CHANGES TO PRIVACY LEGISLATION

WHAT LANDLORDS & PROPERTY MANAGERS SHOULD KNOW

Laura Glithero
Cohen Highley LLP

TOPICS

1. Mandatory reporting of the breach to the Information and Privacy Commissioner;

2. Mandatory notice to affected individuals; and other organizations;

3. Mandatory record-keeping of data breaches; and

4. Incident Report Plan

OVERVIEW

- Landlords and Property Managers have a “duty of care” when collecting, using, storing and disclosing personal information
- Meeting your “standard of care”
  - Comprehensive Privacy Policy
  - Implement risk management procedures
  - Have appropriate security measures
  - Cyber-liability insurance
- Bottom line: take reasonable steps to protect personal information in your control

BREACHES

- There will likely be times when improper disclosure of a tenant or employee's personal information occurs

- Disclosures can occur:
  - accidentally (i.e. by sending a notice of breach of lease to the wrong unit);
  - negligently (i.e. staff overheard gossiping in common areas);
  - criminal activities of third parties (i.e.: office break-ins, theft, or hacking); or
  - by third party suppliers and service providers

CHANGES TO PIPEDA

- As of November 1, 2018, landlords and property managers in Canada will have enhanced obligations to keep records and report data breaches under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).
- If you experience a data breach – referred to in the regulation as a "breach of security safeguards"- you will be exposed to new liabilities, including:
  - Mandatory reporting of the breach to the Information and Privacy Commissioner;
  - Mandatory notice to affected individuals and other organizations; and
  - Mandatory record-keeping of data breaches.

DEFINITIONS

- **"Breach of security safeguards"** is defined as the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards

- **"Significant harm"** is defined as including: bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative affects to credit record, damage to or loss of property

- **"Real risk"** is described as requiring consideration of the sensitivity of the personal information, the probability of misuse, and any other prescribed factor

MANDATORY NOTICE

- Report to the Privacy Commissioner any breaches that pose a “real risk of significant harm” to an individual.
- Notify the individual whose information was involved in a breach of any breach that poses a “real risk of significant harm”.
  - The notification must be given “as soon as feasible” after determining a breach has occurred.
- Notify other organizations or government institutions who may be able to mitigate the harm

MANDATORY RECORD-KEEPING

- Organizations shall maintain records of its breaches.
  - The Regulations prescribe a retention period of 24 months after the determination that a breach has occurred.
  - Records of every breach must be kept, whether or not they pose a real risk of significant harm (a threshold difference from the requirement of reporting to the individual affected).

- An individual may file a written complaint with the Commissioner against an organization for contravening these provisions. The Court may order an organization to align its practices with the provisions.

INCIDENT REPORT PLAN

- When breaches of privacy occur, having a clear plan in place to quickly address the breach is a “best practice” to help meet your legal duty and standard of care; mitigate risk; and, help to preserve a positive relationship with tenants and employees.

- Incident Report Plan
  - **Step 1 – Contain the Breach**
  - **Step 2 – Gather the Information**
  - **Step 3 – Assess the Risks**
  - **Step 4 – Notify those Affected**
  - **Step 5 – Keep a Record**
  - **Step 6 – Prevent Future Breaches**

STEP 1: CONTAIN THE BREACH

- **You should take immediate common sense steps to limit the breach:**
  - Immediately contain the breach
  - Designate an appropriate individual to lead the initial investigation
  - Determine the need to assemble a team which could include representatives from appropriate parts of the business.
  - Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage
  - Do not compromise the ability to investigate the breach

STEP 2: GATHER THE INFORMATION

- The initial investigation should focus on the following:
  - Location and date of the incident
  - Date of the discovery
  - Description of the incident
  - Cause (if known)
  - Estimated number of individuals affected
  - Type of individuals affected (tenants, employees, etc.)
  - Types of personal information involved (financial, medical, etc.)
  - Steps taken to contain the breach
  - Those individuals already notified (police, IT, affected induvial), including how and when notification occurred

STEP 3 – ASSESS THE RISKS

- Is there a "real risk of significant harm to an individual"?
  - Consider what information has been accessed, who is affected by the breach and, if possible, what is the cause of the breach.
  - Consider what steps you can take to reduce potential harm.
  - Potential harm is very broadly defined and can include: security risks; physical safety; identity theft; financial loss; humiliation, damage to reputation or relationships; loss of trust in your organization; financial exposure; or, legal liability.

- Do you and your staff have sufficient training to assess that risk? You may need to contact your insurance company or legal counsel to help you assess the risks and formulate a response strategy

STEP 4 – NOTIFICATION

- Does the Risk Assessment identify that there is a real risk of significant harm to an individual?
  - If yes, notification is mandatory
  - If no, notification is optional

- The following may need to be notified or it may be prudent to notify:
  - Affected Individuals
  - The Office of the Privacy Commissioner of Canada
  - Third Party organization or government institutions
    - Mandatory if the third party organization (i.e. press) or government institution (i.e. police) may be able to reduce the risk of significant harm to affected individuals

STEP 5 – KEEP A RECORD

- As of November 1, 2018 it is mandatory to keep a record of **every breach** for 24 months after the day on which you determine that the breach has occurred
- Records shall be kept about **all breaches**, and not just those that pose a real risk of significant harm
  - Best practice: Keep a complete record of Steps 1-3
- Records shall include information about reports to the Commissioner and notification of affected individuals in accordance with this Policy and PIPEDA
  - Best practice: Keep a complete record of Step 4

STEP 6 – PREVENT FUTURE BREACHES

- Once the immediate steps are taken to mitigate the risks associated with the breach, take the time to investigate the cause of the breach and consider whether to develop a prevention plan
- This plan may include the following:
  - a security audit of both physical and technical security;
  - a review of policies and procedures and any changes to reflect the lessons learned from the investigation (e.g., security policies, record retention and collection policies, etc.); and
  - a review of employee training practices; and
  - a review of service delivery partners (i.e. technology providers)

ADDITIONAL CONSIDERATION

- Compliance with PIPEDA is mandatory
- Developing a clear Incident Report Plan is a prudent way to mitigate your organization's risks and ensure compliance with PIPEDA
- Compliance with the new PIPEDA requirements does not alter potential civil liability
- **Best practice**: Conduct regular risk assessments, ensure staff are properly trained, include indemnity provisions in third party contracts, have appropriate insurance in place

QUESTIONS?