Privacy Breaches

& Best Practices

PRESENTATION BY:
JUSTIN PETRILLO
FOI ASSIST

Privacy Breaches & Best Practices

01. Privacy Breach Basics

02. Response Obligations

03. Bill 194

04. Best Practices

05. Key Points

Part One

Privacy Breach Basics

- What is a Privacy Breach?
- Examples
- Types of Privacy Breaches

What is a Privacy Breach?

A privacy breach is the improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.

MFIPPA: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56

FIPPA: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31

"Personal Information" is defined in MFIPPA as "recorded information about an identifiable individual"

(See the definition of "personal information" in MFIPPA for many different examples.)

JUSTIN PETRILLO, FOI ASSIST (FOR THE FOIPN)
SEPTEMBER 25, 2024

What is a Privacy Breach?

A privacy breach is the improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.

Privacy breaches may occur because of innocent mistakes or intentional actions by:

- The officers and employees of an institution, such as a police service
- Third-party service providers (acting on behalf of the above)
- Malicious individuals or organizations (hackers, scammers, etc.)
- Other parties, whether internal or external

JUSTIN PETRILLO, FOI ASSIST (FOR THE FOIPN)
SEPTEMBER 25, 2024

What is a Privacy Breach?

A privacy breach is the improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.

Per the *Information and Privacy Commissioner of Ontario* (IPC):

"The most common privacy breaches occur when unauthorized persons gain access to personal information. For example, personal information may be seized in a cyberattack, stolen (such as through theft of a portable device) or accessed by an employee for improper purposes."

JUSTIN PETRILLO, FOI ASSIST (FOR THE FOIPN)
SEPTEMBER 25, 2024

Example: Lost Bag

- An officer accidently leaves a bag containing notes of an interview with an informant on a subway, in a café, or other public place. The interview includes personal information about the informant and other individuals. Attempts to track down the bag are unsuccessful.

- This constitutes a privacy breach, as it is reasonable to assume an unauthorized individual was able to access the lost records

Example: Cyberattack

- A police service receives a "ransom notice" demanding a transfer of money or cryptocurrency to restore access to electronic files containing personal information. Following the receipt of the notice, the files described in the notice are determined to be inaccessible.

- A privacy breach occurs when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws. Information being rendered inaccessible is not necessarily a privacy breach.

- However, there is a significant risk that the cyberattacker also gained access to the information, which shouldn't be ignored. (Can your IT team rule it out?)

Example: License Plate Data

- A random review of a police service employee's access to an Automated License Plate Recognition System database reveals the employee accessed the database on multiple occasions for personal reasons, namely, to obtain geolocation data (i.e., where a person was at a certain time) relating to a friend or family member.

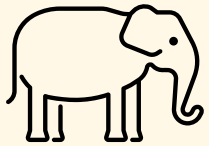
- When information is <u>used</u> in a manner inconsistent with the *Act*, this constitutes a privacy breach as well.

Types of Privacy Breaches

Security Breach

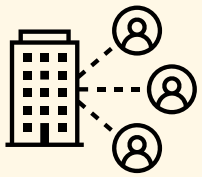
Did the breach reveal a security issue which must be contained?

Significant Breach



Sensitive personal information or large numbers of individuals

Third-Party



Breach at a third party authorized by the institution

Part Two

Response Obligations

- Alert Appropriate Staff
- Identify the Breach
- Contain the Breach
- Notify Affected Persons
- Notify the IPC?

Step One: Alert Appropriate Teams

Privacy breaches are often first discovered by people outside the privacy team.

When a privacy breach is discovered or suspected, the first step should be to reach out to the institution's privacy team, who can lead the response.

Step One: Alert Appropriate Teams

Which teams should be notified?

- If the breach is a security breach, it is important to notify your security team.
  - Some institutions will have different teams for IT security vs. physical security – ensure you notify the appropriate team
- If the breach is a third-party breach, you must coordinate with the third-party/vendor.
  - Determine your points of contact between the institution and vendor.
  - Your contract with the vendor may set out notification deadlines, how to contact the vendor, etc.

Step One: Alert Appropriate Teams

Which other teams should be notified?

- Other teams potentially include:
  - Senior Management
  - Human Resources
  - Legal
  - Contracting/Procurement
  - Public Relations/Media

Step Two: Identify the Breach

It's not always immediately clear how a breach occurred. Sometimes, you may determine information has leaked, but not exactly how the leak happened.

- You might get informed by a member of the public that information the provided to you has been exposed – e.g., a private phone number or email address.
- It's not always clear whether an alleged breach even happened.

Step Two: Identify the Breach

To the best of your ability, try to determine:

- Whether a breach occurred, or is likely to have occurred
- What personal information is potentially involved
- How the breach occurred
- Was it a security breach? Is it a significant breach? Did the breach occur at a third-party authorized by the institution to handle personal information?

Step Three: Contain the Breach

Take corrective action as soon as possible to mitigate the breach.

This can include:

- Shutting down systems, securing access points, or disabling/revoking compromised accounts
  - This covers a lot of ground – you will need the support of your IT team!
- Obtaining the return or destruction of leaked information, especially if the information lost was in "hard copy"

Step Three: Contain the Breach

This can also include:

- Employee training and disciplinary measures
- Improving personal information storage using technologies such as cloud software and encryption
- Improved employee monitoring (checking software audit logs, etc.)
- Monitoring for external uses of the leaked information
- Legal action (especially if parties are uncooperative)

Step Four: Notify Affected Persons

*"You should notify those affected as soon as reasonably possible **if you determine that the breach poses a real risk of significant harm to the individual**, taking into consideration the sensitivity of the information and whether it is likely to be misused.*

If law enforcement is involved, ensure that notification will not interfere with any investigations.

Notification should be direct, such as by telephone, letter, email or in person.

Indirect notification can be used in situations where direct notification is not possible or reasonably practical, for instance, when contact information is unknown or the breach affects a large number of people."

Source: Information and Privacy Commissioner of Ontario, *Privacy Breaches Guidelines for Public Sector Organizations, September 2019*

Step Four: Notify Affected Persons

"***Notification to affected individuals should include***:

- *details of the extent of the breach and the specifics of the personal information that was compromised*
- *the steps taken and planned to address the breach, both immediate and long-term*
- *a suggestion, if financial information or information from government-issued documents is involved, to:*
  - *contact their bank, credit card company, and appropriate government departments to advise them of the breach*
  - *monitor and verify all bank account, credit card and other financial transaction statements for any suspicious activity*
  - *obtain a copy of their credit report from a credit reporting bureau*
- *contact information for someone within your organization who can provide additional information and assistance, and answer questions*
- *a statement that they have a right to make a complaint to the IPC and how to do so*"

Source: Information and Privacy Commissioner of Ontario, *Privacy Breaches Guidelines for Public Sector Organizations, September 2019*

Step Five: Notify the IPC?

The IPC does not expect to be notified of every individual privacy breach. However, they ask that institutions notify them of any significant breach.

The IPC describes significant breaches as involving:

- **sensitive personal information**
  - information which could result in significant harm to the individual to whom it pertains if disclosed
  - could impact an individual's physical or mental health, safety, or financial situation
- **large numbers of affected individuals**

This leaves room for leeway and discretion when notifying the IPC.

Step Five: Notify the IPC?

Keep in mind, the IPC is not primarily out to "expose" or "punish" institutions who have suffered a privacy breach. Rather, the IPC's goals include:

- Helping the institution manage the privacy breach appropriately
- Being prepared to answer questions from members of the public about the privacy breach
- Gathering information and context for potential privacy complaints
- Being prepared for media inquiries

The IPC would much rather hear about the breach from you than from a reporter at *The Globe & Mail*. Don't be afraid to report a significant breach to the IPC.

Part Three

Bill 194

- Mandatory Breach Reporting
- Obligation to Protect Personal Information
- Expanded Powers for the IPC

Bill 194:
Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024

Ontario Bill 194 is currently in second reading.

Bill 194 touches on many areas, but for today's purposes, we'll focus on the parts of the legislation relevant to privacy breaches.

Bill 194:
Mandatory Breach Reporting

Perhaps most importantly, Bill 194 amends FIPPA to require institutions to:

- report "thefts, losses or unauthorized uses or disclosures of personal information" (privacy breaches) to the IPC and to the affected individuals "if there is a real risk of significant harm to the individual or if any other prescribed circumstances exist"
- report annually on the number of breaches reported to the Commissioner during the year.

Bill 194:
Mandatory Breach Reporting

The new statutory requirement to report privacy breaches to the IPC **will affect only institutions who fall under FIPPA**, at least for now.

Breach of privacy safeguards

40.1 (1) The head of an institution shall report to the Commissioner any theft, loss or unauthorized use or disclosure of personal information in the custody or under the control of the institution ***if it is reasonable in the circumstances to believe that there is real risk that a significant harm to an individual would result or if any other prescribed circumstances exist.***

Bill 194:
Mandatory Breach Reporting

Notification to individual (FIPPA ONLY)

40.1 (3) Unless otherwise prohibited by law, the head of an institution shall notify an individual of any theft, loss or unauthorized use or disclosure of the individual's personal information that is in the custody or under the control of the institution if it is reasonable in the circumstances to believe that there is a real risk of significant harm to the individual or if any other prescribed circumstances exist.

Bill 194:
Mandatory Breach Reporting

Real risk of significant harm — factors (FIPPA ONLY)

40.1 (7) The factors that are relevant to determining whether a theft, loss or unauthorized use or disclosure of personal information creates a real risk of significant harm to an individual include,

(a) the sensitivity of the personal information;

(b) the probability that the personal information has been, is being or will be misused;

(c) the availability of steps that the individual could take to,

(i) reduce the risk of the harm occurring, or

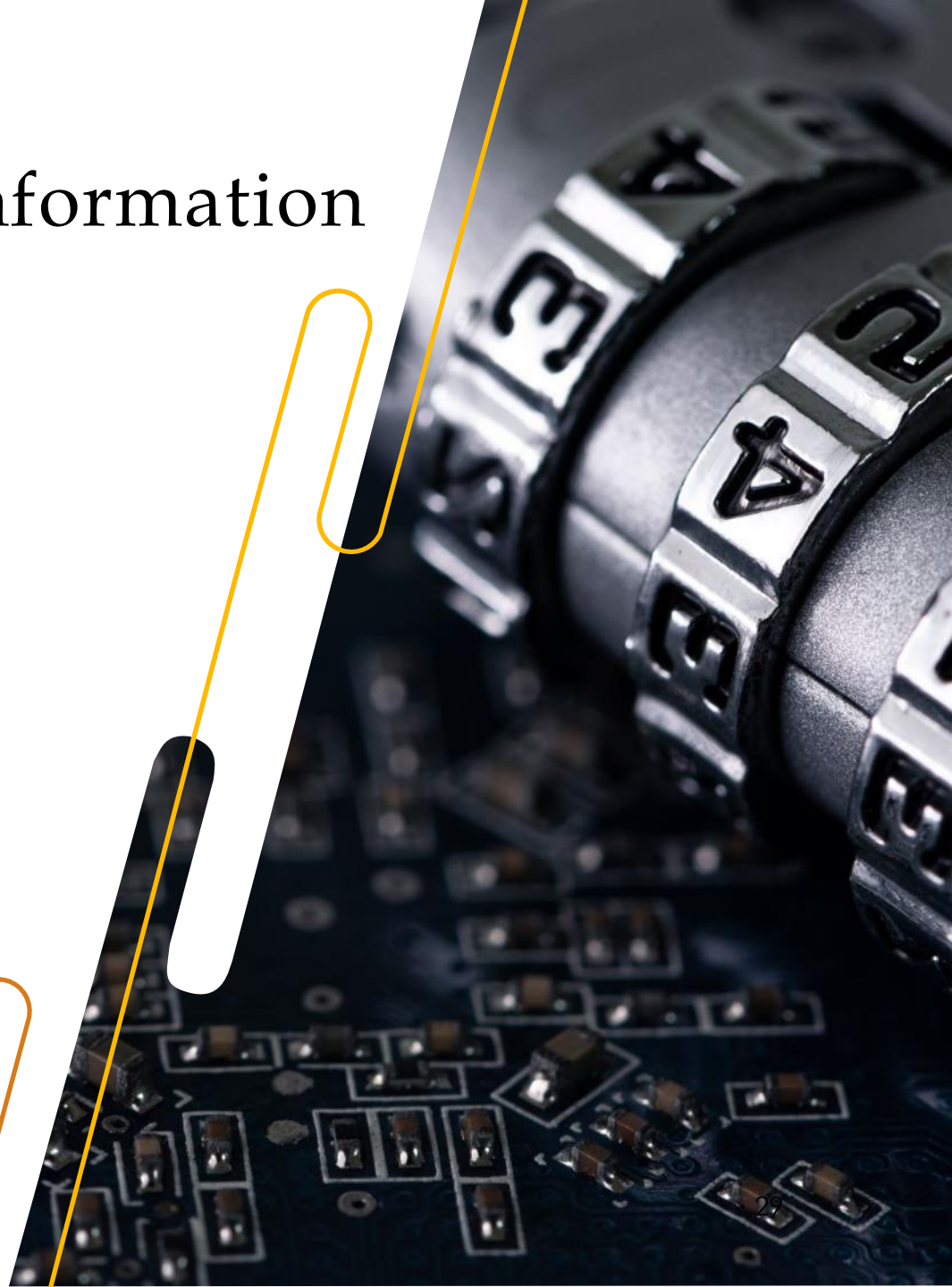
(ii) mitigate the harm should it occur;

(d) any direction, recommendation or guidance provided by the Commissioner pertaining to what constitutes a real risk of significant harm; and

(e) any other prescribed factor. […]

(10) "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Bill 194:
Obligation to Protect Personal Information



New language (FIPPA ONLY)

40 (5) *The head of an institution shall take steps that are reasonable in the circumstances to ensure that personal information in the custody or under the control of the institution is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the personal information are protected against unauthorized copying, modification or disposal.*

Old language (preserved under Bill 194):

Measures to ensure preservation of records

10.1 Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution

Bill 194:
Expanded Powers of the IPC

Commissioner's review of information practices (FIPPA ONLY)

49.0.1 (1) The Commissioner may conduct a review of the information practices of an institution if the Commissioner has received a complaint under subsection 40.1 (4) or has other reason to believe that the requirements of this Part are not being complied with. […]

Orders

(7) If, after giving an opportunity to be heard to the head of the institution, the Commissioner determines that an information practice contravenes this Part, the Commissioner may order the head to do any of the following:

1. *Discontinue the information practice.*
2. *Change the information practice as specified by the Commissioner.*
3. *Return, transfer or destroy personal information collected or retained under the information practice.*
4. *Implement a different information practice as specified by the Commissioner.*
5. *Make a recommendation in respect of how the information practice could be improved.*

Part Four

Best Practices

- Data Policies and Data Security
- Staff Training and Education
- Privacy Breach Checklist

Best Practices:
Data Policies and Data Security

What policies and security measures has your institution taken to reduce the risk of a privacy breach?

- Do remote workers have secure ways of accessing confidential and personal information from home?
- Are you encouraging the use of encryption and cloud services?
  - In the "lost bag" example earlier, if the officer was using an encrypted laptop or a cloud software service to access the personal information, there would have been no breach.

Best Practices:
Staff Training & Education

Staff need to be educated on

- what personal information is
- what policies are in place regarding the use and disclosure of personal information
- what security measures they are supposed to take when dealing with personal information
- How to use such security measures
- **How to recognize a suspected privacy breach and what steps to take**

The last topic is an important one that stands on its own. An institution's privacy team is generally best situated to provide this type of training.

Make your institution aware that the privacy team is the first point of contact for suspected privacy breaches. (Feel free to use this slide deck if it is helpful for your own internal presentations!)

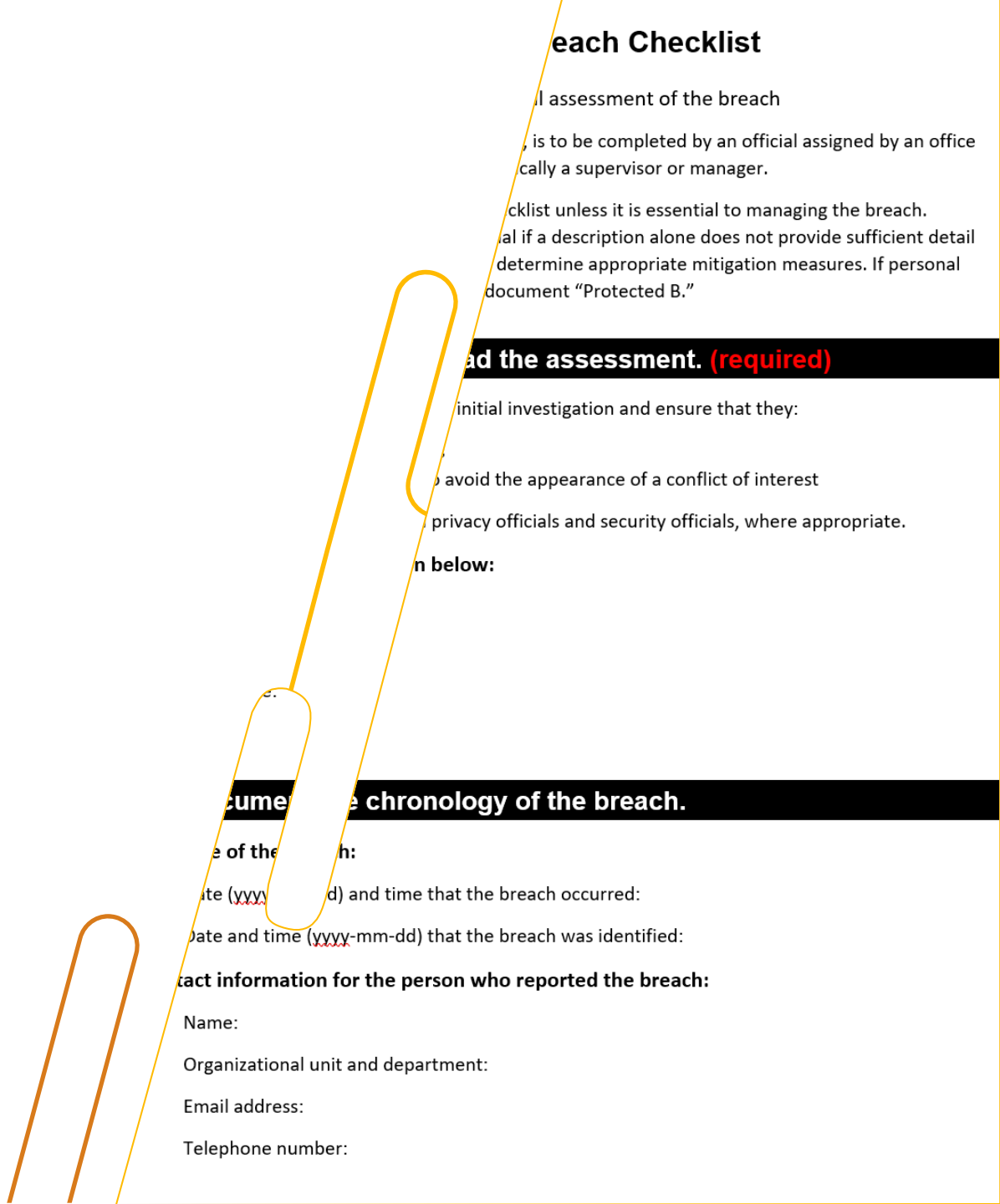
Best Practices:
Privacy Breach Checklist

The Federal Information and Privacy Commissioner recently released a "Privacy Breach Checklist" that can be a very helpful analysis tool for privacy breaches at all levels of government.

Think of it as a Privacy Impact Assessment for privacy breaches. It can be helpful for responding to a privacy breach, and also for learning from the incident after-the-fact, which can help inform policy and security improvements.

To download the checklist, Google canada privacy breach checklist or follow this URL:

https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/privacy-policies-guidance/breach-management/phase-2/complete-privacy-breach-checklist.html


each Checklist

l assessment of the breach

, is to be completed by an official assigned by an office
cally a supervisor or manager.

cklist unless it is essential to managing the breach.
al if a description alone does not provide sufficient detail
determine appropriate mitigation measures. If personal
document "Protected B."

ad the assessment. (required)

initial investigation and ensure that they:

avoid the appearance of a conflict of interest

privacy officials and security officials, where appropriate.

n below:

cume e chronology of the breach.

e of the h:

te (yyyy d) and time that the breach occurred:

ate and time (yyyy-mm-dd) that the breach was identified:

tact information for the person who reported the breach:

Name:

Organizational unit and department:

Email address:

Telephone number:

JUSTIN PETRILLO, FOI ASSIST (FOR THE FOIPN)
SEPTEMBER 25, 2024

Conclusion: Key Points

What we've learned:

Definition of a Privacy Breach

Improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.

Response Obligations

Alert internal teams, identify & contain the breach, notify affected persons – and maybe IPC

Bill 194

Mandates breach reporting, obligates institutions to protect personal information, and gives the IPC new order powers – but these changes are limited to FIPPA institutions for now

Conclusion: Key Points

Best Practices:

Data Policies & Security Measures

Proactively prevent privacy breaches by improving privacy policies and security measures

Staff Education

Teach staff how to recognize a privacy breach and train them to notify the privacy team first

Privacy Breach Checklist

A Privacy Breach Checklist is a great tool for analyzing a privacy breach after the fact and informing policy and security improvements.

Thank you!

Justin Petrillo
justin@foiassist.ca
foiassist.ca

FOI Assist