those reasons, we propose the following recommendations:**

1. Authorized provincial political parties should be subject to a general legislative framework governing personal information protection.

2. Authorized municipal political parties should be subject to a general legislative framework governing personal information protection.

3. Similar requirements should be established for MNAs and candidates in provincial, municipal and school board elections, with the necessary adaptations.

In particular, this legislative framework should include the following requirements:

- Political parties should designate a person in charge of personal information protection.

- Political parties that collect personal information should determine beforehand the purposes for which the information will be collected.

- Prior to collecting, using or communicating personal information, political parties should obtain the consent of the individuals concerned. In addition to being clear, free and informed, this consent should be given for specific purposes and should only be valid for a pre-determined period of time.

- Prior to gathering personal information, political parties should inform the individuals concerned why the information is being collected, how it will be used, what categories of people within the political party will have access to it and where it will be kept. Political parties should also inform the individuals concerned of their access and rectification rights.
• Political parties should use the information they collect only for the purposes to which the individuals concerned gave their consent.

• Political parties should limit the communication of personal information.

• Political parties should ensure that the personal information they hold is accurate and up to date when it is used.

• Political parties should destroy personal information if it is no longer needed.

• Political parties should take appropriate security measures to ensure the protection of all personal information collected, used, communicated, conserved or destroyed.

• Political parties should report any incidents involving personal information that could have an adverse impact on the individuals concerned to a competent supervisory authority.

• Political parties should give their staffers, volunteers and other agents access to personal information only if necessary. They should also keep a record of all individuals authorized to access personal information.

• Political parties should enter into an agreement guaranteeing personal information protection prior to communicating any information to a service provider.

• Political parties should respond diligently to access-to-personal-information requests and rectification requests received from the individuals concerned.

• Political parties should develop policies and procedures setting out measures aimed at meeting personal information protection requirements and should make these documents available upon request.

In addition, birthdate/gender information does not appear to be necessary for political parties to communicate with voters or encourage their participation. The same can be said for the temporary addresses of individuals casting their vote outside Québec or for information on individuals authorized to vote in residential facilities or at home (all of this information is communicated to candidates during electoral periods).

For those reasons, we propose the following recommendations:

4. Gender and birthdate information should be removed from electoral lists sent to MNAs, candidates and political parties, at all levels (municipal and provincial).

5. The Election Act should be amended to stop the transmission of information that could be used to identify vulnerable voters or to disclose temporary addresses outside Québec.
The purposes for which electoral list information can be used are not defined in the *Election Act*, the *Act respecting elections and referendums in municipalities* or the *Act respecting school elections*.

**For those reasons, we propose the following recommendation:**

6. The electoral laws should specify the purposes for which MNAs, candidates and political parties can use or communicate information derived from electoral lists.

Since 2006, all authorized provincial political parties can obtain the provincial electoral lists three times a year, outside of electoral periods. There is good reason to question whether this information needs to be communicated so frequently outside of electoral periods.

An electronic version of the list of electors is available to MNAs, candidates and political parties. A print version is also available because the *Election Act* still provides for this option. The Chief Electoral Officer could determine the criteria for communicating this list to ensure that it is adapted to technological realities and that the necessary security measures are applied.

**For those reasons, we propose the following recommendations:**

7. Electoral lists should be communicated to provincial political parties and MNAs once a year outside of electoral periods.

8. Only the electronic version of electoral lists should be communicated to candidates, MNAs and political parties, in accordance with criteria to be determined by the Chief Electoral Officer.
Review of the Chief Electoral Officer's recommendations

The proposed recommendations in this document could have significant repercussions on the provisions of the Election Act, the Act respecting elections and referendums in municipalities and the Act respecting school elections.

In our view, all stakeholders should be asked to contribute to these legislative amendments, including the Commission d’accès à l’information, the Ministère des Affaires municipales et de l’Habitation (municipal affairs and housing ministry), the Ministère de l’Éducation et de l’Enseignement supérieur (ministry of education and higher education), provincial and municipal political parties, as well as privacy protection experts, who could refine and improve these recommendations.

In our view, these recommendations should not be reviewed without listening to the main individuals concerned, namely Québec's voters.

For those reasons, we propose the following recommendation:

9. Québec's National Assembly should establish a special commission with a view to studying oversight mechanisms for political parties regarding personal information protection and reviewing the Chief Electoral Officer's recommendations.