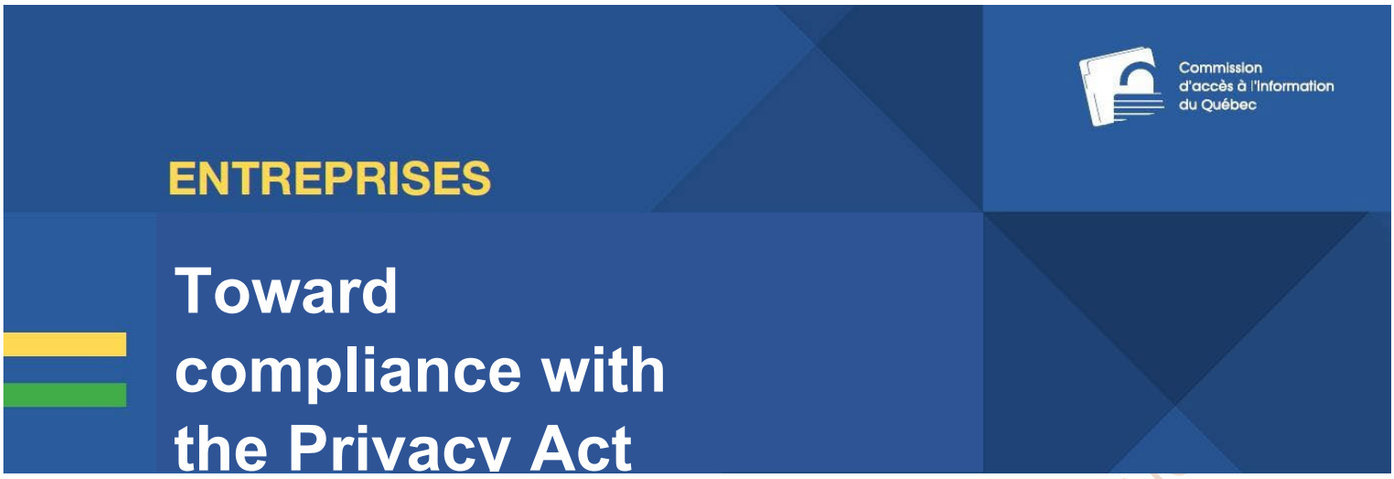

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDAN

The *Act to modernize legislative provisions as regards the protection of personal information* is bringing **important** changes to the *Act respecting the protection of personal information in the private sector* (Privacy Act). They need to be implemented starting in September 2022.

The purpose of this document is to help you to get familiar with some of your **new responsibilities and obligations** (pages 1 and 2) that will come into effect gradually in September 2022, 2023 and 2024.

A few **courses of action** and **best practices** are provided on pages 3 and 4 to help you plan your compliance work.

The information in this document is general and does not take into account the specific characteristics of each company. The statutes and regulations take precedence at all times.

Feel free to contact a privacy lawyer and an information security specialist to assist you.

New responsibilities and obligations for companies

Effective September 22, 2022

In addition to meeting your current privacy obligations, effective September 22, 2022, you will be required to:

1. **Appoint** a privacy officer and post this person's title and contact information on the company's website or, if the company does not have a website, make this information available by any other appropriate means.

Other requirements include:

2. In the event of a confidentiality incident involving personal information, you must:
    a. Take **reasonable measures** to **reduce the risk** of harm to the persons concerned and prevent similar incidents from reoccurring
    b. **Notify the Commission** and the **person concerned** if the incident **poses a serious risk of harm**
    c. **Keep a register of incidents,** a copy of which must be sent to the Commission upon request

3. Observe the **new rules on the disclosure of personal information without the consent of the person concerned for study, research or statistical** purposes and in the context of a **business transaction**
4. Conduct a **Privacy Impact Assessment (PIA)** prior to disclosing personal information without the consent of the persons concerned for study, research or statistical production purposes
5. **Disclose in advance** to the Commission that identity was verified or confirmed using biometric features or measures

Effective September 22, 2023

In addition to your existing privacy obligations, effective September 22, 2023, as an individual carrying on an enterprise, you will be required to:

1. Have **policies and practices on the governance** of personal information and post detailed information on them in **clear and simple language** on the company's website or, if the company does not have a website, through any other appropriate means
2. Conduct a **Privacy Impact Assessment (PIA)** when required by the Act, such as before disclosing personal information outside Quebec
3. Comply with the new rules regarding **consent** to the collection, disclosure or use of personal information
4. **Destroy** personal information once the purpose of its collection has been fulfilled, or **anonymize** it for serious and legitimate use, subject to the conditions and retention period provided for by law
5. Comply with your new obligations of **information and transparency** toward the public
6. Comply with the new rules on the disclosure of personal information without the consent of the person concerned **(carrying out a mandate or a service or business contract)**
7. Comply with the new rules on the **disclosure of personal information outside Quebec**
8. Comply with the new rules on the **use of personal information**
9. Provide, by default, the **settings that ensure the highest level of privacy** for the technology products or services offered to the public
10. Comply with the new rules on the collection of personal information regarding a **minor**
11. Comply with the **right to stop dissemination, re-indexing or de-indexing** (or right to be forgotten)
12. Comply with the new rules on the **disclosure of personal information facilitating the bereavement process**

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Effective September 22, 2024

Effective September 22, 2024, as an individual carrying on an enterprise, you will be required to:

- Respond to requests for the portability of personal information

Courses of action and best practices

By September 22, 2022

1. If you are the highest authority in the company and do not wish to act as **privacy officer**, appoint a person who can effectively carry out this function. For example, the person in question should have the required skills and major decision-making authority.
2. Support the privacy officer with the **necessary resources** (human, technical and financial) to ensure successful compliance.
3. Make an **inventory of the personal information** held by your company (or by a third party on its behalf) and assess the sensitivity of this information.
4. Set up **measures** to **prevent or limit the consequences of a privacy incident involving personal information**.
5. Establish practices that will allow you to **respond appropriately and quickly to privacy incidents** involving personal information (e.g., incident response plan and instructions to personnel).
6. If you plan on **using a biometric technique (e.g., fingerprints, facial or voice recognition), first make sure you understand your obligations** in this respect**.**

By September 22, 2023

To establish and implement your **privacy governance policies,** you will need to:

1. Make an **inventory** of the personal information held by your company (or by a third party on your behalf) and assess the sensitivity of this information
2. Given that the inventory of personal information is constantly changing, it is important to **keep it up to date** to reflect any changes that may have occurred within your company (e.g., new collection of personal information for a project) and to **ensure that you plan your actions properly and meet all your obligations**
3. Define the **roles and responsibilities of personnel** involved in the protection of personal information throughout its life cycle

Completing these tasks is critical to meeting your obligations and prioritizing certain actions going forward.

To conduct a Privacy Impact Assessment, in addition to completing the above tasks, you must also:

1. Assess the project's compliance with privacy laws
2. Identify the project's privacy risks for the persons concerned
3. Set up strategies and measures to effectively avoid or reduce such risks
4. Monitor the application of these measures and revise them

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

To respect the public's new rights and your new transparency obligations, you will need to put in place mechanisms (e.g., directives, processes, forms or technological solutions) that will enable you to:

1. Obtain separate valid consent for each specific purpose in **clear and simple terms**
2. Keep written requests for consent separate from other information being provided
3. Provide the information required by law to the person whose information is being collected
4. Inform a person when they are the subject of a decision based exclusively on automated processing
5. Notify a person before using technology to identify, locate or profile them, and inform them of the means available to activate these features
6. Post detailed information about your policies and practices on the company's website or, if the company does not have a website, make this information available through any other appropriate means
7. Post a privacy policy written in **clear and simple language** on your company's website and disseminate it by any means likely to reach the persons concerned if the personal information is being collected using a technological means such as a website
8. Handle requests and complaints from the public regarding your management of personal information

By September 22, 2024

1. Inform the team responsible for maintaining, updating or developing your IT systems that you have new business needs related to the right to portability of personal information, namely that:
    - Your systems make it possible to disclose, at the request of a person concerned, the computerized personal information collected from that person in a structured and commonly used technological format
    - This information may also be disclosed to a person or body authorized by law to collect the information, at the request of the person concerned

Note:

Be sure to **train your personnel** to develop good privacy habits.

OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE