cyber eco

Practical Guide: Application of Act 25

An Act to modernize legislative provisions as regards the protection of personal information

May 2022

Table of contents

Part 1

Explanation of the Act to modernize legislative provisions as regards the protection of personal information (Act 25)

1. Main objectives of the Act

The Act to modernize legislative provisions as regards the protection of personal information will make significant changes to privacy laws.
The purpose of this legislation is to give citizens more control over their personal information. It modernizes the legislative framework to adapt it to today's technological reality. To do so, several elements already contained in the European regime are now transposed to the Quebec environment. The adoption of this law makes Quebec a forerunner in the field of technology and personal information protection, as it is the first province in Canada to undertake a reform of its privacy legislation.

The Act has been adopted on September 21, 2021, and will come into effect gradually in three phases. Some provisions will come into force on September 22, 2022, others on September 22, 2023, and the last ones on September 22, 2024.

In fact, it is according to that this document is subdivided according to these different effective dates for ease of reference.

2. New obligations for the private sector and their implementation

1. September 22, 2022

1. Compliance and governance

1. Appointment of a person in charge of the protection of personal information

Section 3.1 of the Act respecting the protection of personal information in the private sector

The person with the highest authority in the organization will be responsible for ensuring compliance and implementation of the Act. This person will be known as the person in charge of the protection of personal information.
However, this function may be delegated in writing, in whole or in part, to any person.

The title and contact information of the person in charge shall be published on the company's website or, if the company does not have a website, made accessible by any other appropriate means.

2. Obligations

1. Notification and recording of privacy incidents

Sections 3.5 to 3.8 of the Act respecting the protection of personal information in the private sector

A record of any confidentiality incidents shall also be kept. This record shall be made available to the Commission d'accès à l'information (hereafter "CAI") upon request.

As examples, these different situations could, among others, be qualified as confidentiality incidents:

a) unauthorized access to personal information;
b) the unauthorized use of personal information;
c) the unauthorized disclosure of personal information; or
d) loss of personal information or any other breach of the protection of personal information.

In addition, organizations will be required to notify CAI **AND** affected individuals of any privacy incident if it involves personal information in their possession **AND** presents a risk of serious harm. For example, serious harm could be reputational damage, credit report damage, identity theft, etc.

2. New obligations for the private sector and their implementation

2. September 22, 2023

1. Compliance and governance

1. Adopt or update policies and practices governing the protection of personal information

   Section 3.2 of the Act respecting the protection of personal information in the private sector

   Businesses will be required to establish and implement policies and practices to guide their protection of personal information. These policies should be proportionate to the nature and importance of the company's activities. They should be written in plain language.

2. Provide a framework for the retention, destruction and anonymization of personal information

   Section 3.2 of the Act respecting the protection of personal information in the private sector

   The policies and practices shall include rules to govern the retention and destruction of personal information. Information about these rules shall be set out in clear and simple terms and published on the organization's website (or otherwise made available).

3. Have a complaints process in place

   Section 3.2 of the Act respecting the protection of personal information in the private sector

   A process for handling privacy complaints shall be included in the policies and practices. This process shall be set out in clear and simple terms and published on the organization's website (or otherwise made available).

2. New obligations for the private sector and their implementation

2. September 22, 2023

2. Obligations

1. Publication of information regarding policies and procedures on the website

   Section 3.2 of the Act respecting the protection of personal information in the private sector

   Information about the company's policies, procedures and practices relating to the protection of personal information shall be posted on its website. If they do not have a website, companies shall make this information available through any other appropriate means.

   This ensures that companies are transparent about the policies and procedures they have adopted.

2. Conducting Privacy Impact Assessments (PIAs) for certain personal information processing

   Section 3.3 of the Act respecting the protection of personal information in the private sector

   For any new information system acquisition, development or redesign project or electronic service delivery project that involves the collection, use, disclosure, retention or destruction of personal information, organizations will be required to conduct a PIA. The PIA will need to be proportionate to the sensitivity of the information affected by the project, the purpose for which it is to be used, its amount, distribution and medium. All of these elements should be considered in the PIA. The person in charge of the protection of personal information within the organization should be consulted at the outset of the project. This person will be able to suggest privacy safeguards to be implemented for the project in question.

2. New obligations for the private sector and their implementation

2. September 22, 2023

2. Obligations

3. Change of consent parameters

Sections 4 and following of the Act respecting the protection of personal information in the private sector

Consent is always required to collect, hold, use or disclose personal information. Consent must be manifest, free, informed and given for specific purposes. However, the requirement for consent will be strengthened by requiring that it be sought for each of these purposes, in clear and simple terms, and separately from any other information provided to the individual.

In addition, when an organization wishes to use or disclose sensitive personal information, consent must be expressly given. This involves an action by the individual to confirm consent, such as checking a box. Personal information is considered sensitive when it has a reasonable expectation of privacy, such as a social insurance number or medical information.

4. Destruction and anonymization of personal information

Section 23 of the Act respecting the protection of personal information in the private sector

Once the company has fulfilled the purposes for which it collected personal information from an individual, it will now have two choices. The first is to destroy the personal information. The second is to anonymize the personal information. However, anonymization must be done with a view to using the anonymized information for a serious and legitimate purpose. Therefore, this choice will not be made without good reason.

It is important to specify that for personal information to be considered de - identified within the meaning of the Act, it must no longer allow a natural person to be identified directly or indirectly, and this, in an irreversible manner. This de-identification must be carried out in accordance with generally recognized best practices and according to criteria to be determined by regulation.

2. New obligations for the private sector and their implementation

2. September 22, 2023

2. Obligations

5. Transfer of personal information outside Quebec

Section 17 of the Act respecting the protection of personal information in the private sector

Before disclosing personal information outside of Quebec, businesses will be required to conduct a PIA which will take into consideration the following:

1) the sensitivity of personal information;
2) the purpose of their use;
3) the safeguards associated with the personal information being disclosed;
4) the legal regime applicable to the location where the personal information is disclosed, specifically the privacy principles that apply.

Once these elements have been assessed, personal information may be disclosed if the assessment demonstrates that the information would benefit from protection that is adequate based on generally accepted privacy principles. The disclosure will also be subject to a written agreement outlining the findings of the PIA and, if necessary, the terms and conditions agreed upon to mitigate the risks identified in the PIA.

These obligations will also apply where an enterprise wishes to delegate the task of collecting, using, communicating or retaining personal information on its behalf to a person or organization outside Quebec.

2. New obligations for the private sector and their implementation

2. September 22, 2023

2. Obligations

6. Implementation of the right to de-index

Section 28.1 of the Act respecting the protection of personal information in the private sector

The right to de-index allows an individual to request that an organization stop the dissemination of one or more of his or her personal information or de-index any hyperlink attached to his or her name that provides access to that information. This request can be made when the release of the information in question contravenes the law or a court order.

The person may also request it when all these conditions are met:

1) the dissemination of the information causes him/her serious harm in relation to his/her right to respect for his/her reputation or privacy;
2) the harm clearly outweighs the public interest in accessing the information or the interest of any person in expressing themselves freely; and
3) actions for cessation of dissemination, reindexing, or deindexing requested do not exceed the measures necessary for the harm to cease.

To validate whether all conditions are met, the company will consider the following elements:

1) if the person concerned is a public figure;
2) if the information concerns the person as a minor;
3) whether the information is current and accurate;
4) the sensitivity of the intelligence;
5) the context of intelligence dissemination;
6) the time elapsed between the release of the information and the request of the person concerned; and
7) if the information relates to criminal or penal proceedings, obtaining a pardon or applying a restriction on access to court records

Where such a request is granted, the person in charge of the protection of personal information will be required to certify, in a written response, that the personal information in question is no longer being disseminated, that the hyperlink is being de-indexed or re-indexed.

2. New obligations for the private sector and their implementation

2. September 22, 2023

3. Sanctions

Sections 90.1 and following of the Act respecting the protection of personal information in the private sector

Companies that do not comply with the obligations set out in the law may be subject to various types of sanctions.

1) **Administrative Monetary Penalties (AMPs):**
   The Commission d'accès à l'information may impose AMPs of up to $10,000,000 or 2% of the company's worldwide turnover.
2) **Criminal Sanctions:**
   The Commission d'accès à l'information may also institute penal proceedings. Thus, the Court of Quebec may impose a fine of up to $25,000,000 or 4% of the company's worldwide turnover.
3) **Punitive Damages:**
   Individuals will also have a private right of action against companies that will allow them to claim punitive damages for intentional or grossly negligent infringement.

2. New obligations for the private sector and their implementation

3. September 22, 2024

1. Obligations

1. Implement measures to facilitate the right to data portability

Section 27 of the Act respecting the protection of personal information in the private sector

The right to data portability allows an individual to obtain a copy of his or her personal information held by an organization in an understandable format. In some cases, this right also allows an individual to request the transfer of his or her personal information from one organization to another. One of the main purposes of this right is to allow individuals to have more control over their personal information.

The Act provides that an enterprise that holds personal information about an individual shall, upon request, confirm the existence of the information and disclose it to the individual, while allowing the individual to obtain a copy of the information. This applies to computerized personal information. The information shall be made available to the individual, upon request, in a structured, commonly used technological format. Finally, this information must be communicated, always at his request, to any person or organization authorized by law to collect such information.

Part 2

Act 25 - Suggested Action Plan

Act 25 - Suggested Action Plan
2022-2024

To be completed by **September 2022**

1. Designate a person in charge of the protection of personal information
2. Create or update policies and practices for the protection of personal information
3. Establish a privacy incident log and notification process
4. Have an inventory of the company's personal information
5. Implement a privacy training program

To be completed by **September 2023**

6. Update policies and practices for the retention, destruction and de-identification of personal information
7. Implement a privacy complaint process to address privacy issues
8. Publish key elements of the privacy governance rules on the company's website
9. Implement a Privacy Impact Assessment (PIA) policy and process for handling personal information
10. Implement a process for obtaining consent to collect, hold, use or disclose personal information
11. Implement a de-indexing process

To be completed by **September 2024**

12. Implement measures to facilitate the right to data portability

Actions to be completed by
September 2022

1. Designate a person in charge of the protection of personal information
2. Create or update policies and practices for the protection of personal information
3. Establish a privacy incident log and notification process
4. Have an inventory of the company's personal information
5. Implement a privacy training program

Designate a person in charge of the protection of personal information

Chronological information

- **Required on September 22, 2022 as per 2.1.1.1**
- **Predecessor:** None, first activity to be completed by September 2022
- **Successors:** Create or update policies and practices to support the governance of personal information and have an inventory of personal information in the organization.

Contents

The person in charge of the protection of personal information is the cornerstone of your program. This is the person with the highest authority in the organization and will be responsible for ensuring compliance and implementation of the Act. Some tasks may be delegated, but the responsibility always remains with the person in charge of the protection of personal information.

Key activities

- Describe the roles and responsibilities of the person in charge of the protection of personal information
- Determine to whom the person in charge of the protection of personal information will report to
- Designate hiring criteria for the person in charge of the protection of personal information
- Ensure the training of the person in charge of the protection of personal information
- Define/modify the governance model based on roles and responsibilities
- Publish the contact information of the person in charge of the protection of personal information publicly (e.g. website)

Designate a person in charge of the protection of personal information

Planning factors

This phase potentially requires a hiring process and therefore sufficient time must be allowed for this activity, especially if the person is not already in the organization. Training may also take some time depending on the skills gap between the person selected and the skills required for the position.

Tip

This first action is critical and is a prerequisite for all other actions that follow. The importance of completing it without delay cannot be overstated.

Available resources

- https://www.caij.qc.ca/dossier/projet-de-loi-n-64-loi-modernisant-des-dispositions-legislatives-en-matiere-de-protection-des-renseignements-personnels
- https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/responsable-protection-renseignements-personnels

Create or update policies and practices for the protection of personal information

Chronological information

- **Required on September 22, 2023 as per 2.2.1.2**
- **Predecessor:** Designate a person in charge of the protection of personal information
- **Successor:** Implement a privacy incident log and reporting process

Contents

The policies and practices surrounding the protection of personal information are critical elements in enabling the sound management of personal information. This activity, while not required until September 22, 2023 in the legislation, must be completed as early as 2022 as its outputs will impact the next activities to be completed by September 2022.

Key activities

- The person in charge of the protection of personal information is the person responsible for ensuring that policies and practices are implemented.
- Develop and update policies and practices to address the following issues:
  - What information is collected, retained, disclosed and destroyed?
  - What is the data retention process?
  - What are the reasons, key factors and parameters for making decisions based solely on automated processing of personal information? Who has access to the data?
  - What is the destruction process?
  - What constitutes a privacy incident?
  - What is the procedure for handling a privacy incident?
  - Who will be notified of an incident (internal/external)?
  - What are the notification deadlines for incidents?

Create or update policies and practices for the protection of personal information

Planning factors

To be initiated as soon as the person in charge of the protection of personal information is hired.

Tip

- If the company does not already have personal information policies and practices or an inventory in place, more effort is required to produce them than simply updating existing policies.
- Use simple policy and practice templates aligned with other organizational policies and practices.

Available resources

- https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/pp/
- https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/politiques-pratiques-gouvernance/
- https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1637173195

Establish a privacy incident log and notification process

Chronological information

- ***Required on September 22, 2022 as per 2.1.2.1***
- **Predecessor:** Create or update policies and practices to support protection of personal information
- **Successor:** Inventorying the company's personal information

Contents

As of September 22, 2022, organizations will be required to notify the Commission d'accès à l'information and affected individuals of any privacy incident involving personal information they hold that poses a risk of serious harm.

Organizations will also be required to maintain a confidentiality incident log which shall be made available to the Commission upon request.

Key activities

- Set up a log to capture details of privacy incidents.
- Establish a record of notifications related to the incident.
- Implement a process for updating records.

Establish a privacy incident log and notification process

Planning factors

Begin planning even if all policies and practices are not 100% finalized. The requirement to have everything in place by September 2022 suggests parallelism in activities to the extent possible.

Tip

- With the help of your legal team and the person in charge of the protection of personal information , conduct a risk analysis of serious harm analysis to determine your legal notification obligations.
- Learn about examples of logs available on the web and integrate them into the existing incident management process.
- Emphasize proper identification of the level of severity of an incident to determine whether external assistance will be required.
- Use a simple spreadsheet template that meets the requirements of the law.

Available resources

- https://www.cai.gouv.qc.ca/incident-de-securite-impliquant-des-renseignements-personnels/
- https://cybereco.ca/wp-content/uploads/2021/10/guide-de-gestion-des-incidents-pmes-pdf.pdf
- https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/incident-de-confidentialite

Have an inventory of the company's personal information

Chronological information

- ***Recommended in connection with the operationalization of the protection of personal information***
- **Predecessor:** Designate a person in charge of the protection of personal information.
- **Successor:** Implement a privacy training program.

Contents

This is required in order to have an inventory of the company's personal information and to ensure that the confidentiality incident logbook accounts for all personal information that must be kept confidential.

Key activities

- Develop an inventory of personal information in IT systems and various information sources, including what is outsourced:
  - Where is the personal information?
  - What types of information are stored?
  - What information is collected?
- Control access and transfer of personal information in accordance with company policies:
  - Who has access to personal information? In what context?
  - Are company policies being followed?
  - What personal information is transferred to third parties?
- Be able to identify the link between personal information and the individuals involved:
  - If an incident occurs; do we know what data is involved and who we should notify?

Have an inventory of the company's personal information

Planning factors

This activity can be done in parallel with the previous activity (confidentiality incident log).

Tip

- It is important to ensure that a complete inventory is completed, as it will be used for the activities required for September 2023 and in particular for those activities information systems activities.
- It will be much less expensive to eliminate information not required for business processes as soon as possible than to ensure compliance.
- Provide a process for continuous updating (when applications are added or changed) and annual review.
- The information and where it is kept must be documented.
- Do not hesitate to change practices when highly confidential information is stored in an inappropriate location (e.g. server, laptop).
- Ensure that only what is required (and no more) is collected, used and retained.
- Have technology solutions in place to make the inventory of personal information as simple and efficient as possible.

Available resources

- https://www.cai.gouv.qc.ca/diffusion-de-linformation/inventaire-des-fichiers-de-renseignements-personnels/
- https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/securite-des-renseignements-personnels/gd_rd_201406/

Implement a privacy training program

Chronological information

- ***Recommended in connection with the operationalization of the protection of personal information***
- **Predecessor:** Have an inventory of company information
- **Successor:** See activities for September 2023

Contents

This activity ensures that all staff have been trained to meet the requirements of the privacy legislation within your organization.

Key activities

- Create a presentation that simply and clearly explains the changes related to privacy and identifies the roles and responsibilities of staff throughout the privacy life cycle.
- Present company policies and practices to employees according to a training schedule.
- Ensure that training is up to date.
- Provide more specific training for employees who will play a key role in implementing the company's privacy program.
- Ensure that policies and practices are followed by employees and document gaps. Adjust the training plan to address identified gaps in employee behaviors.
- Notify and re-train employees who fail to comply with policy obligations.

Implement a privacy training program

Planning factors

There is an effort to ensure the production of training materials. You have to think about the type of session that will depend on the audience you are targeting.

Tip

- Use a simple language, standardized to the company.
- Demonstrate how the protection of personal information does not add to the burden, the consequences of an incident and the importance of complying with company policy.
- It is possible to form reference persons who will also form groups to cover the whole company.
- Use existing resources:
  - The Cybereco CyberKit can be used for certain aspects of outreach.
  - Some members of Cybereco make available artifacts that could help you in your outreach activities.

Available resources

- https://cybereco.ca/cybertrousse/
- https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/securite-des-renseignements-personnels/gd_rd_201406/

Actions to be completed by **September 2023**

6. Update policies and practices for the retention, destruction and de-identification of personal information
7. Implement a privacy complaint process to address privacy issues
8. Publish key elements of the privacy governance rules on the company's website
9. Implement a Privacy Impact Assessment (PIA) policy and process for handling personal information
10. Implement a process for obtaining consent to collect, hold, use or disclose personal information
11. Implement a de-indexing process

Update policies and practices for the retention, destruction and de-identification of personal information

Chronological information

- **Required as per 2.2.1.2 on September 23, 2023**
- **Predecessor**: Have an inventory of company information
- **Successors**: Implement a de-indexing process

Contents

This practice protects the privacy of individuals by ensuring that their personal information held by the company is no longer accessible by either the company or a third party through destruction or anonymization. It is triggered when personal information is no longer being used for its original purpose and when the legally prescribed retention period has expired.

Key activities

- Learn about existing best practices, including the regulatory requirements of the Quebec government.
- Define the provisions of the company's applicable policy on the retention and destruction of personal information.
- Identify the tools to be implemented in the company, ideally by a person whose expertise is recognized in the field.
- In accordance with the retention schedule determined by the company, establish practices for personal information collected by the company as identified in the inventory.
- Implement the practices and verify that the required level of anonymization is achieved.
- Adapt the policy and practices regularly, taking into account changes in laws, regulations, accepted practices and any other relevant aspects.

Update policies and practices for the retention, destruction and de-identification of personal information

Planning factors

Knowledge of best practices in de-identification and proper destruction of personal information is a target that may be beyond the company's reach. It would be appropriate to deal with a competent third party. Whether done internally or externally, the time factor will be important.

Tip

- It is important to understand what anonymization is. To qualify as anonymization in the sense of the Act, the selected process must be irreversible and no longer allow for the direct or indirect identification of a person at its conclusion.
- There are long-standing anonymization practices. These practices can be based on cryptography. Cryptography often uses keys, the management of which is very sensitive.

Available resources

- Dwork, C. and A. Roth. (2014) The Algorithmic Foundations of Differential Privacy.
- ENISA proposes Best Practices and Techniques for Pseudonymisation, December 2019
- NIST IR 8053 De-Identification of Personal Information, October 2015
- De-identification, anonymization and de-indexation: new jargon, new obligations!

Implement a privacy complaint process to address privacy issues

Chronological information

- **Required under 2.2.1.3 on September 23, 2023**
- **Predecessor:** Update policies and practices governing collection retention, use, disclosure, destruction and de-identification of personal information
- **Successors:** Publish policies and procedures governing the protection of personal information on the company's website

Contents

The process for handling privacy complaints shall be reflected in the company's privacy governance policies and practices. The process shall be simple and clear and available on the company's website. Individuals can inform the company of improper handling of their personal information or the need to correct it.

Key activities

- Determine your company's complaint handling strategy.
- Identify who will be responsible for responding to complaints from affected individuals.
- Ensure that the policies and practices developed by the company provide for the process for handling complaints, including appropriate authentication methods for individuals making inquiries in person, by phone, email, web, etc.
- Describe the complaints process in a simple and clear manner for the people involved.
- Publish the process on the company's website.
- Once the process is in place, keep a record of complaints and the steps the company has taken to address them.

Implement a privacy complaint process to address privacy issues

Planning factors

In addition to developing the process for handling complaints, you must plan how your company will handle them. The people who will be responsible for handling complaints will have to be trained in order to be able to respond adequately and to have the necessary tools in hand so that the situation that generated the complaint is corrected when necessary.

Tip

- If your organization already has a general complaint handling process or customer service department, it is possible to integrate the privacy complaint handling process into these. If not, you can use your existing inquiry or incident tracking tool.
- Learn about the different treatment processes in place to protect personal information for inspirational purposes.

Available resources

- To denounce a suspicious practice or behaviour | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Making a complaint about a business - Office of the Privacy Commissioner of Canada, December 2020

Publish key elements of the privacy governance rules on the company's website

Chronological information

- **Required as per 2.2.2.1 on September 23, 2023**
- **Predecessor:** Create or update policies and practices to support governance of personal information
- **Successors :** none

Contents

Policies and practices governing the protection of personal information are essential to the sound management of personal information. The publication is required by September 23, 2023. However, as these policies guide the implementation of several other elements, their drafting (or revision) is recommended as early as 2022. The requirement to publish information on policies and procedures governing the protection of personal information stems from the principle of transparency that the company must respect.

Key activities

- Develop or update policies and practices to meet the requirements of the Act 25.
- Provide a clear, detailed presentation in a language accessible to all.
- Publish the substance of these policies and practices on the company's website.
  If the company does not have a website, it should make information about its policies and practices available through any other appropriate means.
- Keep published information up to date.

Publish key elements of the privacy governance rules on the company's website

Planning factors

Ensure that the governance policy and procedures comply with regulatory requirements to highlight the information that is required. Ensure that published information is easily accessible and ensure clear language by consulting relevant resources.

Tip

- The person responsible for the protection of personal information of the company shall ensure that the information published is up to date. He or she may obtain assistance from his or her team for this purpose.
- Ensure appropriate disclosure by consulting with your legal advisors prior to publishing information on the website.

Available resources

- https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/politiques-pratiques-gouvernance/

Implement a Privacy Impact Assessment (PIA) policy and process for handling personal information

Chronological information

- **Required under 2.2.2.2 on September 23, 2023**
- **Predecessor:** Taking an inventory of the company's personal information
- **Successors:** Implement a process for handling privacy complaints

Contents

Conducting a PIA is a preventive approach that consists of considering all factors that will have a positive or negative impact on privacy. This assessment should be conducted for any acquisition, development, information system redesign or electronic service delivery project involving personal information or prior to the disclosure of personal information outside Quebec.

Key activities

- Identify applicable privacy obligations and principles.
- Determine the scope of each project involving the collection, processing disclosure or retention of personal information:
  - Determine the nature of the personal information involved. The risks and impacts of a privacy incident are directly related to the sensitivity of the information involved;
  - Identify the use of personal information (collection, disclosure, retention, destruction, etc.).
- Identify and describe the privacy risks associated with the project and analyze the impact of these risks.
- Where possible, identify measures to eliminate or reduce the likelihood of these risks occurring and/or their impact.
- Ensure that the company's publicly available technology products and services that are used to collect personal information and that have privacy settings provide the highest level of privacy to the user.
- Follow up on the PIA as the project evolves.

Implement a Privacy Impact Assessment (PIA) policy and process for handling personal information

Planning factors

- The PIA should be conducted early in the project.
- The PIA must be proportionate to the sensitivity of the information involved, the purpose for which it is to be used, its quantity, distribution and medium.
- Define roles to facilitate the conduct of the PIA, including the collection of information.
- Document the process in writing to keep track of it.
- Establish a process to adequately review the PIA so that it can keep pace with the evolution of the project and be consistent.

Tip

- It may be helpful to prepare a clear and consistent PIA template with the right questions to be completed in writing. In this way, it will be easy to ensure consistency and facilitate an eventual demonstration of compliance if required. It may also be appropriate to document the reasons why a PIA was not conducted for a given project.
- No system should be put into production if the risk of non-compliance with Act 25 are significant. These risks should be discussed in the decision to go into production.

Available resources

- **Guide D'accompagnement (CAI):** https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf
- **Privacy Impact Assessments (Office of the Privacy Commissioner of Canada):** https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/

Implement a process for obtaining consent to collect, hold, use or disclose personal information

Chronological information

- **Required under 2.2.2.3 on September 23, 2023**
- **Predecessor:** Update policies and practices for the collection, retention, use, disclosure, destruction and de-identification of personal information
- **Successors:** Implement a process of deletion and anonymization in order to implement the right to de-index

Contents

While consent is already required to collect, hold, use or disclose personal information, it will now be necessary to ensure that consent is sought and obtained for each purpose for which personal information is to be processed separately from other information communicated to the individual. This consent will be valid only for the purposes identified by the company at the time of collection.

Key activities

- Review the company's current process for collecting and retaining consent and identify if improvements are needed.
- Ensure that individuals are informed of the business reasons for collecting personal information the collection of personal information, how the information will be used if collected for a third party, of their right to withdraw consent and of their rights of access and rectification of their personal information.
- Ensure that you are able to communicate to the person who makes the request what personal information the company holds about him or her, the categories of persons who have access to the information, the length of time it is kept, and the contact information of the person responsible for the protection of personal information in the company.
- Ensure that the individual have all the necessary information in simple and clear terms in order to give clear, free and informed consent.
- If the company processes sensitive personal information, the consent of the individual will have to be obtained expressly. This will require a process that involves an affirmative action in providing consent, such as checking a box.
- Consider whether the company is collecting personal information from minors under the age of 14. If so, provide a process for obtaining the consent of the minor's parent or guardian.
- Maintain evidence of the consents obtained from the individuals.

Implement a process for obtaining consent to collect, hold, use or disclose personal information

Planning factors

- A review of your organization's current process for obtaining consent from those affected by the collection of personal information is the first step in bringing your organization up to speed with the new legislative requirements. This will allow you to identify any missing elements and make it easier to determine the next steps to take.

Tip

- Consult the resources available on the subject to fully understand the new legislative requirements.
- Encourage explicit and positive consent, i.e., the individual must, for example, check a box to give consent.
- Once the upgrade is complete, do not hesitate to consult your legal advisors who will be able to confirm that your consent process meets all your obligations.

Available resources

- Consent | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Sensitive information | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Guidelines for obtaining meaningful consent - Office of the Privacy Commissioner of Canada, August 13, 2021
- Video: Strengthen Privacy: Get meaningful consent - Office of the Privacy Commissioner of Canada
- PL 64 - C for Consent - A Complex Simplification? | Resources | Fasken, June 29, 2020

Implement a de-indexing process

Chronological information

- **Required under 2.2.2.4 on September 22, 2023**
- **De-indexing required as per 2.2.2.6 on September 22, 2023**
- **Predecessor:** Update policies and practices for the retention, destruction and de-identification of personal information
- **Successors :** none

Contents

The right to de-index allows a third party of a company to demand to be de-indexed from all of its systems under certain circumstances. This means that it will no longer be possible to link the individual to their data, but it does not mean that the information will be deleted. This request must be honored if it does not cause harm to the company and is not subject to a legal, regulatory or standard requirement with which the company must comply.

Key activities

- Set up a process to receive the person's request.
- Verify that there are no legal, regulatory or normative requirements that prevent the company from approving the application.
- Develop deletion, anonymization and de-indexing processes.
- If it is impossible to apply the right to de-index, inform the applicant of the reason why the company cannot proceed.
- If possible, use techniques to anonymize or destroy personal information.

Implement a de-indexing process

Planning factors

Depending on the business sector, the number of requests can be high. It is preferable to set up or adapt a ticketing system that allows you to track the progress of requests in the process.

Tip

- Ensure that applicants are kept informed throughout the process, indicating the expected processing time.
- Personal information can be pervasive in corporate information systems. Care must be taken to ensure that these information systems are adapted to be resilient to anonymized or destroyed third party information. This includes backups, whose lifecycle can be quite long.
- Separate the uses of personal information that are subject to a legal, regulatory or standard requirement from those that are not. If personal information falls into the first category, it will still need to be retained, but the second category will not.
- All of the company's suppliers must comply with this right to de-index. It will be critical to ensure that the IT service chain complies with the company's practices.

Available resources

- ENISA The right to be forgotten - between expectations and practice, 2011
- Erdos, D. (2021) The 'right to be forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps, Journal of Media Law, vol. 13.
- De-identification, anonymization and de-indexation: new jargon, new obligations!

Action to be completed by
September 2024

12. Implement measures to facilitate the right to data portability

Implement measures to facilitate the right to data portability

Chronological information

- **Required on September 23, 2024**
- **Predecessor:** Implement a de-indexing process
- **Successors :** none

Contents

The right to data portability allows an individual to obtain a copy of his or her personal information held by an organization and also allows the individual to request the transfer of that information from one organization to another.

This right applies only to personal information that the company has collected from the individual. It does not extend to information created, derived, calculated or inferred from that information.

Key activities

- Review and, where appropriate, update the process for providing individuals with access to their personal information held by the company.
- Establish a process for individuals to request a copy of their personal information the company holds about them.
- If the personal information is computerized, ensure that you are able to disclose it in a structured and commonly used technological format.
- Find out what organizations are authorized by law to collect personal information in response to a request for transfer from the individual.
- Ensure that those responsible for responding to such requests have the necessary training to disclose personal information in a secure and timely manner.

Implement measures to facilitate the right to data portability

Planning factors

The first step is to review the process already in place within your organization regarding access to personal information. Then, it is suggested that you identify the missing elements in order to meet the new legislative requirements, which will allow you to establish an effective action plan for updating your access and disclosure process.

Tip

- Learn about existing data portability processes (e.g. under the GDPR).
- Involve the person responsible for the protection of personal information in the implementation of your new processes to facilitate the right to data to data portability.
- When disclosing automated personal information, here are some suggestions to ensure that you are able to disclose it in a structured and commonly used technological format:
  - Determine the intelligible format in which to export the data (e.g. CSV, JSON, XML, etc.);
  - Implement a tool to extract an individual's personal information from the company's systems;
  - Define a safe extraction procedure;
  - Perform tests to ensure the completeness of the extracted data.
- Do not hesitate to consult with your legal advisors to ensure that the process in place meets all applicable new legislative requirements and to obtain legal advice.

Available resources

- The right to portability, a real portability or a simple modernization of the right of access? | Resources | Fasken
- Professionals: how to respond to a request for the right to portability?
- The right to portability: obtain and reuse a copy of your data | CNIL

Cybereco would like to thank its members for their valuable contributions in the elaboration of this act 25 guide

While we hope this guide is a useful introduction to better understand and navigate the complex act 25 landscape, it is not meant as a substitute for competent professional advice. Consult one before making decisions that impact your finances, operations or wellbeing.

Deloitte.

Desjardins®

FASKEN

mondata*

QOHASH

UNIVERSITÉ DE SHERBROOKE

Appendix

Other available resources

https://terranovasecurity.com/fr-fr/protection-donnees-personnelles/

https://business.adobe.com/ca_fr/products/advertising/general-data-protection-regulation.html

https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/Cyber%20Security%20Small%20Business%20Toolkit_FR.pdf

https://www.lemagit.fr/conseil/GDPR-une-trousse-a-outils-qui-commence-par-une-cartographie

Diagnostic tool for the new requirements of Act 25

Compliance and governance

By September 22, 2022	By September 22, 2023	By September 22, 2024
• Has the company identified criteria, such as desired knowledge, skills and abilities, for internal designation, lateral hiring or outsourcing of the PRP lead role? • Have the roles and responsibilities of the person in charge been described? • Who will this person report to within the organization? • Are changes in current governance required to incorporate and frame this role? • Has the person responsible for the VRP been identified? • Has this person received training on their role? • Is there a continuing education program in place to close any knowledge gaps and update the leader's knowledge? • Has an assessment been made of the human and physical resources required to carry out the company's compliance activities?	• Is the company aware of its handling of personal information, have deviations from the new requirements been identified, and is an action plan to correct the situation being followed? • Does the company have an up-to-date inventory[1] of processes that use personal information? • Have company policies been updated to comply with the requirements of the new law (including: protection, retention, destruction, transfer and de-identification)? • Are the updated policies approved by the PRP manager (private sector) or the Access to Information and Privacy Committee (public sector)? • Is there a process in place for handling requests for information, access, correction and complaints? • Do you have adequate authentication methods for people making requests in person, over the phone, via email, the web, etc.?	• Does the company have a policy addressing access, rectification and portability of data? • Does the company have the technology to meet the portability requirements of the law?

1. This requirement is scheduled for 2023, but CyberEcho advises that this step should be taken as early as 2022 as it is a prerequisite for several other actions.
2. Act 25 introduces the right of the person concerned to obtain certain information "upon request", in particular following the obtaining of his or her consent to the collection of personal information or during an automated decision.

Diagnostic tool for the new requirements of Act 25

Information requirements		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
• Is the contact information for the PRP manager published on the website or other means of reaching the company (e.g. Facebook site)?	• Is information about the company's privacy policies and practices posted on the website? • Has the company identified and documented situations where it uses personal information to make a decision based solely on automated processing? Is the company able to identify the reasons, key factors and parameters leading to this type of decision?	

Training		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
• Has a privacy training program been developed for employees and officers? Does the organization have a periodic update of its program? • How will updated policies and procedures be communicated within the company?		

Diagnostic tool for the new requirements of Act 25

Privacy incidents		
By September 22, 2022	By September 22, 2023	By September 22, 2024
• Has the privacy incident response plan been designed? Is it up to date to meet the requirements of the new law? • Does the organization have an incident log template? • Does the organization have an incident reporting process in place and socialized to its employees? • Has the organization assessed the resource and training needs for implementing and maintaining the incident log?		

Diagnostic tool for the new requirements of Act 25

Privacy Impact Assessment		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
	• Have projects requiring a PIA been identified? • Have situations involving the transfer of personal information outside Quebec been identified? • Is there a policy in place to achieve PIAs? • What process will be followed to bring a project to the attention of the PRP Manager to initiate a PIA? • Is the methodology for conducting PIAs established? • Who will accompany the PRP manager in conducting the PIAs?	

Diagnostic tool for the new requirements of Act 25

Design of products and services		
By September 22, 2022	By September 22, 2023	By September 22, 2024
	• Do the company's technology products and services offered to the public, when used to collect personal information and with privacy settings, provide the highest level of privacy to the user? • Has an inventory of information or electronic service delivery systems involving the identification, location or profiling of an individual been completed? • Has an analysis of the compliance of the process of activating the identify, locate, or profile functions with the law been conducted? • Do the information systems used by the company's employees comply with the requirements of the new law?	

Diagnostic tool for the new requirements of Act 25

Consent		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**

	• Have the forms, processes and other consent gathering tools used been revised to reflect the requirements of the new legislation?
	  • Serious and legitimate interest
	  • Determine specific purposes before collection
	  • Collect only what is necessary for the purposes identified prior to collection
	  • Disclose, at the time of collection, the information listed in sections 8 and 8.1, if applicable
	  • Use simple and clear language when obtaining consent
	  • Consent must be clear, free and informed. For sensitive information, consent must be express.
	  • Compliance with the requirements of section 14 for any consent obtained in writing
	• If third-party collection is required, has the company identified and documented that the criteria of the law are met?
	• Has the company identified whether personal information of minors under the age of 14 is being collected and, if so, has the company put in place procedures to validly collect such information (e.g., obtaining consent from a parent or guardian)	

Diagnostic tool for the new requirements of Act 25

Use of personal information		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
	• Has the company identified situations where it needs to implement additional consent for the use of personal information for purposes other than those originally disclosed, and developed a process for doing so in compliance with the law?	

Retention and Destruction of Personal Information		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
	• Does the company have a retention and destruction policy that meets the requirements of the law? • Has the company adopted and updated its personal information retention schedule? • Does the company have de-identification techniques in place that meet the requirements of the law? • Has the company documented the purposes for which it is de-identifying the personal information it holds rather than destroying it?	

Diagnostic tool for the new requirements of Act 25

Security measures		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
• Measures to Strengthen the Cybersecurity of Small and Medium-Sized Enterprises (ITSAP.10.035) • Other frameworks such as ISO 27001 & 2 (security), ISO 29100 (privacy), NIST - CSF, NIST - Privacy framework can be used to identify the security measures to be implemented.		

Right to be forgotten		
By September 22, 2022	**By September 22, 2023**	**By September 22, 2024**
	• Does the company have a legally compliant process for dealing with requests for deletion, de-indexing, re-indexing or stopping the release of individuals' personal information? • Does the company have the necessary resources and technology to respond to requests from individuals in this regard?	

cyber eco