POLICY

GOVERNANCE FRAMEWORK REGARDING PROTECTION OF PERSONAL INFORMATION

Last updated:
March 25, 2024

The Policy

The Governance Framework Policy regarding Protection of Personal Information (hereinafter referred to as the "Policy") was pursuant to the *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1 (hereinafter referred to as the "*Act*").

As accounting firms, Amyot Gélinas and the members of its group[1] ("Amyot Gélinas" or "we") have a professional and legal obligations to protect the privacy and confidentiality of all information that comes into the possession of all members of our respective teams that relates to the practice of our profession. This policy applies to all Amyot Gélinas staff members, board members, registered students of the Ordre des comptables agréés and volunteers, as the case may be.

This Policy applies throughout the life cycle of the personal information and covers all uses of the information, including the collection, transmission, communication, retention, destruction and de-identification of such information.

Amyot Gélinas maintains and updates a number of internal documents aimed at providing a governance framework for confidentiality of personal information, including the following:

- an employee handbook on professional confidentiality
- a mandatory confidentiality agreement that all employees must sign
- an IT resource usage policy
- the CPA Code of ethics
- a quality management system

Amyot Gélinas undertakes to publish on its website, in clear and simple terms, the information required under this Policy. By using the Amyot Gélinas website, users are regarded as having agreed to the Policy and as having consented to the collection, use, disclosure and retention of the personal information they provide on the website in accordance with the Policy.

You may address any questions or concerns you may have regarding this Policy to the attention of the President of the Information Governance and Security Committee by e-mail or regular post as follows:

President of the Information Governance and Security Committee
confidentialité@amyotgelinas.com

OR

President of the Information Governance and Security Committee
Groupe Amyot Gélinas
124, rue Saint-Vincent
Sainte-Agathe-des-Monts (Québec) J8C 2B1

[1] For the purposes of this Policy, the term "group" refers to all Amyot Gélinas affiliates, namely Amyot Gélinas, s.e.n.c.r.l, Amyot Gélinas Conseil inc. and Le Groupe Amyot, Gélinas inc.

Table of Contents

1 Definitions

For the purposes of this Policy, where a word is undefined, it has the meaning ascribed to it in the *Act*.

2 Roles and responsibilities of Amyot Gélinas personnel

In addition to the roles set out in this Section 2, other specific roles are set out in later section.

2.1. The primary task of the person in charge of the protection of personal information is to ensure that the principles set out in this Policy and in the Act are complied with and applied. That person is also required to oversee proper application of the complaints-handling process set out in Section 8.

2.2. The person in charge of the protection of personal information chairs the proceedings of the Information Governance and Security Committee and holds the title "President of the Information Governance and Security Committee".

2.3. The title, e-mail and postal address of the person in charge of the protection of personal information are as follows:

President of the Information Governance and Security Committee
confidentialité@amyotgelinas.com

OR

To the attention of: President of the Information Governance and Security Committee
Groupe Amyot Gélinas
124, rue Saint-Vincent
Sainte-Agathe-des-Monts (Québec) J8C 2B1

2.4. Amyot Gélinas has set up an Information Governance and Security Committee ("the Committee"), which must, among other things:

- recommend the adoption of governance rules concerning the protection of personal information;
- approve internal documents aimed at providing a governance framework regarding the confidentiality of personal information;
- implement strategies aimed raising the awareness of Amyot Gélinas employees regarding best information security practices;
- support the Person in charge of the protection of personal information in fulfilling his or her responsibilities and obligations under the *Act*.

2.5. Every employee is responsible for protecting personal information obtained in the course of Amyot Gélinas operations. If any employee detects a confidentiality incident, he or she must report it without delay to the President of the Governance and Information Security Committee, using the form provided for this purpose.

2.6. No employee may use any personal information to which that employee has access by virtue of his or her duties for any purpose other than the performance of such duties.

2.7. Amyot Gélinas must ensure all its contracts with suppliers, partners, consultants, professionals or any other company to which it transmits personal information, contain a clause requiring compliance with this Policy and the applicable provisions of the *Act* and its regulations. The following are examples of such third parties:

- providers of services such as cloud software and databases;
- suppliers and hosts of personnel management databases;
- group insurance partners;
- credit rating agencies;
- other relevant sources used in the provision of Amyot Gélinas services;

3 Sensitivity scale and inventory of personal information held by Amyot Gélinas

3.1. In this Policy, personal information means information concerning a natural person (individual) that allows that person to be identified. This Policy does not apply to Information concerning a legal entity.

3.2. Personal information related to a person's position in a company (e.g. name, title, position, address, e-mail address, work telephone number) is not subject to this Policy.

3.3. Amyot Gélinas obtains personal information in a variety of situations, including the following:

- when we provide services, or when a person communicates with us, regardless of the method of communication used (in person, by phone, e-mail or online chat);
- when individuals browse our website;
- in employment-related matters concerning our own employees;
- in matters involving the enforcement of penal and criminal law;
- for statistical purposes;
- when an individual registers for any of our seminars or training sessions.

3.4. The scale for determining personal information sensitivity is set out in Appendix A “Information Sensitivity Assessment Grid”. For that purpose, we propose the following sensitivity levels for assessing various information:

External: Clients

Type of information	Sensitivity
Contact's surname and first name	2
Business name	2
Postal address	2
E-mail address	2
Telephone and fax numbers	2
Date of birth/age	3
Identification numbers or other identifying information with government or regulatory bodies	3
Credit card numbers	3
SIN numbers	3
Partial medicals	3
Language	1
Gender	2
Matrimonial status	2
Sexual orientation	2
Personal relationships	2
Political, religious, social or other affiliations	2
Life-style information	2
Buying practices and consumption patterns	2
Financial or business Information of any kind whatsoever	3
Exclusive commercial information, trade secrets, processes, products or market intelligence	3
Electronic documents, data or communications	3
Copies of identity documents for REQ [Québec enterprise register] updates	3

Internal: Employees

Type of information	Sensitivity
Curriculum vitae	1
Surname, first name	1
Postal address	1
E-mail address	2
Telephone number(s)	2
Date of birth	3
Social Insurance Number (SIN)	3
Ordre des CPA du Québec permit number - CPA (auditor)	0
Ordre des CPA du Québec permit number - CPA (non-auditor)	1
Clic Sécur numbers - access to client files	3
Bank account numbers for direct deposit	3
Online government files if T1 prepared in office	3
Medical information related to work stoppages	3
Photos	1

Employee number	1
Professional accounts and access passwords	3
Financial: salaries, RRSP, RESP, investments, etc.	3
Information on employees' children	3
Taxation (SIN, deductions at source, etc.)	3
Court record	0

HR: Prospective job candidates:

Type of information	Sensitivity
Curriculum vitae	1
Surname, first name	1
Postal address	1
E-mail address	2
Telephone number(s)	2

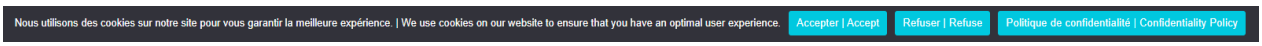
Internal – Service providers:

Type of information	Sensitivity
Contact surnames, first names	1
Business name	1
Tax numbers	0
Postal address	0
E-mail address	2
Telephone number(s)	2
Bank account information for electronic payments	3

4 Web browser cookies

Amyot Gélinas uses cookies and other similar technology on its website to collect usage data. Cookies are small text files created on a user's hard drive to provide a more personalized browsing experience.

Users can refuse the use of cookies from the amyotgelinas.com website:



You can also configure your browser to block cookies, but doing so could affect your website browsing experience.

To obtain visitor statistics and manage cookies, Amyot Gélinas uses Google Analytics, a tool for measuring web traffic and analyzing visits to a website. Through the use of cookies, Google Analytics collects information about your navigation on some or all of our website pages. This information is used for statistical purposes in order to improve your browsing experience.

The following information is collected:

- your truncated IP computer address (your provider modifies your IP address, which prevents connection to it);
- your internet service provider;
- your operating system (i.e.: Mac OS, Windows);
- your device type and model (e.g.: iPhone 12)
- the device's screen resolution;
- browser type and language (e.g.: Chrome, Safari)
- region or municipality, determined by IP address;
- the domain of the previous site visited (e.g.: lapresse.ca);
- point of origin (i.e. banner, e-mail, social network, etc.);
- the pages consulted on our website (consultation sequence, interactions on the page, the date, time, duration and frequency of your visits and your activities (clicks, scrolling, etc.)

This information is stored in the U.S. Google may share the above information with third parties if required to do so by law or when processing information on behalf of third parties. Information is also shared on the Google Ads and Google Search Console accounts of the Conseil de Presse du Québec.

Google's advertising cookies are also used to collect demographic and information on web-user interests. That information cannot be associated with a specific individual. Google states that it will never link the information it collects with any other data or information that it stores.

For further information regarding the kind of information collected by Google and how it is used, consult Google's Privacy Policy and Terms of Use.

If you wish, you can prevent Google from recording information regarding your browsing by installing the Google Analytics deactivation browser add-on on your computer. On your mobile phone you can use a private browser or browse in "incognito" mode.

5 Confidentiality Incidents

5.1. For the purposes of this Policy, "confidentiality incident" means:

(1) access to personal information not authorized by law;
(2) use of personal information not authorized by law;
(3) communication of personal information not authorized by law;
(4) loss of personal information or any other information protection breach.

5.2. Should a confidentiality incident occur, or if there is reason to believe that such an incident has occurred, the employee who detects it must complete the form provided for this purpose and forward it to the Information Governance and Security Committee. The employee must also notify his or her line manager without delay.

5.3. The person in charge of the protection of personal information must record the confidentiality incident in a confidentiality incident register. He or she must also ensure that immediate measures are taken to prevent harm being caused by the incident and by contacting all official contact persons to ensure that the incident is dealt with and that a response plan is deployed, if necessary.

5.4. The person in charge of the protection of personal information, assisted by the Information Governance and Security Committee will analyze the confidentiality incident to determine if there is a risk of serious harm. The assessment will be conducted on the basis of the degree of information sensitivity using the scale set out in Appendix A.

5.5. The confidentiality incident analysis procedure, outlined in a document available on request, is conducted by the Information Governance and Security Committees.

5.6. If the Committee concludes that there is no risk of serious harm, the person in charge of the protection of personal information will record it in the *Register of Confidentiality Incidents* together with recommendations for preventing a recurrence of such an incident.

5.7. In the event of an incident involving a risk of serious harm, the person in charge of the protection of personal information must notify the CAI, all persons concerned and, if applicable, any person or organization that could reduce the risk. The person in charge of the protection of personal information must keep a copy of such notifications on file.

The person in charge of the protection of personal information and the Committee must identify further measures to be taken to limit the risk of injury and make recommendations to prevent a recurrence.

5.8. Should a confidentiality incident involving personal information held by Amyot Gélinas occur, and should that incident present a serious risk of injury, the person in charge of the protection of personal information must notify the *Commission d'accès à l'information* using the form provided for that purpose by the Commission.

5.9. All notices to persons affected by a confidentiality incident must adhere to the model provided in Appendix B of this Policy.

6 Life cycle of personal information

6.1. These rules apply throughout the life cycle of the personal information.

6.2. Before collecting personal information, Amyot Gélinas provides individuals with the information they need to understand the purposes for which the personal information is to be used or disclosed. Consent may be withdrawn or modified regarding the disclosure and use of personal information, subject to applicable legal restrictions.

6.3. Amyot Gélinas collects personal information only where necessary for the proper performance of its activities, particularly in order to:

- provide services to clients;
- carry out activities integral to the operation of Amyot Gélinas ;
- communicate personal information to third parties where necessary, such as to service providers, insurers, tax authorities or any other third party as required by law.

6.4. Amyot Gélinas must ensure that individuals are informed of the purposes for which their personal information is collected and the means by which it is collected.

6.5. Unless the personal information involved is in the public domain, access to such information is restricted to employees who require such information in connection with the performance of their duties.

6.6. The person who has custody of physical files containing personal information must ensure that only persons who actually need that information can access the files.

6.7. Amyot Gélinas has adopted appropriate practices for the storage and processing of data, as well as security measures to protect personal information from unauthorized access.

6.8. When we need to transmit personal information or give third parties access to it, the person in charge of the protection of personal information must ensure that the written agreements prescribed by the *Act* are entered into. He or she must also ensure that all communications of personal information are recorded in accordance with the requirements of the *Act*.

6.9. Amyot Gélinas retains personal information as long as necessary for the purposes for which it was collected, subject to legislative and professional requirements regarding the retention of certain types of information. However, if the information remains useful for statistical purposes, it can be de-identified instead.

7 Staff awareness and training

7.1. Amyot Gélinas has designed information capsules for distribution to all its employees.

7.2. All employees must familiarize themselves with the information capsules upon receipt.

7.3. New employees or employees assigned to new duties must familiarize themselves with the information capsules intended for their new jobs or new duties.

7.4. All employees must individually sign an attestation indicating that the applicable information capsule has been read.

7.5. In addition to information capsules, the person in charge of the protection of personal information must make all persons concerned aware of any new measure aimed at better protecting personal information, including any recommendations made following a confidentiality incident.

8 Complaints-handling process

8.1. Any person who believes that his or her personal information has been inadequately protected by Amyot Gélinas may file a complaint using the form provided in Appendix C.

8.2. Complaints shall be handled on a confidential basis.

8.3. The person in charge of the protection of personal information must review the complaint and determine whether:

- a confidentiality incident has occurred, in which case he or she must trigger the confidentiality incident procedure;
- the complaint indicates a possible breach of an Amyot Gélinas obligation under this Policy or under the *Act* or a regulation enacted thereunder.
- the complaint indicates a breach of any applicable standard;
- the complaint is frivolous pr clearly unfounded.

8.4. In order to analyze the complaint, the person responsible for the protection of personal information may contact the complainant and any employee who could have information that would facilitate the analysis. The person in charge of the protection of personal information may not disclose the name of the complainant unless that information is necessary to analyze the complaint.

8.5. Upon terminating the complaint analysis process, the person in charge of the protection of personal information shall communicate with the complainant in writing setting out the results of the analysis.

9 Privacy impact assessment

9.1. The person in charge of the protection of personal information must assess various privacy-related factors before taking any of the following actions:

(a) embarking on any project involving the acquisition, development or redesign of an information system or the electronic provision of services involving the collection, use, communication, retention or destruction of personal information;

(b) disclosing personal information without the consent of the persons concerned to a person or body that wants to use such information for study, research or statistical purposes; or

(c) communicating personal information outside of Québec.

9.2. At any stage of a project contemplated in the above section 9.1 (a),the person in charge of the protection of personal information may suggest measures for the protection of personal information applicable to the project, such as:

(1) the designation of a person responsible for implementing personal information protection measures;
(2) measures ensuring the protect ion of personal information in any project-related document;
(3) a description of project participant responsibilities aimed at the protection of personal information;
(4) training activities for project participants concerning the protection of personal information

9.3. If the assessment concerns the communication of personal information for study, research or statistical production purposes, the information may not be communicated unless a privacy impact assessment finds that:

(1) the purpose of the study, research or statistical production is achievable only if information is communicated in a form allowing for identification of the persons concerned;

(2) it would be unreasonable to require that the relevant person or body obtain the consent of the persons concerned;

(3) taking into account public interest considerations, the purpose of the study, research or production of statistics far outweighs the impact of the communication and use of the information on the privacy of the persons concerned;

(4) the manner in which the personal information is used is designed to ensure its confidentiality;

(5) only necessary information is disclosed.

9.4. If the assessment involves a situation in which information is communicated, collected used, or retained outside of Québec, Amyot Gélinas must take into account the following factors:

(1) the sensitivity of the information;

(2) the purpose for which the information is to be used;

(3) the information protection measures, including contractual measures, such as;

(4) The legal system in the jurisdiction in which the information is to be communicated, and the applicable personal information protection principles.

The information may be communicated if the assessment indicates that the information would be properly protected, specifically as regards generally accepted personal information protection principles.

9.5. The person in charge of the protection of personal information must take the following steps:

(a) prepare an inventory of the personal information that will be involved in connection with the action requiring assessment;

(b) identify the nature, sensitivity, quantity and purpose of the personal information;

(c) identify the person entitled to access the personal information;

(d) identify the methods used for processing, storing, destroying and de-identifying personal information;

(e) draw up a list of Amyot Gélinas' obligations regarding the contemplated project or action;

(f) consider the following privacy-related factors:

(i) conformity of the project or action with applicable legislation regarding the protection of personal information and compliance with the governing principles;

(ii) identification of the privacy infringement risks of the project or action and assessment of the consequences of any such infringement;

(iii) implementation of risk avoidance strategies or effective risk reduction strategies and their sustainability over time.

(g) determine if, in light of the assessment, the project or action involves too many risks, despite the implementation of risk-avoidance or risk-reduction strategies;

(h) Inform Amyot Gélinas senior management of the results of the assessment;

(i) provide a written report of the assessment.

9.6. A privacy impact assessment conducted pursuant to this Policy must be commensurate with the sensitivity of the information involved, the purpose for which the information is to be used, as well as the quantity, distribution and format thereof. An in-depth assessment is necessary to determine the number of people to be involved, the time to be invested and the documentation to be produced.

10 Communication of information without the consent of the person concerned

10.1 Amyot Gélinas may, without the consent of the person concerned, communicate personal information to:

(a) any person or body if such communication is necessary to perform a mandate or contract for services conferred on such person or body by Amyot Gélinas;

(b) a third party if the communication is necessary to conclude a business transaction to which Amyot Gélinas intends to be a party;

(c) an archive, if the archive is a person carrying on a business involved in the acquisition, preservation and dissemination of documents for their general information value and if the information is communicated in connection with a transfer or deposit of Amyot Gélinas archives;

(d) any person, if the information is in a document that is over 100 years old or if more than 30 years have elapsed since the death of the person concerned. However, unless the person concerned consents, information relating to a person's health may not be communicated before the expiry of 100 years from the date of the document.

10.2. If, without the consent of the person concerned, Amyot Gélinas discloses information as authorized by Section 10.1 (a) of the Policy, Amyot Gélinas must:

(1) confer the mandate or contract in writing;

(2) in the mandate or contract, indicate what measures the mandatary or person performing the contract must take to ensure that the confidentiality of the personal information communicated is protected, that the information is used solely in carrying out the mandate or performing contract and that such information is not retained after termination of such mandate or contract.

The first paragraph of Section 10.2 (2) does not apply if the mandatary or person performing the contract is a public body within the meaning of the *Act respecting Access to document held by public bodies and the Protection of personal information* (c. A-2.1) or is a member of a professional order.

10.3. If. without the consent of the person concerned, and as authorized by Section 10.1 b) of the Policy, Amyot Gélinas communicates personal information, it must have signed a prior agreement with the other party, with express undertakings given by that other party to do the following:

(1) use the information solely for the purposes of concluding the commercial transaction;

(2) not communicate the information without the consent of the person concerned, unless expressly authorized by law;

(3) take the necessary measures to ensure that confidentiality of the information is protected;

(4) destroy the information if the business transaction is not concluded or if its use is no longer necessary for the purposes of finalizing the business transaction.

APPENDIX A – INFORMATION SENSITIVITY ASSESSMENT GRID

SENSITIVITY ASSESSMENT SCALE		
Level	**Classification**	**Characteristics**
Public information		
0	**Public information**	• Publicly accessible, either locally or online. • Requires little security, and disclosure would not result in a compliance breach.
Confidential information: requires authorization to access it. Specific authorization to access identified data is given to designated employees or third-party suppliers.		
1	**Low**	• Requires little security to protect it from a data breach. • The individuals concerned by a disclosure of information do not sustain significant harm.
2	**Medium**	• Requires the same access controls as high-sensitivity data but is accessible by a greater number of users. • The individuals concerned by a disclosure of information may experience consequences, but they will recover with little difficulty.
3	**High**	• Must be secured and monitored to ensure protection against threats. Often subject to compliance regulations as information requiring strict access controls that also minimize the number of users who can access such information. • The individuals concerned by a disclosure of information may experience irreparable or significant or consequences, that may be in insurmountable or, if surmountable, only with great difficulty.

APPENDIX B – MODEL NOTICE TO INDIVIDUAL AFFECTED BY A CONFIDENTIALITY INCIDENT

Sir, Madam,

Amyot Gélinas places great importance on the protection and confidentiality of personal information held in connection with its activities. Although we have implemented security measures to protect such information, we wish to advise you of the occurrence of a confidentiality incident.

On [insert date], an incident [describe the incident in clear and simple language, including the date of the incident]. As your personal information [describe the personal information affected by the incident] was affected, we considered it essential to inform you of the situation and the measures that were put in place to remedy it.

As soon as we became aware of the situation, we were able to [specify what was done to put an end to the incident].

We promptly put measures in place to [control or contain] the risk of adverse consequences. We have actively [describe the action taken to remedy the breach and the preventive measures that were put in place]

You too can reduce the risks by [describe the measures that the person(s) concerned could take to reduce the risk of harm as a possible result of the Incident, or to mitigate the harm].

The Commission d'accès à l'information du Québec has also been advised of the occurrence of the incident.

We are fully aware of the inconvenience this situation may have caused you and we extend our sincerest apologies. Rest assured that maintaining the confidentiality of personal information is a priority for Amyot Gélinas, and that we will strengthen existing measures to prevent any further incidents of such a nature.

If you have any questions, you can contact us at the following address:

Attention: President of the Information Governance and Security Committee
confidentialite@amyotgelinas.com
Groupe Amyot Gélinas
124, rue Saint-Vincent
Sainte-Agathe-des-Monts (Québec) J8C 2B1

APPENDIX C – COMPLAINT FORM

COMPLAINT FORM
Complainant's full name and contact information:
Name of the person(s) concerned (if different):
Date of the incident giving rise to the complaint:
Employee(s) and department(s) concerned:
Description of the circumstances of the incident giving rise to the complaint:
Description of the harm suffered: