



NATIONAL ASSEMBLY OF QUÉBEC

FIRST SESSION

FORTY-THIRD LEGISLATURE

Bill 38

**An Act to amend the Act respecting
the governance and management of
the information resources of public
bodies and government enterprises
and other legislative provisions**

Introduction

**Introduced by
Mr. Éric Caire
Minister of Cybersecurity and Digital Technology**

**Québec Official Publisher
2023**

EXPLANATORY NOTES

This bill makes various amendments to the Act respecting the governance and management of the information resources of public bodies and government enterprises and to the Act respecting the Ministère de la Cybersécurité et du Numérique.

The bill specifies, in particular, that the Minister of Cybersecurity and Digital Technology assumes the leadership of the Public Administration's digital transformation and cybersecurity. The bill also tasks the Minister with ensuring that government actions are cohesive and concordant in matters of cybersecurity and digital technology and provides that the Minister must take part in the development of measures and in ministerial decisions in these areas. With regard to public bodies, the bill expressly establishes their obligation to apply the guidelines, strategies, policies, standards, directives, rules and application instructions made under the Act respecting the governance and management of the information resources of public bodies and government enterprises and provides that responsibility for ensuring that this obligation is complied with is incumbent on the body's most senior officer.

The bill assigns to the Minister the responsibility for proposing to the Government a portfolio of priority resource information projects in order to establish government priorities as regards public bodies' digital transformation initiatives. The bill provides that public bodies responsible for the projects included in the government priorities must give priority to carrying out those projects. Furthermore, the Minister is empowered to make a directive whose purpose is, among others, to establish rules to ensure centralized governance of priority projects portfolio management, including the follow-up of such projects. Such a directive must be approved by the Government.

The bill also provides for various measures to enhance and standardize information security practices. To that end, the bill empowers the Minister to make an order setting out the obligation for any public body the Minister designates to call on the services of the Minister to carry out cybersecurity activities. The Minister is also empowered, in certain circumstances, to order a public body to remove from its infrastructure or from its systems any software, application or other information asset that the Minister determines.

In addition, the bill authorizes the Government to provide, on the joint recommendation of the Minister and the minister responsible for the administration of the Act governing a government enterprise, that all or part of certain provisions of the Act respecting the governance and management of the information resources of public bodies and government enterprises relating to information security apply to such an enterprise.

The bill also makes the Minister responsible for providing public bodies with the certification, directory and electronic signature services that the Government determines by order. In particular, the bill provides that such an order may, for the purposes of its implementation, transfer to the Minister a public body's information assets as well as the resulting obligations. The bill also provides that the Minister may provide any other information resource service to meet a specific need of a public body.

Moreover, the bill enables the Government to authorize the implementation of a pilot project aimed at studying, testing or innovating in the areas of cybersecurity or digital technology, or at defining standards applicable to those areas. It also replaces the obligation, for a public body designated as an official source of government digital data, to obtain the approval of the Commission d'accès à l'information du Québec for the rules that the body must establish for its governance in respect of personal information by an obligation to transmit such rules to the Commission.

Lastly, the bill makes certain consequential amendments to the Act respecting the Ministère de la Justice and contains miscellaneous, transitional and final provisions.

LEGISLATION AMENDED BY THIS BILL:

- Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03);
- Act respecting the Ministère de la Cybersécurité et du Numérique (chapter M-17.1.1);
- Act respecting the Ministère de la Justice (chapter M-19).

Bill 38

AN ACT TO AMEND THE ACT RESPECTING THE GOVERNANCE AND MANAGEMENT OF THE INFORMATION RESOURCES OF PUBLIC BODIES AND GOVERNMENT ENTERPRISES AND OTHER LEGISLATIVE PROVISIONS

THE PARLIAMENT OF QUÉBEC ENACTS AS FOLLOWS:

ACT RESPECTING THE GOVERNANCE AND MANAGEMENT OF THE INFORMATION RESOURCES OF PUBLIC BODIES AND GOVERNMENT ENTERPRISES

1. Section 5 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03) is amended by adding the following paragraph at the end:

“It may also, on the joint recommendation of the Minister of Cybersecurity and Digital Technology and the minister responsible for the administration of the Act governing a government enterprise referred to in section 4, determine that all or part of the provisions of Chapter II.2, of the provisions of any regulation made under section 22.1.1 or of the guidelines, strategies, policies, standards, directives, rules or application instructions related to information security made under this Act apply to such an enterprise, on the conditions it determines.”

2. The Act is amended by inserting the following section after section 5:

“5.1. A public body must apply the guidelines, strategies, policies, standards, directives, rules and application instructions made under this Act.

The responsibility for ensuring that that obligation is complied with is incumbent on the chief executive officer of the public body, who must take measures to make the obligation known to the body’s personnel members and to ensure that they comply with it.

For the purposes of this Act, the chief executive officer of the public body is the person having the highest administrative authority, such as the deputy minister, the president, the director general or any other person responsible for the day-to-day management of the body. However, in the case of a public body referred to in subparagraph 4 or 4.1 of the first paragraph of section 2, the chief executive officer of the body is the board of governors or, in the case of a school board governed by the Education Act for Cree, Inuit and Naskapi Native Persons (chapter I-14), the council of commissioners.

3. Section 8 of the Act is amended by striking out the third paragraph.

4. The Act is amended by inserting the following sections after section 12.5:

“12.5.1. The Minister may, by order, set out the obligation for a public body the Minister designates to call on his services to carry out cybersecurity activities, according to the conditions and procedures determined by the Minister.

“12.5.2. The Minister may, by any means, and for the purpose of supporting a public body if a breach or the risk of a breach referred to in the second paragraph of section 12.2 occurs, order the body to remove from its infrastructures or from its systems any software, application or other information asset that the Minister determines.

The power provided for in the first paragraph may only be exercised in either of the following cases:

(1) where the Minister considers that urgent action is immediately required in the area of cybersecurity or that there is a risk of irreparable harm to an information resource or to information under the responsibility of the public body concerned; or

(2) where the Minister considers that urgent action is required within a short period of time in the area of cybersecurity.

In the case provided for in subparagraph 2 of the second paragraph, the Minister may exercise the power provided for in the first paragraph only following thorough and documented verification. In addition, the Minister may not exercise such a power without there first being a consultation between the government chief information security officer and the deputy chief information security officer attached to the body and without notifying the chief executive officer of the public body concerned beforehand of the Minister’s intention to do so.”

5. Section 12.6 of the Act is amended by inserting the following paragraph after paragraph 4:

“(4.1) making tools and best practices in that area available to public bodies and informing the Minister of the results observed;”.

6. Section 12.8 of the Act is amended by inserting “, in accordance with the guidelines defined by the Minister concerning digital transformation initiatives” after “must” in the first paragraph.

7. The Act is amended by inserting the following sections after section 12.8:

“12.8.1. Each year, the Minister proposes to the Government, within 60 days after the investment and expenditure plan for the information resources of public bodies referred to in section 16.1 is tabled in the National Assembly, a portfolio of priority information resource projects in order to establish government priorities as regards public bodies’ digital transformation initiatives.

Subject to obtaining the authorizations required in accordance with this Act, a public body must give priority to the carrying out of any project included in the government priorities and for which the body is responsible.

The Minister may make a directive specifying guidelines regarding prioritization criteria for public bodies’ information resource projects and establishing rules to ensure centralized governance of priority projects portfolio management, including as regards project follow-up.

A directive made under this section must be approved by the Government and is applicable on the date specified in the directive. Once approved, the directive is binding on the public bodies concerned and the rules it establishes apply to those bodies in addition to the rules already applicable to them under this Act, in particular as regards reporting and audits.

“12.8.2. The Minister presents to the Government, at the time the Minister considers appropriate, a consolidation of the progress reports on the information resource projects of public bodies included in the portfolio of priority projects.”

8. Section 12.9 of the Act is amended

(1) by inserting the following paragraph after paragraph 3:

“(3.1) keeping up to date a consolidation of the progress reports on the information resource projects of public bodies included in the portfolio of priority projects;”;

(2) by striking out paragraph 5.

9. Section 12.12 of the Act is amended by inserting the following subparagraph after subparagraph 8 of the first paragraph:

“(8.1) proposing strategies to the Minister to foster an open government approach and seeing that they are implemented; and”.

10. Section 12.16 of the Act is amended

(1) by replacing “have the rules approved by” in subparagraph 2 of the first paragraph by “send them to”;

(2) by striking out the last sentence of the second paragraph.

11. Section 19 of the Act is amended by adding the following paragraph at the end:

“The Minister assumes the leadership of the Public Administration’s digital transformation and cybersecurity.”

ACT RESPECTING THE MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE

12. Section 2 of the Act respecting the Ministère de la Cybersécurité et du Numérique (chapter M-17.1.1) is amended by inserting the following paragraph after the first paragraph:

“The Minister must, in the areas of cybersecurity and digital technology, ensure that government actions are cohesive and concordant and must, to that end, take part in the development of measures and in ministerial decisions regarding these matters, and give an opinion whenever the Minister deems it appropriate.”

13. Section 4 of the Act is amended

(1) by inserting “, the conditions for their use, including the responsibilities of the Minister and users” after “extent” in the third paragraph;

(2) by adding the following paragraph at the end:

“The Minister may provide any other information resource service to a public body to meet a specific need of such a body, where the latter so requests.”

14. The Act is amended by inserting the following section after section 5:

5.1. The Minister provides public bodies with certification services, including the related directory services, and the electronic signature services that the Government determines.

An order made under the first paragraph determines the services covered, the terms and conditions under which they are to be provided, and the cases in which and conditions on which a public body is required to call on those services to meet its needs. The order may authorize the Minister to delegate certain functions relating to such services to a public body. To enable its implementation, the order may also provide for the transfer to the Minister of a public body’s information assets as well as of the resulting obligations.

Where an order made under the first paragraph concerns certification and directory services, it must contain the policy statement provided for in section 52 of the Act to establish a legal framework for information technology (chapter C-1.1).”

15. Section 7 of the Act is amended by replacing “section 4 and” by “sections 4 and 5.1 as well as”.

16. The Act is amended by inserting the following section after section 10:

“10.1. The Government may authorize the Minister to implement a pilot project aimed at studying, testing or innovating in the areas of cybersecurity or of digital technology, or at defining standards applicable to those areas. Such a project may involve public bodies or government enterprises within the meaning of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03), any other enterprise, or individuals.

In compliance with the applicable legislative provisions, in particular regarding the protection of personal information and of privacy, the Government determines the standards and obligations applicable within the scope of a pilot project. It also determines the monitoring and reporting mechanisms applicable within the scope of a pilot project.

A pilot project is established for a period of up to three years which the Government may extend by up to one year. The Government may modify or terminate a pilot project at any time.

The results of a pilot project are to be published on the website of the Ministère de la Cybersécurité et du Numérique not later than one year after the end of the pilot project.”

ACT RESPECTING THE MINISTÈRE DE LA JUSTICE

17. Section 32.1 of the Act respecting the Ministère de la Justice (chapter M-19) is amended by striking out “the certification required to ensure the security of electronic exchanges involving the Government, government departments and government bodies, within the scope of functions delegated pursuant to section 66 of the Public Administration Act (chapter A-6.01), or” in paragraph 2.

MISCELLANEOUS, TRANSITIONAL AND FINAL PROVISIONS

18. The Directive sur les services de certification offerts par le gouvernement du Québec (French only) approved by Order in Council 6-2014 dated 15 January 2014 ceases to have effect on the coming into force of an order made under section 5.1 of the Act respecting the Ministère de la Cybersécurité et du Numérique (chapter M-17.1.1.), enacted by section 14 of this Act, for the same purpose.

19. Any public body designated to act as an official source of government digital data in accordance with an order made under section 12.14 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03) may exercise its function as a source once it has complied with the obligations set out in section 12.16 of that Act, as amended by section 10 of this Act.

20. The provisions of this Act come into force on (*insert the date of assent to this Act*), except those of section 17, which come into force on the date to be set by the Government.

