



Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

May 17, 2007

HAND DELIVERED

The Honourable Donald H. Oliver, Senator
Chair of the Standing Senate Committee on Legal and Constitutional Affairs
The Senate of Canada
Ottawa, Ontario
Canada, K1A 0A4

Dear Senator:

Re: Bill C-31 (An Act to amend the *Canada Elections Act* and the *Public Service Employment Act*)

Thank you for the invitation to appear before the Senate Committee on Legal and Constitutional Affairs on May 17, 2007. The Office of the Information and Privacy Commissioner of Ontario welcomes the opportunity to provide its perspective on privacy protections in the handling of personal information in the context of election law reform.

Introduction

Our submissions will focus on 1) overarching privacy principles, 2) relevant legislative developments in Ontario, 3) our privacy views on the Ontario context, and 4) privacy issues raised by Bill C-31. From the outset, we note that the Privacy Commissioner of Canada, Commissioner Stoddard, has concerns about Bill C-31 related to the disclosure of the full birth dates of voters. We wish to add our voice to hers and urge you to prohibit the disclosure of this personal information.

The IPC/O's Submission

1. Overarching Privacy Principles

Consistent with privacy legislation in Ontario and across Canada, the perspective of Ontario's Commissioner on matters involving the handling of personal information is grounded in the fair information principles and practices (FIPS). These principles and practices underpin the Global Privacy Standard (GPS) which was accepted at the 28th International Data Protection Commissioners' Conference in the United Kingdom on November 3, 2006 (attached).

.../2



Legal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services juridiques
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9186
TTY: 416-325-7539
www.ipc.on.ca

It is also important to measure the handling of personal information against principles articulated under the *Canadian Charter of Rights and Freedoms*. For example, particular attention should be paid to the four part test set out by the Supreme Court of Canada in *R. v. Oakes*, [1986] 1 S.C.R. 103. The principle point of the analytical framework set out in the *Oakes* test is to ensure that government action that affects the individual go no further than is necessary to accomplish a pressing and substantial objective. The implementing law, program or system should be rationally related to that objective, minimally impair rights, and the benefits obtained should be proportional to any rights infringements. This analysis should, we submit, govern the development of new program elements even where it is not clear that the level of intrusion will raise constitutional problems.

We say this, in part, because the notion of minimal impairment or, in informational terms, “data-minimization”, is one of the critical themes that runs across both the FIPS and the GPS. Following these standards, data-minimization should be built in to any new or evolving program involving the handling of personal information. Data-minimization is grounded in an understanding of the purpose of a particular data collection. The purposes for which personal information is collected, used, retained and disclosed should be clear, limited and relevant to the circumstances. The collection of personal information should be kept to a strict minimum. The use, retention, and disclosure of personal information should be limited to the relevant purposes.

2. Legislative Developments in Ontario

Currently, in Ontario, citizens in possession of the voter’s card mailed to their residence may simply state their name and address to authenticate that they are a person on the voters list and entitled to cast a ballot. If they are challenged, they may be required to execute a statutory declaration and otherwise establish their identity. Bill 218 (the Election Statute Law Amendment Act, 2007), which was referred to the Standing Committee on the Legislative Assembly on May 8, 2007, will require individuals to present identification in order to authenticate or verify their entitlement to vote, to change information on the voters list or to add a name to the voters list on polling day. The stated purpose of these changes is to improve the integrity of the voting process and reduce the likelihood of voter fraud.

3. Our Privacy Views on the Ontario Context

While we do not know the actual prevalence of voter fraud, we accept that improving the integrity of the voting process is an important objective. It is also noteworthy that the move from a more honour-based system to an identity-based system at Ontario polling stations will not involve the collection of personal information. Voters will simply be asked to present appropriate identification. It is our understanding that no information on, within or about the presented identification document will be recorded or otherwise collected at polling stations. This approach accords with the data-minimization principles set out above.

The determination as to which identification documents will be acceptable at polling stations is an important issue that may raise concerns about the integrity and accessibility of the voting process as well as concerns about privacy. In regards to the latter, consider, for example, that, while individuals may volunteer to present their health cards for the purpose of verifying their identity, third parties must not mishandle such information, for example, by collecting it for

purposes unrelated to the provision of provincially funded health resources. This prohibition applies to any individual or institution in Ontario including federal and provincial government agencies involved in the electoral process.

As for the administration of the permanent registry of electors, personal information is collected, cross referenced, and retained as the permanent register is updated. The information on the Ontario permanent register includes surname, given names, home address, gender, and date of birth. In this regard, it is noteworthy that, in Ontario, not all the personal information on the permanent register is disclosed to political parties, elected members of the Ontario Legislative Assembly, or candidates. In particular voters' birth dates and gender are not disclosed to these "political actors". Instead, they receive an extract of the permanent register – the voters list – comprised of voters' names and address. Political parties receive the province-wide voters list. Elected members and candidates are only entitled to that part of the voters list that relates to their electoral district. And while a copy of the voters list is made available for public viewing in the returning office and through the municipal clerk, no copies of it may be made.

Critically, section 17.4 of the *Election Act* of Ontario sets strict limits around the use of the information in the register and voters list, as well as the handling of information obtained from the permanent register in electronic form. Under section 17.4(1) any "person who obtains information, directly or indirectly, from the permanent register or from a list of electors prepared from the permanent register,

- a) shall use it only for electoral purposes;
- b) shall not use it for commercial purposes; and
- c) may disclose it to others only after obtaining their written acknowledgment that they are bound by the restrictions in this subsection.

In addition, pursuant to section 17.5, Ontario's Chief Election Officer (CEO) provides guidelines for compliance with section 17.4 and publishes them in the Ontario Gazette on the Internet. (I attach a copy of Elections Ontario's "Guidelines for Use of Information Obtained from the Permanent Register of Electors".) Under section 17.6, every registered party must develop and implement a policy to ensure that its candidates, members of the Assembly, employees and agents comply with section 17.4 and any guidelines provided under section 17.5. Furthermore, the CEO's guidelines contemplate the CEO's receipt of reports alleging contraventions of section 17.4 and allow the CEO to take "such steps as he or she considers necessary to pursue appropriate legal remedies against the person alleged to have contravened the section." Finally, the Chief Election Officer may review and publicly comment on any discrepancies between a party's policies and actual practices and the rules and guidelines established in section 17.4 and 17.5. In total, these statutory rules, guidelines, policies, and oversight powers serve to ensure that electoral integrity is advanced while minimizing the impact on privacy rights.

All of the critical legal limitations on the use and disclosure of the personal information on the permanent register are to be continued under Bill 218. In the view of our office, such limitations are vital and should be interpreted strictly and rigorously enforced to ensure that personal information is handled appropriately. For example, the use of birth dates should be confined to cross-referencing by the CEO. Secondly, "electoral purposes" should not necessarily be readily equated with purposes related to political activity outside the electoral period that commences with the dropping of the writ and ends with the closing of the polls.

4. Privacy Issues Raised by Bill C-31

While Bill C-31 and the *Canada Elections Act* share features in common with Bill 218 and the *Election Act* of Ontario, the federal Act does not specify the safeguards found in sections 17.4 to 17.6 of the provincial Act. (I attach sections 17.4 to 17.6.) The absence of these safeguards becomes more critical in light of provisions in Bill C-31 that allow for the disclosure to and use of the full date of birth of each voter by political actors. First, we note that under section 110 of the *Canada Elections Act*, the relevant political parties may "use the lists [of electors] for communicating with electors, including using them for soliciting contributions and recruiting party members." Secondly, subsection 110(3), explicitly confines candidates to using lists of electors "during an election period." In contrast, registered parties and elected members of Parliament do not appear to face any such restriction.

A person's full date of birth is sensitive information used by elections officials to distinguish and identify individuals for the purpose of maintaining the Register of Electors. In this context, a birth date is treated as a "shared secret" between the institution and the individual. In the absence of a demonstrated need, the further wide and ready dissemination of this sensitive personal information should be resisted as a needless breach of the data-minimization principle and a disproportionate intrusion of personal privacy. In addition to the potential for pre-writ and post election dissemination, we note that the dissemination of birth dates will occur in the fast paced setting of election campaigns. These campaigns are facilitated and run by a variety of elections staff, political workers, agents, and volunteers, many of whom are likely to lack adequate privacy training and supervision. There exists the real risk of lost, stolen, or otherwise misappropriated personal information with consequent risks to privacy including that raised by identity theft.

Accordingly, we urge the Senate to carefully consider whether there is a demonstrated need for political actors to receive and use birth dates from the Register of Electors. We recommend that information contained in an individual's date of birth only be used by the Chief Electoral Officer of Canada for the purpose of cross-referencing information on the Register of Electors. Disclosure of this personal information to political actors should be prohibited.

We also respectfully urge the Senate to consider recommending or introducing amendments to the *Canada Elections Act* that would provide for obligations and powers similar to those found in sections 17.4 to 17.6 of the *Elections Act* of Ontario. We appreciate that these changes would require that sections 110 and 111 of the federal Act be amended. In our view, these changes would be worth introducing even if our other recommendation is adopted.

Summary of Recommendations

The Office of the Information and Privacy Commissioner of Ontario recommends that the Senate examine the purpose of the electoral use of birth dates in the Register of Electors and the handling of personal information in the lists of electors and amend Bill C-31 to:

1. Ensure that information contained in an individual's date of birth only be used by the Chief Electoral Officer of Canada and only for the purpose of cross-referencing information on the Register of Electors.
2. Provide for obligations and powers similar to those found in sections 17.4 to 17.6 of the *Elections Act* of Ontario.

Conclusion

Thank you again for the invitation to appear before the Senate Committee on Legal and Constitutional Affairs and the opportunity to assist the Senate in its efforts to provide for privacy protections in the handling of personal information under Bill C-31.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Ken Anderson', with a long horizontal flourish extending to the right.

Ken Anderson,
Assistant Commissioner

cc: Jennifer Stoddard, Privacy Commissioner of Canada

Creation of a Global Privacy Standard

By Commissioner Ann Cavoukian, Ph.D.

Introduction

In 2005, at the 27th International Data Protection Commissioners Conference in Montreux, Switzerland, I chaired a Working Group of Commissioners. This Working Group was convened for the sole purpose of creating a single Global Privacy Standard. Faced with globalization and convergence of business practices, regardless of borders, I thought there was a pressing need to harmonize various sets of fair information practices into one Global Privacy Standard. Once such a foundational policy piece was in place, then businesses and technology companies could turn to a single instrument for evaluating whether their practices or systems were actually privacy enhancing, in nature and substance.

While attempting to develop a single law on data protection was beyond our reach, I was confident that we could develop a single privacy instrument, globally. In advancing my objective to develop a harmonized set of fair information practices, my office embarked on the preliminary work of conducting a “Gap Analysis.” This was the process of comparing leading privacy practices and codes from around the world, comparing their various attributes, and the scope of the privacy principles enumerated therein. We identified the strengths and weaknesses of the major codes in existence and then tabled our Gap Analysis with the Working Group of Commissioners.

In the months that ensued, we embarked upon the work of harmonizing the principles into a single set of fair information practices. This led to the development of the attached Global Privacy Standard (GPS), which builds upon the strengths of existing codes containing time-honoured privacy principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of “data minimization” under the “collection limitation” principle.

After successive drafts of the GPS were developed, revised and circulated for review, the attached final version of the GPS was formally tabled and accepted in the United Kingdom, on November 3, 2006, at the 28th International Data Protection Commissioners Conference.

Objective

The objective of the Global Privacy Standard is to form a set of universal privacy principles, harmonizing those found in various sets of fair information practices presently in existence.

The Global Privacy Standard draws upon the collective knowledge and practical wisdom of the international data protection community.

Scope

The Global Privacy Standard reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policymakers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personal information.

The GPS addresses privacy concerns for decision-makers in any organization that has an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is not intended to pre-empt or contradict any other laws or legal requirements bearing upon privacy and personal information in various jurisdictions.

GPS Privacy Principles

1. **Consent:** The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

2. **Accountability:** Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3. **Purposes:** An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4. **Collection Limitation:** The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

Data Minimization -- The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5. **Use, Retention, and Disclosure Limitation:** Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6. **Accuracy:** Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

7. Security: Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8. Openness: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9. Access: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Compliance: Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

ELECTIONS ONTARIO

GUIDELINES FOR USE OF INFORMATION OBTAINED FROM THE PERMANENT REGISTER OF ELECTORS

 [Print-friendly version](#)

* VOTERS

- > who can vote?
 - voters list
 - identification
- > what happens when i vote?
- > when can i vote?
- > where do i vote?
- > how can i vote?
- > why should i vote?
- > alternative needs
- > by-elections 2007

* CANDIDATES & PARTIES

* MEDIA

* EDUCATION

* RESULTS & STATS

* LEGISLATION

* ELECTION FINANCES

* ABOUT

* FREQUENTLY ASKED QUESTIONS

* HOME

[Go back](#)

These Guidelines are intended to help recipients of information from the Permanent Register of Electors for Ontario or the Lists of Electors that are prepared from the Register, to follow the provisions of section 17.4 of the *Election Act*, Chap E-6, RSO 1990, as amended, relating to restrictions on the use and distribution of that information.

For the authoritative provisions, reference should be made to the statute.

1. Principles

The principles underlying the prohibitions and restrictions against the dissemination of information obtained from the Permanent Register of Electors and the Lists of Electors prepared from the Permanent Register of Electors is that the information is personal information. Such information is generally not disseminated without first obtaining the consent of the person whom it concerns. Fundamental to the democratic process, however, is the identification of every elector. It is also essential to the democratic process for registered political parties to be aware of who the electors are so that they are able to present to them their political platform and thereby place the electorate in a position to make an informed choice when voting.

Section 17.4 of the *Election Act* requires that any information obtained by anyone from the Permanent Register of Electors or the Lists of Electors prepared from the Permanent Register of Electors must be used for electoral purposes only. The section also prohibits the use of any such information for commercial purposes.

2. Overview

The limitation placed upon the dissemination of personal information respecting electors is therefore an attempt to achieve a balance between the protection of privacy and the need to facilitate the electoral process which is fundamentally essential to the democratic process.

Any person who receives information from the Permanent Register of Electors or the Lists of Electors must, before he or she discloses the information to any other person, obtain a written acknowledgment that the other person will be bound by the specific provisions of section 17.4. The acknowledgement also provides that the other person must also obtain a similar written acknowledgment before information is further disclosed to anyone else.

Section 17.4 of the *Election Act* applies irrespective of how the information is obtained and whether it is in electronic form or in printed form. Where the information is received in electronic form, the section prohibits reproduction, storage or transmitting of the information electronically. Any person who receives the information from a party or member must complete the written acknowledgement under section 17.4 before he or she can reproduce, store or transmit the information. The prohibition against electronic reproduction, storage or transmission does not apply to a registered party or a member of the Legislative Assembly receiving the information in accordance with section 17.3 of the Act.

3. Procedures - Copy of, or extract from, the Permanent Register of Electors for Ontario**1. Chief Election Officer**

1. Every registered party and member of the Assembly will be notified by the Chief Election Officer when updating of the Permanent Register of Electors for Ontario is complete. The notification will include a form

QUICK LINKS

[Permanent Register of Electors for Ontario](#)[Guidelines for Use of Information Obtained from the Permanent Register of Electors \(PDF 31Kb\)](#)[Download Adobe Acrobat Reader](#)

- to be returned to the Chief Election Officer to request a copy of the Register or part of the Register. The request form will set out the restrictions on use and disclosure of the information, identify the person designated to receive the information (the recipient) on behalf of the registered party or member, and provide a form of undertaking to be signed by that person, signifying acceptance of the restrictions of the Act.
2. On receipt of the completed request form from a registered party or a member of the Assembly, the copy or extract from the Permanent Register of Electors for Ontario will be produced by the Chief Election Officer on a CD-ROM including a statement about the general restrictions on use of the information.
 3. The Chief Election Officer will provide the information to the person designated by the registered party or member, with a reminder of the restrictions and instructions relating to the security features of the information release.
 4. Where the Chief Election Officer receives a written report alleging a contravention of section 17.4 of the Act and the Chief Election Officer is of opinion that the allegation has merit, the Chief Election Officer may take such steps as he or she considers necessary to pursue appropriate legal remedies against the person alleged to have contravened the section.
- 2. Recipient of information from the Permanent Register of Electors for Ontario (person designated under 3.1.1)**
1. The recipient is responsible for ensuring that the registered party or member that he or she represents adheres to the requirements of section 17.4
 2. Where the recipient has reason to believe that there has been a contravention of section 17.4 of the Act, the recipient must forthwith provide the Chief Election Officer with a full and complete written report of the alleged contravention.
 3. Before allowing access to the copy of the Register or information contained in the Register, the recipient must obtain a written acknowledgement from every person who will have access, that he or she understands and is bound by the provisions of section 17.4. This applies to employees and any other authorized person. A form of acknowledgement (FO102) will be included with the delivery of the information from the Chief Election Officer.
 4. The recipient is responsible for ensuring that any person who has access to the electronic file containing information from the Register is aware that the information is not to be reproduced, stored or transmitted electronically for any purpose.
 5. The recipient is responsible for ensuring that, within five days of receiving an updated copy of or extract from the Permanent Register of Electors from the Chief Election Officer, every printed obsolete copy of the Permanent Register of Electors in his or her possession is shredded, and within ten days of receiving the updated copy all obsolete electronic copies of the Permanent Register of Electors in his or her possession are returned to the Chief Election Officer.
- 3. Registered parties and independent candidates and independent members of the Assembly**

1. Every registered party, independent candidate and independent member of the Assembly is required to develop and implement a policy that ensures candidates, members of the Assembly, staff and agents, as appropriate, comply with section 17.4 and these guidelines.
 2. The policy must be disclosed to the Chief Election Officer at his or her request and may be published by the Chief Election Officer.
4. **Procedures after a Writ of Election has been issued - Copy of, or extract from, the Lists of Electors prepared from the Permanent Register of Electors for Ontario**

1. Chief Election Officer

1. When the Writ for an election or by-election is issued, the Chief Election Officer will prepare the Lists of Electors from the Permanent Register of Electors and provide a copy to the Returning Officer as required by section 19 of the *Election Act*.

2. Returning Officer

1. Upon receipt of the copy of the Lists of Electors prepared from the Permanent Register of Electors for Ontario and delivered according to section 19 of the *Election Act*, the Returning Officer is required to arrange for copies of the Lists to be made and distributed according to subsection 19(3)
2. The Returning Officer must ensure that election workers who have access to the Lists or information from the Lists, are aware of and comply with the provisions of section 17.4 of the Act. A written acknowledgement (Form FO101) must be completed before workers are granted access to the information.

3. The person who receives a copy of, or information from, the List of Electors

1. The person who receives a copy of, or information from, the Lists of Electors must not use the information for any purpose other than electoral purposes, nor for any commercial purpose.
2. The person who receives the information must advise every other person who will become aware of information from the Lists of Electors of the statutory prohibitions and restrictions respecting the use of such information.
3. The person who receives the Lists of Electors or information therefrom has a responsibility to ensure that every person supervised by him or her who becomes aware of information from the Lists of Electors complies with the statutory prohibitions and restrictions respecting the use of such information.
4. Before allowing access to the copy of the Lists of Electors or information contained in the Lists, a written acknowledgement must be obtained from every person who will have access, that he or she understands and is bound by the provisions of section 17.4. This applies to employees and any other person. A form of acknowledgement (FO101) will be included with the delivery of the information from the Returning Officer.
5. Where a person who has received information has reason to believe that there has been a contravention of section 17.4 of the Act, he or she must provide the Chief Election Officer with a full and complete written report of the alleged contravention as

soon as possible after he or she becomes aware of the possible contravention.

Sections 17.4 to 17.6 of the Elections Act, R.S.O. 1990, Chap. E.6

Restrictions on use of information

17.4 (1) A person who obtains information, directly or indirectly, from the permanent register or from a list of electors prepared from the permanent register,

- (a) shall use it only for electoral purposes;
- (b) shall not use it for commercial purposes; and
- (c) may disclose it to others only after obtaining their written acknowledgment that they are bound by the restrictions in this subsection. 1998, c. 9, s. 15.

Scope

(2) Subsection (1) applies,

- (a) whether the information was obtained under section 17.3, under subsection 19 (3) or in some other way; and,
- (b) whether the person obtained it in printed or electronic format or examined it in either format without obtaining a copy. 1998, c. 9, s. 15.

Downloading

(3) A person who obtains information from the permanent register in electronic format shall not reproduce, store or transmit any part of the information by electronic means for any purpose. 1998, c. 9, s. 15.

Exception

(4) Subsection (3) does not apply to,

- (a) a person or party who obtains the information under section 17.3; or
- (b) a person or entity who obtains the information from a person or party described in clause (a), if there is compliance with clause (1) (c). 1998, c. 9, s. 15.

Guidelines

17.5 The Chief Election Officer may provide guidelines for compliance with section 17.4 and publish them,

- (a) in *The Ontario Gazette*; and
- (b) on a website on the Internet. 1998, c. 9, s. 15.

Policy re information from permanent register or list of electors

17.6 (1) Every registered party shall develop and implement a policy to ensure that its candidates, members of the Assembly, employees and agents comply with section 17.4 and any guidelines provided under section 17.5. 1998, c. 9, s. 15.

Disclosure of policy to Chief Election Officer

(2) The party shall disclose the policy to the Chief Election Officer on his or her request. 1998, c. 9, s. 15.

Publication of policy and discrepancies

(3) The Chief Election Officer is entitled to make public,

- (a) a policy disclosed under subsection (2);
- (b) any discrepancies among,
 - (i) the policy,
 - (ii) the guidelines, if any, provided under section 17.5, and
 - (iii) the actual practices of the party and of its candidates, members of the Assembly, employees and agents. 1998, c. 9, s. 15.

Independent candidates and members

(4) Subsections (1), (2) and (3) also apply to independent candidates and members of the Assembly, with necessary modifications. 1998, c. 9, s. 15.