IPC Guidance on Public Sector Outsourcing

Fred Carter

Senior Policy & Technology Advisor

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

OPBA

16 Oct 2024

Overview

About the IPC

Context

Origins

Relevant investigations

Scope and process

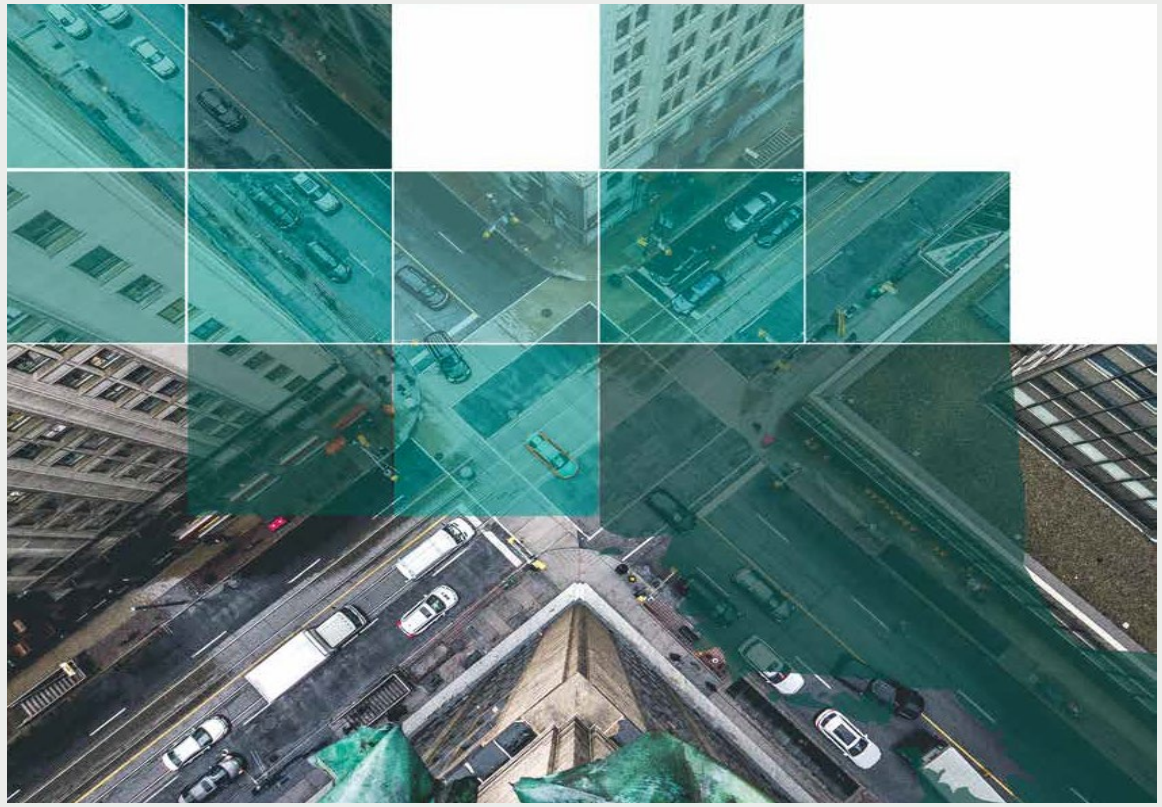
Definitions

Guidance

The Information and Privacy Commissioner of Ontario

- The IPC oversees Ontario's **access and privacy** laws
  - Our access and privacy laws establish the public's right to *access government-held information* and *protect their personal privacy rights*

- The IPC provides **independent** review of government decisions and practices on access and privacy



Information and Privacy Commissioner of Ontario

- **Patricia Kosseim**—appointed by Ontario Legislature (July 1, 2020)
- 5 year term
- Officer of the Legislature appointed by, and reports to, the Legislative Assembly of Ontario. Independent of the government of the day
- Assistant Commissioners:
  - Michael Maddock, Strategic Initiatives and External Relations
  - Warren Mar, Tribunal and Dispute Resolution Services

IPC Mandate

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - covers 1,200 municipal organizations
- *Personal Health Information Protection Act* (*PHIPA*)
  - covers individuals and organizations involved in the delivery of health care services
- *Child, Youth and Family Services Act* (Part X) (*CYFSA*)
  - children's aid societies, child/youth service providers
- *Anti-Racism Act (ARA)*
  - oversight of the privacy protective rules

IPC Roles

- **investigate privacy complaints** related to personal information
- **resolve appeals** when there is a refusal to grant access to information
- **ensure compliance** with the acts we oversee
- **review** privacy policies and information practices
- **conduct research** on access and privacy issues and **provide comment** on proposed government legislation and programs
- **reach out and educate** the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

Context

- Growing reliance on 3rd-party service providers and complex “public-private partnerships”
- Blurred lines of accountability? Custody versus control of institutional records including personal information.
- New privacy and security risks when outsourcing
  - Unauthorized disclosures and uses of personal information, sensitive records
  - Half of all reported cybersecurity breaches in 2023 originated from third parties
- General trends in third-party risk management

Origins

- “You can outsource services but not accountability”
- IPC MNR investigation report (2012)
- IPC guidance on cloud computing (2016)
- Edtech investigation reports (2020-23)
- OPS procurement policies and practices
- Accelerating digitization and public-private partnerships
- Gap in public sector guidance

Relevant IPC investigations

- Edsby: Agent breached: concurrent investigation by IPC and OPC
  Key lesson: contract terms not enforced, e.g. ISO 27001
- Google G Suite / Classroom: Value of contract addendum negotiated by province.
  Key lesson: need to monitor evolving services and update contract requirements
- HRDSB: Menu of permissible apps included questionable privacy policies and TOUs
  Key lesson: need to systematically review/vet/approve apps for use by teachers and students
- **Need for greater due diligence**
- **Contracts are not enough: they must be coupled with appropriate monitoring and oversight to ensure compliance with privacy and access to information laws**

Scope and Process

- Targeted at FIPPA and MFIPPA institutions
- For use by FOICs, privacy officers, legal, procurement specialists, project managers
- Developed with input from: • provincial ministries • municipalities • education sector • law enforcement • transportation • gaming and alcohol institutions
- Voluntary and adaptable recommendations
- NOT standard contractual clauses
- NOT a legal research report

Definitions

- Institutions / organizations / agents
- Data / information / personal (health) information (almost anything)
- Identifiable / de-identified data
- Outsourcing / contracting / procurement
- PIA / TRA
- Institutional Records (types: structured/unstructured, transient, logs)
- Agreement / contract

IPC Guidance on Contracting

Due diligence checklist for key phases of procurement:

1. Planning
2. Tendering
3. Vendor selection
4. Agreement
5. Agreement management / close-out

1. Planning

- Engage relevant experts (including FOIC and privacy staff) to identify and address access and privacy matters.
- Define types of records / personal information to be covered by the services
- Identify access, privacy and security risks, and develop appropriate measures to mitigate them
- Define specific access, privacy and security requirements (or prohibitions) to be imposed on the service provider.

2. Tendering

The tendering documents (and agreement) should define:

- Records to be processed
- Limits on processing
- Notices of collection
- Privacy and security program requirements
- Reporting requirements (e.g. evidence of compliance)
- data de-identification requirements
- breach management requirements
- Prior notices of significant changes (e.g. sub-contracting)

3. Vendor Selection

Institutions should select a service provider with capacity to comply with the tendering conditions, eventual agreement and other requirements.

They should ensure:

- access, privacy and security components of the evaluation are assigned appropriate criteria and weighting relative to the sensitivity, scope and scale of records and personal information that will be processed.
- access, privacy and security components of the selection process receive thorough evaluation by subject-matter experts, and are documented.
- prospective service providers know that records they submit or share as part of the procurement process are subject to the FOI provisions of MFIPPA.

4. Agreement

Service agreement should reflect scope and deliverables of procurement including access, privacy and security requirements defined in the tendering documents, including:

- Contract provisions should address: ownership of data; collection, use and disclosure of records and personal information, treatment of confidential information; notices of compelled disclosure, subcontracting, safeguards, audits, and retention / destruction.
- Recommended contract provisions are neither authoritative nor exhaustive. Please consult with relevant experts.

5. Agreement management and close-out

Institutions should take specific action(s) to monitor service providers' performance to ensure compliance with contract requirements and prohibitions, including:

- Ensuring risk assessments, audits, or inspections are undertaken on a timely basis,
- Ensuring timely and appropriate reporting of privacy breaches
- Enforcing agreement terms in the event of a breach of contract involving access, privacy or security violations.
- Defining what close-out actions (such as return of records, secure disposal, including backups) will be undertaken

Discussion

Contact Us

info@ipc.on.ca