



NATIONAL ASSEMBLY OF QUÉBEC

FIRST SESSION

FORTY-SECOND LEGISLATURE

Bill 95
(2021, chapter 22)

**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**

**Introduced 5 May 2021
Passed in principle 1 June 2021
Passed 9 June 2021
Assented to 10 June 2021**

**Québec Official Publisher
2021**

EXPLANATORY NOTES

This Act amends mainly the Act respecting the governance and management of the information resources of public bodies and government enterprises.

In the area of information security, the Act, in particular, requires public bodies to ensure the security of the information resources and the information they hold or use. If a breach of the confidentiality, availability or integrity of the information resources or information has occurred or if such a risk is apprehended, the bodies have an obligation to take all measures aimed at correcting the impacts of such a breach or reducing the risk of a breach. Under the Act, the Chair of the Conseil du trésor also has all the powers necessary to support public bodies if such a breach or risk of a breach occurs, including the power to enter into agreements with any person or any body in Canada or abroad.

In the area of digital transformation, the Act notably provides that a public body must establish a digital transformation plan, the terms of which are determined by the Chair of the Conseil du trésor.

The Act also establishes a new framework for the management of government digital data held by public bodies. It provides that such data constitute a strategic information asset of the Government's digital heritage, and that their mobility and valorization for administrative or public service purposes the Act defines, taking into account the data's nature and characteristics, and the rules which otherwise govern access to them and protect them, are of government-wide interest.

The new management framework established by the Act allows the Government to designate official sources of government digital data. The official sources of government digital data may, where necessary for an administrative or public service purpose, collect digital data from public bodies, use the data and communicate them to those bodies, as well as collect information from any person, including personal information. Under the Act, the Government must, in particular, specify the data concerned and the administrative or public service purposes for which such data may be the subject of a mobility or valorization authorization. The Act establishes that the designation of an official source of government digital data is made

on the joint recommendation of the Chair of the Conseil du trésor and the minister responsible for the public body that holds the data concerned, except where certain data are held by the Minister of Health and Social Services or by any public body within the Minister's portfolio, in which case the official source of government digital data is designated on the recommendation of that Minister.

Under the Act, specific rules apply where the government digital data in question include personal information. Among other things, in such a case, the purposes specified by the Government must be in the public interest or to the benefit of the persons concerned. The Act also provides that a public body designated as an official source of government digital data must make an evaluation of the privacy factors, establish governance rules relating to such information that must be approved by the Commission d'accès à l'information and submit a report to the Commission every year on the personal information collected, used or communicated.

In order to implement the new measures, the Act amends the governance framework applicable to information resources. The Act creates the positions of government chief information security officer, government chief digital transformation officer and government digital data manager. It determines the responsibilities related to the positions and provides that those responsibilities are to be assumed by the chief information officer. The officer is given a greater role with respect to public bodies, including that of making application instructions, communicating expectations, overseeing the implementation of the obligations under the Act, authorizing the mobility or valorization of data and requiring information or reports concerning the bodies' activities. The Act also creates the positions of deputy chief information security officer and delegated manager of government digital data and determines the related responsibilities. With some exceptions, those responsibilities are assumed by the public bodies' information officers, whose designation conditions are also amended.

Under the Act, the government digital data manager may entrust a public body with the mandate to circulate open data or a dataset in an open document format. The Government is also given the regulatory powers to oversee the management of government digital data, including the power to exclude data from the application of certain provisions, determine data quality standards and establish rules applicable to public bodies covered by a data mobility or valorization authorization.

The Act reinforces the role of the Chair of the Conseil du trésor with respect to public bodies, in particular by giving the Chair powers to establish control mechanisms, conduct audits and designate a person to verify compliance under the Act.

The Act amends the Public Administration Act to detail the functions of the Chair of the Conseil du trésor in connection with the new framework. For measures on the mobility and valorization of government digital data to be applied, the Act also amends the specific information protection plans provided for by the Tax Administration Act, the Health Insurance Act and the Act respecting health services and social services.

Lastly, the Act amends the Act to establish a legal framework for information technology to regularize certain electronic document signature processes by representatives of a department or body. The Act also includes miscellaneous and transitional provisions, one of which retroactively validates the electronic signature of those documents, as well as a provision that postpones until 13 June 2026 the obligation of the Chair of the Conseil du trésor to report to the Government on the carrying out of the Act respecting the governance and management of the information resources of public bodies and government enterprises and the advisability of maintaining it in force or amending its provisions.

LEGISLATION AMENDED BY THIS ACT:

- Tax Administration Act (chapter A-6.002);
- Public Administration Act (chapter A-6.01);
- Health Insurance Act (chapter A-29);
- Act to establish a legal framework for information technology (chapter C-1.1);
- Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03);
- Act respecting health services and social services (chapter S-4.2).

Bill 95

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 1 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03) is replaced by the following section:

“1. The object of this Act is to establish a framework for the governance and management of information resources applicable to public bodies and government enterprises that focuses specifically on

(1) offering individuals and enterprises simplified, integrated and quality services based on information technologies, including digital technologies, while ensuring the preservation of government digital heritage;

(2) optimizing the management of information resources and public services by encouraging pooling, among other things, of know-how, information, systems, infrastructures and resources;

(3) ensuring proper protection of the information resources of public bodies used to support the delivery of the State’s public services or the carrying out of its missions;

(4) establishing optimal governance and management of digital government data to simplify access to public services by individuals and enterprises, better support government action, increase the performance and resilience of the public administration and enhance the quality and protection of such data;

(5) coordinating public bodies’ digital transformation initiatives to offer fully digital public services;

(6) ensuring rigorous and transparent management of the amounts allocated to information resources;

(7) promoting the use of best practices in the governance and management of information resources and the development of government expertise in information technologies, including digital technologies; and

(8) fostering the implementation of guidelines and strategies common to all public bodies.”

2. Section 2 of the Act is amended by inserting “, which form the Public Administration for the purposes of this Act” at the end of the introductory clause of the first paragraph.

3. Section 7 of the Act is amended

(1) in paragraph 0.1,

(a) by inserting “Chair of the” after “submitting to the”;

(b) by inserting “, including for the digital transformation of the Public Administration, and proposing the means for its implementation” at the end;

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

“(1.1) making and sending to public bodies application instructions with respect to information resources with which the public bodies must comply;”;

(3) by inserting “Chair of the Conseil du trésor and the” after “advising the” in paragraph 2;

(4) by striking out paragraph 6;

(5) by inserting “Chair of the” after “informing the” in paragraph 7;

(6) by inserting the following paragraph after paragraph 7:

“(7.1) developing expertise with respect to information resources, in particular information security, digital transformation and information technologies, including digital technologies, so as to offer services, advice or support to public bodies and to strengthen the State’s know-how in such matters;”;

(7) by replacing “and all the” in paragraph 8 by “, or the pooling or sharing of such technologies, as well as”;

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

“For the purposes of this Act, “application instruction” means any instruction given in writing that is related to the carrying out of activities, the fulfillment of responsibilities or the application of measures with respect to information resources.”

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

“7.1. The chief information officer acts, for the Public Administration, as

(1) government chief information security officer, by assuming the responsibilities under section 12.6;

(2) government chief digital transformation officer, by assuming the responsibilities under section 12.9; and

(3) government digital data manager, by assuming the responsibilities under section 12.12.

The chief information officer may delegate in writing to a person under the officer’s direction the exercise of any of the responsibilities the officer assumes.”

5. Section 8 of the Act is amended

(1) by replacing “, after consultation with the chief information officer, designates an information officer within the department” in the first paragraph by “designates, from among the members of the management personnel who report directly to his or her deputy minister and after a recommendation from the chief information officer, an information officer”;

(2) by replacing “body after consultation with” in the second paragraph by “public body after a recommendation from”.

6. Section 10.1 of the Act is amended, in the first paragraph,

(1) by replacing “governance and management rules established under this Act and that the guidelines determined under the second paragraph of section 21 are implemented” in subparagraph 1 by “guidelines, strategies, policies, standards, directives, rules and application instructions made under this Act”;

(2) by inserting “and on compliance with the obligations under this Act” at the end of subparagraph 3;

(3) by replacing “and all” in subparagraph 8 by “or the pooling or sharing of such technologies, as well as”;

(4) by inserting the following subparagraphs after subparagraph 9:

“(9.1) acting as deputy chief information security officer by assuming the responsibilities under section 12.7;

“(9.2) acting as delegated manager of government digital data by assuming the responsibilities under section 12.13, except where the incumbent minister of the department to whom the delegated manager reports or the chief executive officer of a public body who is so authorized by the Conseil du trésor designates

another person as delegated manager of government digital data, following the rules set out in section 8 for the designation of the information officer, with the necessary modifications; and”.

7. The Act is amended by inserting the following chapters after Chapter II.1:

“CHAPTER II.2

“INFORMATION SECURITY

“12.2. Every public body must ensure the security of the information resources and the information that it holds or uses under the obligations governing it, in keeping with the guidelines, strategies, policies, standards, directives, rules and application instructions made under this Act.

Where a public body becomes aware that an information resource or information under its responsibility is or has been the subject of a breach of confidentiality, availability or integrity, or that a risk of such a breach is apprehended, the body must take all measures to correct the impacts or reduce the risk of such a breach.

If such a public body becomes aware or apprehends that an information resource or information of another public body may experience such a breach, the public body may communicate to the other public body any information, including personal information, considered necessary for correcting the impacts or reducing the risk of such a breach.

“12.3. A public body must, at the request of the government chief information security officer, communicate to the officer without delay any information, including personal information, even if the information must be generated or its communication involves extraction operations, if such communication is necessary for taking measures to correct the impacts of a breach referred to in the second paragraph of section 12.2 or to reduce the risk of such a breach.

“12.4. The Chair of the Conseil du trésor may use information referred to in section 12.3 to support public bodies if a breach or the risk of a breach referred to in the second paragraph of section 12.2 occurs, and the Chair has all the powers necessary to that end, including the power to enter into agreements, in accordance with the applicable legislative provisions, with any person or any body in Canada or abroad where the Chair considers it necessary to ensure information security.

The Chair of the Conseil du trésor may communicate to those persons or bodies the information referred to in the first paragraph that is necessary to prevent, detect or reduce the impacts in the event of a breach or the risk of a breach.

“12.5. The Chair of the Conseil du trésor maintains an administrative unit specialized in information security within the secretariat of the Conseil du trésor. The unit is under the direction of the government chief information security officer.

“12.6. The government chief information security officer assumes the following responsibilities:

- (1) directing government action with respect to information security;
- (2) recommending to the Conseil du trésor rules to ensure information security, including authentication and identification rules, and recommending to the Chair of the Conseil du trésor performance targets applicable to public bodies with respect to information security;
- (3) establishing the government digital data security classification model based on the data’s nature, characteristics and use, and the rules governing them, and obtaining approval for the model from the Conseil du trésor;
- (4) communicating expectations to public bodies with respect to information security and making application instructions for them;
- (5) overseeing the implementation by public bodies of the information security obligations resulting from the application of this Act, seeing to compliance with those obligations and evaluating the measures taken by public bodies in that area;
- (6) reporting to the Chair of the Conseil du trésor, according to the conditions and procedures determined by the latter, on performance target results as well as on compliance with obligations and making any necessary recommendation; and
- (7) exercising any other function assigned by the Chair of the Conseil du trésor or by the Government.

“12.7. A deputy chief information security officer assumes the following responsibilities with respect to the public bodies to which the deputy is attached:

- (1) supporting the government chief information security officer in taking responsibility for government action with respect to information security;
- (2) applying, under the direction of the government chief information security officer, the standards, directives, rules or application instructions related to information security made under this Act;
- (3) ensuring the protection of information resources and information, in particular by managing risks and vulnerabilities and by implementing measures to provide protection against any form of breach such as threats or cyber attacks;

(4) taking any action required in the event of a breach of the protection of information resources and information;

(5) making specific application instructions with respect to information security for those bodies;

(6) overseeing the implementation of the information security obligations under this Act, seeing to compliance with those obligations and evaluating the measures taken by those bodies in that area; and

(7) reporting on his or her management to the government chief information security officer and sending that officer any information required, according to the procedure determined by the Chair of the Conseil du trésor.

If the provisions of an application instruction of the government chief information security officer made under paragraph 4 of section 12.6 are incompatible with the provisions of an application instruction of the deputy chief information security officer made under subparagraph 5 of the first paragraph concerning the same object, the provisions of the former prevail.

“CHAPTER II.3

“DIGITAL TRANSFORMATION

“**12.8.** A public body must establish a digital transformation plan and send it to the government chief digital transformation officer.

The Chair of the Conseil du trésor determines the information to be included in the plan, the period it covers, its form and the intervals at which it must be reviewed.

The Chair of the Conseil du trésor may ask a public body to make any amendment to its digital transformation plan that the Chair considers necessary to ensure it is consistent with the government digital transformation strategy.

“**12.9.** The government chief digital transformation officer assumes the following responsibilities:

(1) advising the Chair of the Conseil du trésor with respect to digital transformation, in particular by proposing guidelines, strategies, action plans and initiatives for optimizing and simplifying the services offered to individuals and enterprises, supporting the State’s missions and increasing the Public Administration’s performance;

(2) making tools, services and expertise for supporting digital transformation available to public bodies;

(3) presenting a portfolio of priority projects to the Conseil du trésor every year for accelerating the Public Administration’s digital transformation;

(4) evaluating action taken by public bodies to achieve the Government's digital transformation vision, in particular on the basis of information collected from the bodies and by conducting any appropriate follow-ups;

(5) proposing strategies to the Chair of the Conseil du trésor to foster an open government approach and seeing that they are implemented; and

(6) exercising any other function assigned by the Chair of the Conseil du trésor or by the Government.

“CHAPTER II.4

“GOVERNMENT DIGITAL DATA

“DIVISION I

“GENERAL PROVISIONS

“§1. — *Principles and definitions*

“12.10. Government digital data constitute a strategic information asset of the Government's digital heritage. The data's mobility and valorization within the Public Administration for administrative or public service purposes, taking into account their nature, characteristics and the access and protection rules which otherwise govern them, are of government-wide interest.

For the purposes of this Act,

(1) “government digital data” means any information inscribed on a technological medium, including a digital medium, held by a public body, excluding

(a) information under the control of a court of justice or another public body exercising adjudicative functions; and

(b) any information or category of information determined by Government regulation, in particular information that may be covered by a restriction to the right of access under the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1);

(2) “administrative or public service purposes” means any of the following purposes:

(a) the optimization or simplification of services offered to citizens or enterprises;

(b) support to the various missions of the State, to the provision by more than one public body of common services or to the carrying out of missions common to more than one public body;

(c) the accomplishment of a mandate assigned under an Act or a government-wide initiative;

(d) the planning, management, assessment or control of resources, programs or government services;

(e) the production of information in support of the decision-making of a minister or the Government;

(f) the verification of a person's eligibility to a program or measure; or

(g) research and development;

(3) "mobility" means the communication or transmission of government digital data between public bodies for an administrative or public service purpose;

(4) "valorization" means the development of government digital data within the Public Administration for an administrative or public service purpose, excluding sale of the data or any other form of alienation.

The first paragraph must not be interpreted as having the effect of changing public bodies' obligations in respect of personal information that they hold or a person's rights in respect of such information.

"12.11. The powers conferred by this chapter must be exercised in a manner consistent with respecting the right to privacy and the principle of transparency and with promoting public confidence in measures to ensure the security, confidentiality, availability and integrity of government digital data.

"§2. — Management of government digital data

"12.12. The government digital data manager assumes the following responsibilities:

(1) advising the Chair of the Conseil du trésor with regard to government digital data, in particular regarding their mobility and valorization;

(2) keeping up to date a consolidation of the inventories of such data that public bodies must keep in accordance with the regulation made under paragraph 1 of section 12.21 and identifying the data that have a mobility or valorization potential;

(3) developing and implementing data mobility or valorization strategies;

(4) authorizing, for any administrative or public service purpose specified in an order made under section 12.14, the mobility or valorization of the government digital data concerned in keeping, as applicable, with the mobility or valorization strategies;

(5) ensuring the application of the data security classification model established by the government chief information security officer under paragraph 3 of section 12.6, and of the quality standards for government digital data determined by the Government under paragraph 2 of section 12.21;

(6) controlling the quality of government digital data and the measures ensuring their security and requiring for that purpose any information the manager considers necessary from the public bodies holding the data;

(7) seeing to the application of the rules or measures established by the Government under paragraphs 4 and 5 of section 12.21;

(8) supporting and assisting public bodies and delegated managers for government digital data in public bodies in implementing the obligations provided for in this chapter; and

(9) exercising any other function assigned by the Chair of the Conseil du trésor or the Government.

Every public body must send the government digital data manager, within the time and in accordance with the terms determined by the latter, the information required to carry out the consolidation referred to in subparagraph 2 of the first paragraph.

“12.13. A delegated manager for government digital data assumes, in respect of the public bodies to which the manager is attached, the following responsibilities:

(1) supporting those bodies in applying the provisions of this Chapter;

(2) supporting the government digital data manager in the exercise of his or her responsibilities; and

(3) applying any application instruction made by the chief information officer under paragraph 1.1 of section 7, or any rule or measure made by the Government under paragraphs 4 and 5 of section 12.21.

“§3. — *Official source of government digital data*

“12.14. The Government may, on the joint recommendation of the Chair of the Conseil du trésor and the minister responsible for the public body holding the government digital data concerned, designate a public body to act as an official source of government digital data.

An official source of government digital data collects, uses or communicates government digital data, or collects information, including personal information, from any person, where necessary for an administrative or public service purpose.

The Government specifies the government digital data concerned and the administrative or public service purposes for which such data may be the subject of a mobility or valorization authorization. It may determine the public bodies that must collect such data from the source and use them or that must communicate them to the source.

Public bodies referred to in an order made under this section must comply with the rules or measures established by the Government under paragraphs 4 and 5 of section 12.21.

Despite the first paragraph, where the government digital data concerned are held by the Minister of Health and Social Services or by any public body within the Minister's portfolio, the official source of government digital data is designated under this section on the recommendation of that Minister.

“DIVISION II

“SPECIAL PROVISIONS FOR PERSONAL INFORMATION

“**12.15.** Government digital data that include personal information are communicated by any public body to an official source of government digital data where such communication is necessary for the purposes specified in an order made pursuant to section 12.14. Such purposes must be in the public interest or for the benefit of the persons concerned.

Such data are communicated by an official source of government digital data to another public body where such communication is necessary for the purposes specified in such an order.

When such data may be used or communicated in a form that does not allow direct identification of the person concerned, they must be used or communicated in that form.

“**12.16.** The public body designated as an official source of government digital data must, before collecting, using or communicating personal information in the exercise of its function,

(1) make an evaluation of the privacy factors and send the evaluation to the Commission d'accès à l'information; and

(2) establish rules for its governance in respect of personal information and have the rules approved by the Commission.

The rules must include rules applicable to the preservation and destruction of the personal information concerned, the roles and responsibilities of the public body's personnel members with regard to such information over the course of its life cycle and a procedure for dealing with complaints regarding personal information protection. They must be submitted again for approval to the Commission every two years.

“12.17. The public body designated as an official source of government digital data must, for the purposes of this division, submit to the Commission d'accès à l'information a report on the personal information collected, used or communicated within 45 days after the end of each fiscal year containing

(1) a description of the personal information collected or the personal information communicated to the public body and its origin;

(2) the names of the public bodies to which personal information is communicated;

(3) a description of the purposes for which the personal information is collected, used or communicated;

(4) a description of the terms for the communication of the personal information; and

(5) a description of the measures to ensure the protection of the personal information.

“12.18. A public body designated as an official source of government digital data makes public on its website, in a section dedicated to that function, the rules referred to in subparagraph 2 of the first paragraph of section 12.16 and the report referred to in section 12.17. It must promptly send copies of those documents to the government digital data manager.

“12.19. Any person to whom or body to which personal information is communicated by a body designated as an official source of government digital data or by another public body referred to in an order made under section 12.14, in the context of a mandate or contract related to carrying out an administrative or public service purpose specified in such an order and entrusted to the person or body in accordance with section 67.2 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1), must submit to an external audit aimed at ensuring compliance with the highest standards and best practices in matters of information security and protection of such information.

The Chair of the Conseil du trésor may determine the cases and circumstances in which the first paragraph does not apply, and makes the criteria leading to the decision public.

“DIVISION III**“OTHER PROVISIONS**

“12.20. The government digital data manager may entrust a public body with the mandate to circulate open data or a dataset in an open document format.

The public body entrusted with the mandate referred to in the first paragraph acts as an official source of reference data and must, as such, circulate such data or dataset on its website or on another site indicated by the government digital data manager, in accordance with the terms determined by the manager.

The terms may, in particular, pertain to the quality of the data, the required formats for their circulation, the main elements to be documented or other compliance rules. Where the terms include rules for the use of the data or dataset, including any secondary use, the terms are binding on public bodies.

“12.21. The Government may, by regulation,

(1) determine the terms governing the keeping of government digital data inventories by public bodies;

(2) determine quality standards for government digital data based on their nature, characteristics, use and their mobility and valorization potential, as well as, if applicable, special protection standards for those data;

(3) exclude categories of data for the application of this chapter;

(4) determine rules for the mobility or valorization authorization referred to in subparagraph 4 of the first paragraph of section 12.12 given by the government digital data manager and rules applicable to public bodies covered by such an authorization; and

(5) prescribe any other measure necessary for the application of this chapter.”

8. Section 13 of the Act is amended by replacing “an information resource master plan that sets out, among other things, its risk management practices and the measures relating to information resources that will be implemented to achieve its mission and its strategic priorities in keeping with the guidelines determined under the second paragraph of section 21” in paragraph 1 by “, in keeping with the guidelines determined under the second paragraph of section 21, an information resource strategy that sets out its digital transformation plan, its risk management practices and any other information prescribed by the Conseil du trésor”.

9. Section 15 of the Act is amended by replacing “a consolidation of the planning tools obtained from the public bodies to which the information officer is attached” in the second paragraph by “the documentation prescribed by the latter”.

10. Section 16.3 of the Act is amended by inserting “or if it involves the designation of a public body to act as an official source of government digital data under section 12.14” after “trésor” in the first paragraph.

11. The Act is amended by inserting the following sections after the heading of Division III of Chapter III:

“16.6.1. A public body must send the Chair of the Conseil du trésor or the chief information officer any information and any report they require concerning its information resource activities.

It must also send to the government chief digital transformation officer, the government chief information security officer or the government digital data manager any information and any report they require concerning its activities related to their respective fields of jurisdiction.

“16.6.2. A public body must, not later than 10 June 2023 and subsequently every five years, carry out an audit on compliance with the information security obligations under this Act.

“16.6.3. The Chair of the Conseil du trésor may, where warranted by the situation and on the recommendation of the chief information officer, establish control mechanisms and carry out audits to ensure that the objectives of this Act are achieved.

In particular, the Chair may require a public body to establish an evaluation program or an internal audit program, or carry out a comparative cost study.”

12. The Act is amended by inserting the following section after section 22.1:

“22.1.1. The Government prescribes by regulation the terms and conditions of application of sections 12.2 to 12.4. The regulation must, in particular, specify the procedures and the grounds for communications between the government chief information security officer or the deputy chief information security officer and a public body whose resources or information have been the subject of a breach referred to in the second paragraph of section 12.2 or are at risk of such a breach, as well as the conditions for providing proper protection of personal information communicated abroad under section 12.4.”

13. Section 22.2 of the Act is amended, in the first paragraph,

(1) by replacing “conduct an audit to determine whether a public body’s information resource investment and expenditure planning and information resource project management are consistent with the measures established under” by “; if he or she considers it advisable, verify whether a public body complies with the provisions of”;

(2) by replacing “rules and directives issued under it to which the body is subject” by “guidelines, standards, strategies, directives, rules and application instructions made under this Act”.

14. Section 22.4 of the Act is amended

(1) by replacing “. The latter” by “and to the minister responsible for the body being audited. The Chair of the Conseil du trésor”;

(2) by replacing “The Conseil du trésor may also” by “The Chair of the Conseil du trésor may also”;

(3) by adding the following sentence at the end: “All or part of the amount intended for such a body may also be retained or cancelled by the minister responsible, on the recommendation of the Conseil du trésor.”

TAX ADMINISTRATION ACT

15. Section 69.0.0.7 of the Tax Administration Act (chapter A-6.002) is amended by inserting the following subparagraph after subparagraph *b.3* of the first paragraph:

“(b.4) the application of Chapter II.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03);”.

16. The Act is amended by inserting the following section after section 69.0.0.16:

“**69.0.0.16.1.** Information contained in a tax record may be communicated, without the consent of the person concerned, to a public body referred to in 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), where the Agency is designated to act as an official source of government digital data for the purposes of that Act and the information is necessary for an administrative or public service purpose specified by the Government under section 12.14 of that Act.

Information communicated under the first paragraph is accessible only to persons qualified to receive it where such information is necessary for the discharge of their duties.

Such information may be used only for the administrative or public service purposes specified by the Government under section 12.14 of that Act.

Where the information may be communicated then used in a form that does not allow direct identification of the person concerned, it must be communicated then used in that form.”

17. Section 69.1 of the Act is amended by adding the following subparagraph after subparagraph z.9 of the second paragraph:

“(z.10) a public body designated as an official source of government digital data 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), solely to the extent that the information is required for an administrative or public service purpose specified by the Government under that section.”

18. The Act is amended by inserting the following section after section 69.1:

“**69.1.1.** For the purposes of subparagraph z.10 of the second paragraph of section 69.1, the public body must, prior to the communication,

(a) make an evaluation of the privacy factors, with the necessary modifications relating to the information required under this division, and send the evaluation to the Commission d'accès à l'information; and

(b) establish rules for its governance in respect of information obtained under subparagraph z.10 of the second paragraph of section 69.1 and have the rules approved by the Commission.

The first paragraph also applies when the public body uses or communicates information obtained under subparagraph z.10 of the second paragraph of section 69.1 in the exercise of its function.

The rules provided for in subparagraph *b* of the first paragraph must include rules applicable to the preservation and destruction of the information concerned, the roles and responsibilities of the public body's personnel members with regard to such information over the course of its life cycle and a procedure for dealing with complaints regarding information protection. They must be submitted again for approval to the Commission every two years.

The body must also, for the purposes of sections 12.17 and 12.18 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03), take into account the information obtained under subparagraph z.10 of the second paragraph of section 69.1.”

19. The Act is amended by inserting the following section after section 69.5.3:

“**69.5.4.** A public body designated as an official source of government digital data may, without the consent of the person concerned, and only if the information is necessary for an administrative or public service purpose specified by the Government 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), communicate information obtained in accordance with subparagraph z.10 of the second paragraph of section 69.1 to another public body referred to in an order made under section 12.14.”

20. Section 69.8 of the Act is amended by inserting “section 69.0.0.16.1 if the information is not communicated solely to confirm a person’s identity,” after “may be communicated under” in the introductory clause of the first paragraph, and by inserting “and subparagraph z.10 of that second paragraph, solely to the extent that communication of the information is required to confirm a person’s identity” after “of the second paragraph of that section 69.1” in that introductory clause.

PUBLIC ADMINISTRATION ACT

21. Section 77.1 of the Public Administration Act (chapter A-6.01) is amended, in the first paragraph,

(1) by replacing subparagraph 6.1 by the following subparagraph:

“(6.1) ensure the implementation of a strategy for the public administration’s digital transformation, including, as applicable, the implementation of any related plan, and assist public bodies in implementing the strategy;”;

(2) by inserting the following subparagraphs after subparagraph 6.3:

“(6.4) ensure government coordination in matters of information security and establish performance targets applicable to all public bodies to measure their performance in strategic, tactical and operational terms, as well as government efficiency in addressing threats, vulnerabilities and incidents involving information security;

“(6.5) establish information security requirements applicable to public bodies and order them, when required, to implement those requirements to improve government efficiency in that respect;”.

HEALTH INSURANCE ACT

22. The Health Insurance Act (chapter A-29) is amended by inserting the following section after section 65.0.4:

“65.0.4.1. The Board shall use the information obtained for the carrying out of this Act for the purposes of Chapter II.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03).

The Board shall also communicate the information to a public body referred to in 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 where the Board is designated to act as an official source of government digital data under that section and the information is necessary for an administrative or public service purpose specified by the Government in the order, as well as to a public body designated to act as an official source of government digital data under that section and the information is necessary for such a purpose.”

ACT TO ESTABLISH A LEGAL FRAMEWORK FOR INFORMATION TECHNOLOGY

23. The Act to establish a legal framework for information technology (chapter C-1.1) is amended by inserting the following section after section 75:

“75.1. Where it is provided by law that a signature affixed to a document by the representative of a department or body referred to in section 3 of the Public Administration Act (chapter A-6.01) shall be done by means of a process authorized by law, in particular where the law provides that the signature requirements are determined by the Government or the Minister or the body, the signature may, in the absence of such authorization or such requirements, be affixed by means of any process that meets the requirements of article 2827 of the Civil Code.”

ACT RESPECTING HEALTH SERVICES AND SOCIAL SERVICES

24. Section 19 of the Act respecting health services and social services (chapter S-4.2) is amended by adding the following paragraph at the end:

“(20) to a public body referred to in 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), where the institution is designated to act as an official source of government digital data under that section, and the information is necessary for an administrative or public service purpose specified by the Government in the order, as well as to a public body designated as an official source of government digital data under that section, where the information is necessary for such a purpose.”

TRANSITIONAL, MISCELLANEOUS AND FINAL PROVISIONS

25. Section 8 of the Act respecting the governance and management of the information resources of public bodies and government enterprises (chapter G-1.03), as amended by section 5, applies to the first designation of an information officer made after 10 June 2021.

26. The Chair of the Conseil du trésor is exempt from the obligation to submit to the Government, not later than 13 June 2021, the report referred to in the first paragraph of section 47 of the Act respecting the governance and management of the information resources of public bodies and government enterprises concerning the carrying out of that Act and the advisability of maintaining it in force or amending its provisions. The next report must be made to the Government by the Chair of the Conseil du trésor not later than 13 June 2026.

27. Documents signed by the representative of a government department or body referred to in section 3 of the Public Administration Act (chapter A-6.01) before 10 June 2021 are validated, provided the signature was affixed to the document by means of a process other than that authorized under the law, in particular where the law provides that the signature requirements are determined by the Government, the Minister or the body, on the condition that the signature was affixed by any process meeting the requirements of article 2827 of the Civil Code.

28. This Act comes into force on 10 June 2021, except for section 7, to the extent that it enacts sections 12.2 to 12.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises, which comes into force on the date of coming into force of the first regulation made under section 22.1.1 of that Act, enacted by section 12 of this Act.