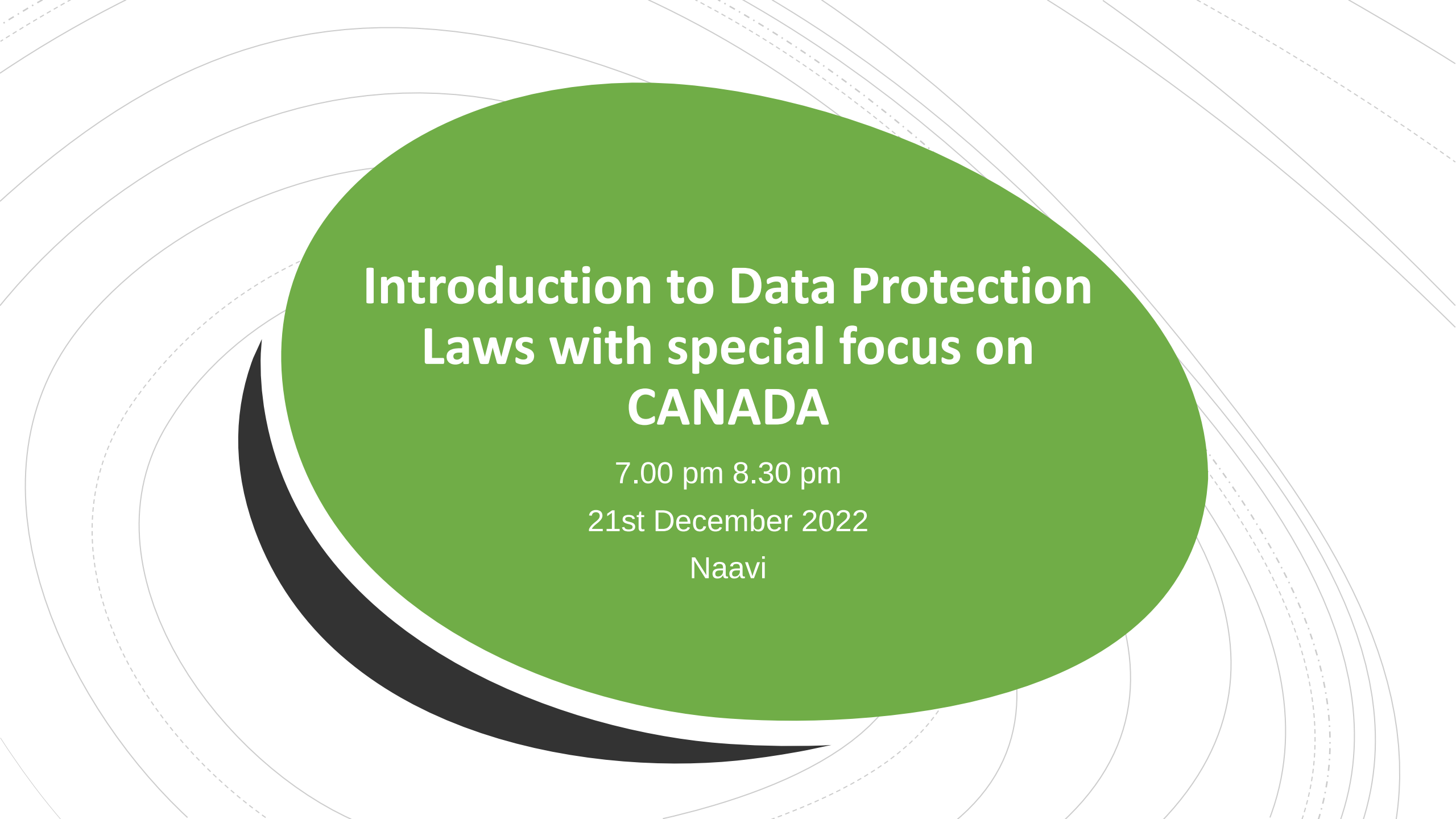


The background features a series of concentric circles in light gray, some solid and some dashed, creating a ripple effect. A large, solid green oval is centered on the page, containing the main text. A thick, dark gray curved line sweeps across the bottom left, partially overlapping the green oval.

Introduction to Data Protection Laws with special focus on CANADA

7.00 pm 8.30 pm

21st December 2022

Naavi



Data Protection in Canada

...

Canada have several laws on Privacy Rights

- Federal Privacy Laws
 - The Privacy Act
 - The Personal Information Protection and Electronic Documents Act (PIPEDA)
- Provincial Privacy Laws
 - Alberta
 - British Columbia
 - Quebec
- Health Related laws substantially similar to PIPEDA
 - Ontario, New Brunswick, Newfoundland and Labrador, Novascotia
- Employment Related laws
 - Alberta and British Columbia
- Sector Specific Privacy Laws
 - The Federal Bank Act
 - Provincial Laws Governing Credit Unions, Consumer Credit Reporting

A complex maze of laws

- The Privacy Act 1983 applicable to the Government
- PIPEDA 2000 applicable as a federal law to non Government agencies
- After GDPR, a similar law...Canadian Consumer Privacy Protection Act or CPPA.... Under consideration
- Federal *Bank Act*, is a sectoral privacy act and contains provisions regulating the use and disclosure of personal financial information by federally regulated financial institutions.
- Provincial Laws (Replacing PIPEDA)
 - Alberta
 - British Columbia
 - Quebec
- Each province and territory in Canada has a Commissioner or Ombudsman responsible for overseeing provincial and territorial privacy legislation
- Alberta and British Columbia have separate privacy laws applicable to employee information

Privacy Act 1983 Applicability:

- No Separate definition of Sensitive Personal Information.
- Personal Information means
 - **(a)** information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
 - **(b)** information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
 - **(c)** any identifying number, symbol or other particular assigned to the individual,
 - **(d)** the address, fingerprints or blood type of the individual,

Privacy Act 1983 Applicability:

- **(e)** the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,
- **(f)** correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,
- **(g)** the views or opinions of another individual about the individual,
- **(h)** the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and
- **(i)** the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

Excluded under Privacy Act 1983

- Information about
 - An officer or an employee of a Government institution
 - Title, business address, telephone number, salary etc
 - The information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and
 - information about an individual **who has been dead for more than twenty years**

Collection, Retention and Disposal

- Restricts personal information to be collected by the Government institution only to that which relates to an operating program or activity of the institution. (Purpose Limitation)
- Wherever possible, the Government shall only collect personal information that is intended to be used for an administrative purpose directly from the individual ...except where the individual authorizes otherwise or where personal information may be disclosed to the institution under any other act. (Direct Collection)
- Consent and Notice required
- Exemption
 - Consent exemption when accuracy of the information is to be ensured
 - Disclosure exemption for purposes such as law enforcement, or against a warrant
 - Disclosure for Library and archival purpose, research and statistical purpose etc

Retention

- Head of a government institution keep a record of uses and disclosures of personal information and shall cause to be included in **a personal information banks** all personal information under the control of the government institution that
 - (a) has been used, is being used or is available for use for an administrative purpose; or
 - (b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual
- Personal information banks (**PIBs**)
 - describes how personal information is collected, used, disclosed, retained and/or disposed of in the administration of a government institution's program or activity
- There are three types of PIBs: central, institution-specific and standard.

Rights

- **Right of access**
 - (a) any personal information about the individual contained in a personal information bank; and
 - (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.
- **Right for Correction**

Privacy Impact Assessments

PIAs, which are required under federal policy, are a type of risk-assessment exercise that helps reassure Canadians that privacy issues are thoroughly taken into account during the design or redesign of federal programs or services.

They also help to avoid or mitigate the risk that the privacy of Canadians could be compromised when a program is developed or substantially changed.

Institutions must submit their PIAs to **the Privacy Commissioner of Canada**, who may advise institutions on ways to address potential privacy risks.

Institutions have to publish summaries of their PIA results so that Canadians can see how privacy issues have been addressed in the design of a program or service.

Complaints



Individuals may lodge complaints with the Privacy Commissioner



The Privacy Commissioner may also initiate a complaint and order investigation if there are reasonable grounds for the same.



Investigations shall be conducted by the Privacy Commissioner in private and the complainant has the right to be present during the hearings.

Personal Information Protection and Electronic Documents act (PIPEDA)

- **Applicability**

- PIPEDA combines protection of personal information with some other aspects of **regulation of electronic documents**
- applies to every organization in respect of personal information that it collects, uses or discloses **in the course of commercial activities** and employees of an organization including the applicants for employment.
- It does not apply to Government bodies
- does not apply to “Business Contact Information” which is the information collected, used or disclosed solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession.

Principles of Processing

Principle 1: Accountability	Principle 6: Accuracy
Principle 2: Identifying Purposes	Principle 7: Safeguards
Principle 3: Consent	Principle 8: Openness
Principle 4: Limiting Collection	Principle 9: Individual Access
Principle 5: Limiting Use, Disclosure and Retention	Principle 10: Challenging Compliance

Key aspects of Principles

- **Designation** of a Compliance person mandatory
- No definition like “**Data Controller**”.
 - Data Collector is responsible for the purpose determination and adherence to other principles.
- Knowledge and **Consent required** for collection, use or disclosure
 - Notice can be oral or written
- No separate definition of “**Sensitive**” information
 - Sensitivity is recognized by the context
 - Eg: Name and address of subscribers to a magazine are generally non sensitive but if it is a special purpose magazine, it could be considered sensitive
- Provides for Reasonable expectation of a consent in certain circumstances, (deemed consent) Express Consent.
- Consent can be given by a legal guardian or a power of attorney holder
- Right to withdraw consent recognized.

Key Aspects of Principles

- Collection should be by fair and lawful means without misleading or deceiving
- Retention guidelines to be developed by the organization
- Disclosure should be purpose specific
- Information no longer required should be destroyed, erased or **made anonymous**
- Accuracy, safeguards, openness required
- Individual access subject to exceptions such as legal or security requirements and commercial proprietary reasons (Legitimate interest?)
- An individual can challenge the organization on compliance

Compliance Requirements

- Comply with fair information principles
- Appoint a Compliance official
- Security of information processed including transferred to the processor
- Develop and implement personal information policies and practices
- A Privacy Impact assessment need to be conducted
- Ensure compliance of Data Breach notification requirements

Data Breach Notification

- an organization shall report to the Commissioner any breach of security safeguards
 - if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.
- as soon as feasible after the organization determines that the breach has occurred.
- Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards
 - if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual

Penalties

An individual can file a complaint with the Commissioner after exhausting grievances

Commissioner may investigate if it does not constitute a contravention of other laws

May attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

May order the organization to correct

Award damages to the complainant

Fines upto \$100,000 may be possible

Exemptions

- Collections clearly in the interest of the individual, under reasonable expectation,
- Solely for Journalistic, artistic , literary purpose or for statistical research
- Information is publicly available
- Requirement under law, to report a contravention of law
- Emergencies threatening life, health or security of an individual
- Debt recovery

Employment Relationship

- Undertaking or business may collect, use and disclose personal information **without the consent** of the individual if
 - **(a)** it is necessary to establish, manage or terminate an employment relationship between the federal work, undertaking or business and the individual; and
 - **(b)** the federal work, undertaking or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purpose

National Security

- Further the rights of an individual may be objected to under the following circumstances.
- national security, the defence of Canada or the conduct of international affairs;
- - the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or
 - - the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

Cross Border transfer

- No separate restrictions are imposed on cross border transfer except what is applicable for transferring data to a third party processor under a contract.
 - This is part of the Accountability and Safeguards.
- However, a separate guideline has been issued by the Office of Privacy Commissioner of Canada for this purpose.

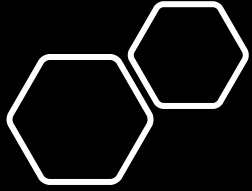
Provincial Privacy Laws



- The **provinces and territories of Canada** are sub-national divisions within the geographical areas of Canada under the jurisdiction of the Canadian Constitution.
- The major difference between a Canadian province and a territory is that provinces receive their power and authority from the Constitution Act, 1867 (formerly called The British North America Act, 1867), whereas territorial governments are creatures of statute with powers delegated to them by the Parliament of Canada.
- Unlike the provinces, the territories of Canada have no inherent sovereignty and have only those powers delegated to them by the federal government.
 - PIPEDA allows for similar provincial laws to continue to be in effect.

British Columbia Personal Information Privacy Act (Effective from January 1, 2004)

- BC-PIPA, is therefore applicable to every organization **other than** the following
 1. the collection, use or disclosure of personal information, if the collection, use or disclosure is
 - i. for the personal or domestic purposes of the individual who is collecting, using or disclosing the personal information and for no other purpose
 - ii. for journalistic, artistic or literary purposes and for no other purpose;
 2. if the federal Act applies to the collection, use or disclosure of the personal information
 3. if the *Freedom of Information and Protection of Privacy Act* (Similar to our RTI Act) applies
 4. personal information in Judicial records, solicitor-client privilege, used in legislature
 5. The collection of personal information that has been collected on or before this Act comes into force.



General Principles (BCPIPA)

- In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances (Duty?..Fiduciary?)
- An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization (Responsibility for Data Processor?)
- An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act. (DPO?)
 - An individual designated under subsection (3) may delegate to another individual the duty conferred by that designation.
- An organization must make available to the public
 - (a) the position name or title of each individual designated under subsection (3) or delegated under subsection (4), and
 - (b) contact information for each individual referred to in paragraph (a).

Policies and Practices (BCPIPA)

- An organization must
- (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,
- (b) develop a process **to respond to complaints** that may arise respecting the application of this Act, and
- (c) make information available on request about
 - (i) the policies and practices referred to in paragraph (a), and
 - (ii) the complaint process referred to in paragraph (b).
- These requirements of policies and practices are similar to the “Privacy by Design” principle in other laws and the Right to information and Right to get grievances redressed.

Consent (BCPIPA)

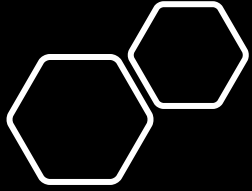
The Act prescribes “Consent” as the legal basis for collection, use and disclosure and mandates that the organization provides information in the form of a notice the purpose for which the personal data is collected.

Where information is collected from another entity the recipient organization is required to inform the purpose of collection to the organization providing the information.

The consent can be withdrawn after giving a reasonable notice.

Exemptions of Consent is available in certain cases such as in the interest of the individual, medical reasons, Credit rating, collection from public resources, collection for employment purpose, etc.

Similarly use and disclosure is normally driven by the consent but with exemptions for purpose such as journalistic purpose, public interest, statistical purpose etc.



Rights, Penalties (BCPIPA)

- The Act recognizes the right to access, right to correction.
- The organization also requires the organizations to protect the personal information, retain the information only for a limited period and maintain its accuracy.
- The non compliance of the Act attracts the following penalties.
- An organization or person that commits an offence is liable,
 - (1) if an individual, to a fine of not more than \$10 000, and
 - (2) if a person other than an individual, to a fine of not more than \$100 000.

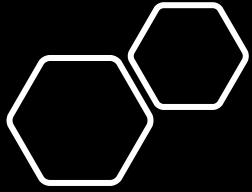
Alberta (PDPA-AI)

The Alberta provincial law titled “Personal Data Protection Act” came into force from 1st January 2004

The law is defined as applicable to every organization and all personal information except the list of activities listed for which it is not applicable

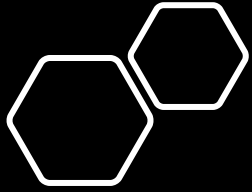
Negative list includes

- domestic purpose, literary purpose, journalistic purpose, regarding business contact information, Judicial or Legislative purpose etc



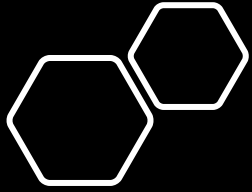
Legacy Information (PDPA-AI)

- In respect of the personal information collected prior to the date of effect of this law, “Consent” is presumed and it may be used and disclosed for the purposes for which the information was collected.
- Unlike the British Columbia law, Alberta law does not make direct reference to PIPEDA in the applicability clause.
 - The BC law states clearly that is not applicable where the PIPEDA is applicable. But no such exemption is specifically provided under Alberta Law.
- The responsibility for compliance lies with the organization that has the “Custody” or “Control” of personal information which extends to the organization engaged if any as an agent.
- Designation of a person accountable for compliance is mandatory.
- The organization must develop and follow policies and practices that are reasonable for the organization



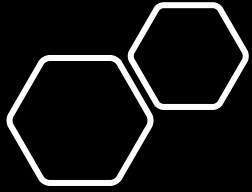
Miscellaneous (PDPA-AI)

- Consent is required but exemptions are available
- The lawfulness of usage of personal information is directed by stating that an organization may use or disclose personal information only for the purposes that are **reasonable**
- Rights of the Trade unions to collect information is also specifically provided under the Alberta law.
- The law also speaks of “Reasonable Security Arrangement” to describe the obligation on security which can be interpreted as the industry best practice based on risk assessment
- It is interesting to note that “Consent” provided to one organization for disclosure may be considered as “Deemed Consent” for collection, use or disclosure even by the other organization if the data is being processed for the same purpose.
 - This seems to indicate that “Consent for Disclosure” once given is a general deemed consent for use by any other organization.
- The Alberta law has a separate part on “Professional Regulatory and Non Profit Organizations”.
- As regards transfer of data outside Canada,
 - Alberta law provides that a notification has to be provided to the individual.
 - Otherwise no other restriction is mentioned.



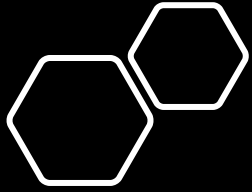
Quebec Law (Appl-Qu)

- Law Effective from 1st January 1994-"Act for protection of personal information in the Private Sector".
- Applies irrespective of the medium of information
- Does not apply to Journalistic, Historical or Geneological material collected, held used or communicated for the legitimate information of the public.
- Does not apply to information held by a public body.
- The law applies to any person carrying on an enterprise who may, for a serious and legitimate reason, **establish a file** on another person must, when establishing the file, enter its object and when the entry is part of the file



Collection (Appl-Qu)

- Consent required except for the serious and legitimate reason in the interest of the person,. (Vital Interest?)
- Notice required about the “Object” of creation of the personal file, who will access, where the file is kept etc
- Confidentiality should be maintained (Security)
- Every person carrying on an enterprise must ensure that any file held on another person is up to date and accurate when used to make a decision in relation to the person concerned. (Indicates need for Accuracy or Quality)
- Once the object of a file has been achieved, no information contained in it may be used otherwise than with the consent of the person concerned, subject to the time limit prescribed by law or by a retention schedule established by government regulation



Miscellaneous (Appl-Qu)

- **Cross Border Restrictions**

- Every person carrying on an enterprise in Québec who communicates personal information outside Québec or entrusts a person outside Québec with the task of holding, using or communicating such information on his behalf must first take all reasonable steps to ensure ... that the information will not be used for purposes not relevant...

- **Minor**

- No person of less than **14 years** of age may demand to be informed of the existence of information of a medical or social nature concerning him and contained in a file established on him, or receive communication of such information, except through his attorney in the context of judicial proceedings.
- On September 22, 2021, amendment bill has been passed to bring the law in tune with EU GDPR.
 - Provisions would be applicable by September 22, 2023



Thank you..

Naavi