Privacy Legislation in Canada.

Based on this video.

What Legislation is Out There?

- The Privacy Act & Provincial Privacy Laws
- The Personal Information Protection & Electronic Documents Act (PIP[EDA) & Provincial Equivalents
- Canada's Anti-Spam Legislation
- Sector Specific Laws

Privacy Act

- The privacy act will not directly impact most of you in daily work, as it applies to federal Gov institutions
    - Departments like foreign affairs
    - Any body acting on the behalf of the gov is protected under the privacy act
- Regulations on how personal information is collected, used, & managed
- Each province & territory has a similar act regulation how provincial gov institutions collect, use, & manage personal information
    - Has to at least be similar to the federal act
    - But sometimes even stronger
- Personal information is any piece of information that can concretely identify a person.
    - Not part of a public domain
    - Your name alone is not
    - Business contact is not
    - Personal phone number, age, email, … is a personal information
- Privacy commissioner and their office
    - Has the authority to manage this act and investigate its breaches
    - You can complain to him, …

PIPEDA & Provincial Equivalents

- Stands for Personal Information Protection & Electronic Documents Act
- This act governs the collection, use & storage of personal information for business purposes
- Part 1 of act is about the private sector
- PIPEDA is a federal act & applies everywhere in Canada (BC, Alberta, Quebec have provincial legislation that replaces part 1 of PIPEDA)
- Personal Information about identifiable individuals, does not include the name, title or business address or telephone number of an employee of an organization.
- Any other info that could identify a person is considered personal info under PIPEDA
    - Age, gender, health info, …
- Providing the information must consent to provide & understand why they are providing it. (collection)
- Personal info can only be released w/ the consent of the client
- Personal info can only be used for the purposes it was collected for
- Privacy Commissioner can investigate breaches of this act
- The privacy commissioner can audit personal information management practices of a business.

- **Exceptions to Consent**
    - Part of legal proceedings, investigations, & gov use
    - Some new development in Digital Privacy Act: Info produced by a witness statement when the collection is necessary to assess, process or settle an insurance claim does not require consent

PIPEDA Compliance

- The privacy commissioner can have violations investigated and they will report violations publicly and suggest remedies
- Individuals can take legal action if against you if you are in violation of PIPEDA
- Verification questions is to know that you are the client to give personal information
- Checks if the collection by consent, use, & management has been done properly done

PIPEDA Best Practices

- Physical files should be put away at the end of the day and kept ina locked location
- Computers and databases should have passwords
- Remember to protect removable hardware too (memory sticks, external hard drives).
- Take extra care when sending emails
    - You should take care not to send the wrong email to the wrong person, that could be a violation issue.
- Include an email footer on your emails
    - Some mumble jumble footer
- A culture of confidentiality
    - Have a privacy officer, in charge of ensuring PIPEDA is upheld
    - Include confidentiality in everyone's training
        - Why it is important
        - The benefits of confidentiality
        - The consequences of lacking confidentiality
    - Review regularly
        - Look at regulatory changes
            - The digital privacy act change
        - Do quick refresher training even if there are no changes. \

Personal Information Protection Act

- In Alberta & BC personal info is protected under provincial legislation called the personal information protection act (PIPA)
- A similar act was passed in Quebec (Protection of Personal Information in the Private Sector)
- In Ontario, the personal health information protection act has been deemed substantially similar to PIPEDA in regards to health info

PIPA Principles

- Organization are accountable for the protection of personal information under their control
- The purposes for which the personal info is being collected must be identified during or prior to the collection
- Personal information may only be collected, used, or disclosed by an organization w/ the knowledge and consent of the individual, w/ limited exceptions as specified in the legislation

- The collection of personal info is limited to what is necessary for the identified purposes and will be collected by fair and lawful means.
- Personal info must only be sued and disclosed for the purposes it was collected, except w/ consent or as required by law.
- It can be retained only as long as it is necessary to fulfill those purposes.
- Organization is seen more in PIPA than PIPEDA
- More recent than PIPEDA
- Provisions made to have consumer have access to the data
- Personal info must be accurate, complete and up to date
- Info about an organization's privacy policies and practices must be readily available to individuals upon request
- An individual has the right of access to personal info about himself and has the right to seek correction. Both these rights are subject to some exceptions
- Organization must provide the means for an individual to challenge an organization's compliance of the above principles

PIPA - What is an Organization?

- May or may not be incorporated
- It may be an individual acting in a business capacity
- May be non-profit
- Alberta's PIPA specifically includes professional regulatory organizations, whereas in BC they are covered by other legislation
- PIPA does not apply to individuals acting in a personal or domestic capacity

PIPA - Exceptions

- Class of non-profit organization in Alberta PIPA only applies to their commercial activities
- Alberta and BC, when organizations subject to PIPA engage in commercial trans-border personal info flows, they also have to follow PIPEDA for those specific transactions.

PIPA vs PIPEDA

- Note even in BC and Alberta are non subject to PIPA
    - Federal works undertaking or businesses FWUBs
    - Commercial activity that crosses borders
        - Banks, radio, tv, Airports, shipping companies by water, railways, pipelines
    - Employee information of FWUBs
- PIPA will apply when
    - The activity is provincially regulated
    - It is employee information of a provincially regulated industry.

PIPA - Compliance

- Under each privacy law, a Commissioner is designated for overseeing the application of the statute and investigating disputes between individuals & organizations
    - Alberta: Office of the Information & privacy commissioner of alberta
    - BC: office of the information & privacy commissioner for BC
    - Quebec: something in french with the same meaning

PIPA - Enforcement

- Much like PIPEDa, privacy officers for PIPA can:
    - Investigate breaches of the act

    - Report violations of the act
    - Suggest remedies for poor conduct
- Individuals can take legal action if against organizations in violation of PIPA

PIPA - Best Practices

- Protect the info
    - Physical files secure
    - Computers and databases should have passwords
- Culture of confidentiality
- Be open w/ individuals about your practices
- Review regularly
- Similar to PIPEDA best practices

Canada's anti-Spam Law CASL

- CASL dictates the do's and don'ts of electronic communications including
    - **commercial electronic messages CEMs**
        - An electronic message is any communication that is sent by means of telecommunication email or text eg
        - A message is commercial if the content is leading someone to engage in a purchase or other financial exchange with you
- Three areas: Consent, identification, unsubscribing
- Applies to anyone sending CEMs regardless of the industry they are in

CASL Consent

- Consent may be expressed or implied
- Express ⇒ opt in
- Implied is when a person could reasonably be expected to expect information form you (related product)
- A person can withdraw their consent at any time and you are required to stop sending them CEMs up to 10 days

CASL Identification

- All CEMs must clearly identify who the sender is
- Includes:
    - Name of business
    - Name of sender specific person (kelly from marketing)
    - Physical location of the sender
    - Email address, phone number, or other contact info of the sender

CASL Unsubscribing

- Clear and simple way to allow customers to understand how to stop communication from you
- Needs to be in every CEM
- When someone asks to unsubcribe you must make the change within 10 days
- You cannot charge any fee to unsubscribe

CASL Compliance

- Compliance w/ CASL is manages by the CRTC (Canadian Radio-television and Telecommunications Commission)
- If you are in violation of CASL, CRTC can issue warnings or fines
- They usually send warning first, then if you are very stubborn they fine you
- Fines can be up to $1 million for an individual or up to $10 million for a business.
- PIPEDA cannot issue a fine can only sue.

CASL Best Practices

- Use email marketing program
    - Have CASL protections built into their systems to help you out
- Train yourself and your reports on CASL
- Keep up to date some gov link

Sector Specific Laws

- Some sectors required to follow PIPDA in addition to what is in their own regulations
- Banking, telecommunications, and airlines
- Could be federal or provincial depending on the sector
- Banking has a federal law regulating it ⇒ collection, and storage of financial information
- Provincial laws for insurance
- You can't ignore other laws when there are sector specific laws.
- The same PIPEDA best practices apply for sector specific laws.

Why be compliant?

- Create goodwill
    - Clients will appreciate protection of their info & respect of privacy
- Maintain strong reputation
    - Public has access to info on violations of these regulations
- Avoid legal action
    - Could compromise your licenses and your reputation
- Avoid financial penalties