Privacy Impact Assessments

Pre-conference Workshop

October 9, 2013 - Privacy and Access 20/20

Linda Sasaki, Mary Golab and Veronica Chodak

Office of the Information and
Privacy Commissioner of Alberta

Introductions

- A bit about us
- Housekeeping
- Objectives/purpose of the workshop
- Workshop agenda

Workshop Agenda

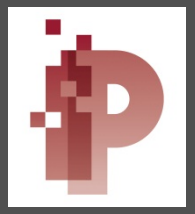
Planned time	Topic/Activity
9:15-9:55	Presentation on Basic PIA
9:55-10:35	Group exercise & discussion
10:35-10:45	Break
10:45-10:55	Presentation on Complex PIA
10:55-11:30	Group exercise & discussion
11:30-11:35	Recap/Resources
11:35-12:00	Questions and Wrap-up

BASIC PIA

What is it, Laws & Legislative Requirements, Triggers, Nuts & Bolts, Tools, and Case Study I.

WHAT IT IS

Defining what a PIA is

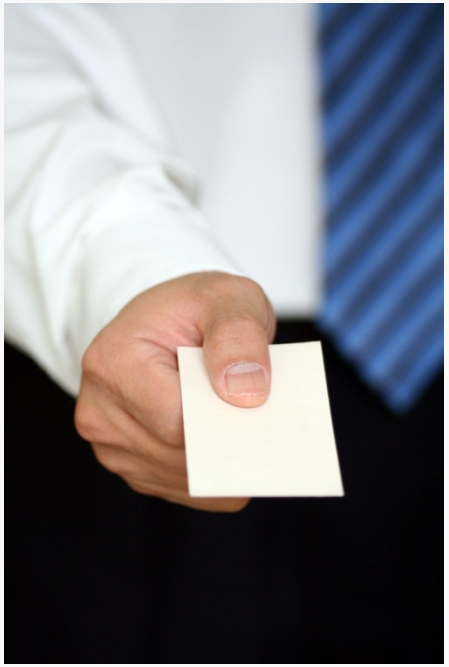


A PIA is…

- An assessment of privacy risk for a new project
  - Describes the project
  - Provides analyses of personal and health information
  - Confirms legal authority to collect, use and disclose personal and/or health information
  - Identifies risks to confidentiality, integrity and availability of personal and/or health information
  - Describes measures to mitigate risk
  - Describes plans to ensure on-going compliance

A PIA is not …

- Project charter
- Technical architecture
- Contract
- Security assessment
- Marketing
- **Get out of jail free card**



What’s the Pay-Off ?

- Proactive Approach to Privacy Management
- Building Trust
- You are the first to learn about any potential privacy pitfalls related to the project

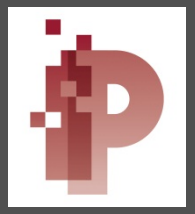
More Pay-Offs…

- PIAs contribute to compliance which hopefully reduces the numbers of complaints and alleviates the need for subsequent investigations, audits, complaints, etc.

- Reputation

- Legal Requirement – you just gotta do one!

COMPLIANCE WITH PRIVACY LAWS



Why include privacy law(s)?

- Helps to ensure that a project complies with privacy law and other legislative requirements.
- Initiates discussion about the project's information-handling practices and business rules comply with specific legal obligations (consent, protection)
- Provides a listing of relevant privacy laws applicable to the project.

Applicable provincial and federal privacy laws

- Freedom of Information and Protection of Privacy Act (FIPPA) (British Columbia)
- Freedom of Information and Protection of Privacy Act (FOIP) (Alberta)
- Health Information Act (HIA) (Alberta)
- Personal Information Protection Act (PIPA) (AB)(BC)
- Personal Information *Protection and Electronic Documents Act* (PIPEDA) (Federal)

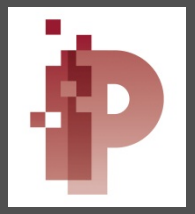
Roles of the OIPC (BC) and Gov (BC)

- OIPC Role
  - Reviews and comments on PIAs that address a common or integrated program or activity or a data-linking initiative.
  - Does not approve PIAs

- Government Role
  - The Office of the Chief Information Officer (within the Ministry of Technology, Innovation and Citizen‘s’ Services) coordinates ministry PIAs. All government PIAs go through this entity.

WHAT TRIGGERS A PIA

Ready, set…PIA!



What Would Trigger a PIA?

- Mandatory triggers to PIA
  - Legislative Requirements etc.

- Best Practice
  - Circumstances where PIAs should be considered

Mandatory Triggers

- FIPPA– British Columbia:
  - Mandatory for most public bodies planning a “data-linking initiative” or a “common or integrated program or activity” to provide early notice (by letter) to OIPC (s. 69)
  - Government can prescribe regulations related to data-linking initiatives (s.36.1) Public Bodies considering a data-linking initiative should check with the Ministry of Technology, Innovation and Citizens’ Services.

Best Practice Triggers

- Consider a PIA when you plan a

- New System or administrative practice

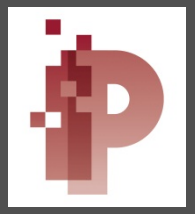
  Or

- Major change to an existing system or practice

  That will

- Collect, use and disclose identifying information

PIA NUTS & BOLTS



When do you start?

- Privacy should be considered when developing business requirements

- Start considering privacy early
  - PIA simply becomes a matter of documenting the privacy design

Getting started

- Determine the purpose of the PIA
  - Internal use
  - Submission to oversight body
  - Available to public
- Get executive buy-in, using purposes as selling points

Getting started… continued

- Begin working with project team
- Project team cooperation is essential
- Important that privacy not seen as roadblock

- Observation: you may be the only one that really understands the project holistically

Who Should Conduct the PIA ?

- Someone with an intimate understanding of your business, who knows privacy law, your regulatory environment, technology, risk analysis, security, records management, project management, communications and who can achieve executive buy-in

- Or…

Who Should Conduct the PIA ? - Cont

- Or a **team**…

  - Privacy lead
  - Business area
  - Legal counsel
  - Information technology
  - Records management
  - Communications

Build PIA into existing business processes

Privacy Check (informal)
Information Flow Analysis
Privacy Scan
Legal consult
OIPC consult

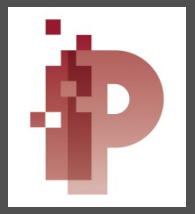
Formal PIA submission
Business Area sign-off
Executive sign-off
Formal 3rd party review

Draft PIA
Confirm Information Flow Analysis
Business Area Review
Formal Legal Opinion
OIPC consult

Post Implementation
Privacy/security audit
Amendments

KEY ELEMENTS OF A GOOD PIA

Now that’s a good PIA!



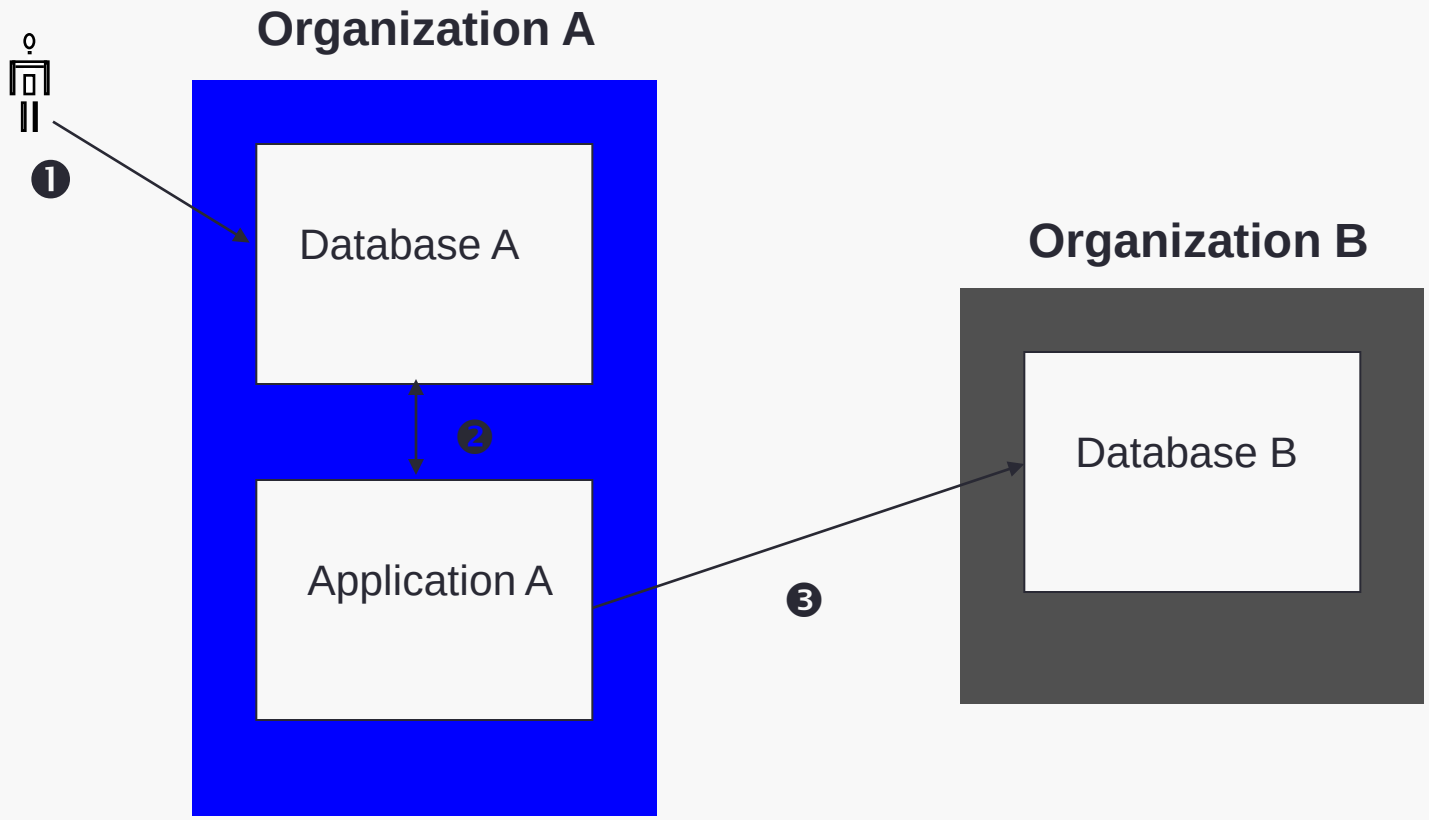
Elements of a good PIA

- Description of the entity's privacy management program
  - Is there a "privacy culture"?
  - Is there someone in charge of privacy?
  - Are privacy policies in place?
- Overview of the project and benefits
- How are your employees and parties trained in privacy?
- Incident Response
- Access Requests

Elements of a good PIA Continued….

- Legal authority to collect (notification), use and disclose personal or health information
- Information flow
- Analysis of privacy risks and mitigations
- Who has access to personal or health information?
- Consent and “Expressed Wishes"
- Identifies relationships with parties
- Review and compliance plans

Information flow diagram



PIA Elements - legal authority and purposes table

Information flow	Description	Information type(s)	Purpose	Legal authority
1.	Collection of personal information directly from individual	Name, address, DOB	Registration and participation in program	Sec. 33(c) FOIP Act
2.	Use of p.i.	Name, address	Billing of registration fees	Sec. 39(1)(a) FOIP Act
3.	Disclosure of p.i. to collection agency	Name, address	Debt Collection	Sec 40(1)(k)(i)

Good PIA: Risk Analysis & Mitigation

- Identify potential threats to privacy
  - Consider impact and probability
  - Should be project-specific
- Determine ways to reduce risk
  - Mitigate
  - Transfer (Can't contract out….)
  - Accept
- We recognize that you can't eliminate all risk
  - No risk = no business

Risk Mitigation Table

Privacy Risk	Description	Mitigation Measures	Policy Reference
What is the risk	Describe the risk	Administrative, technical and physical measures	Refer to policies and procedures that mitigate this risk.
1. Unauthorized access	Snooping by users	Access controls. Training. Confidentiality agreements. Audit logs.	Privacy Policy Manual (Appendix 7) Confidentiality Agreement (Appendix 8)

5 common privacy risks in a project

1. Unauthorized access of personal or health information by internal or authorized parties.
2. Unauthorized c,u,d of personal or health information by external parties.
3. Loss of integrity of personal or health information.
4. Loss, destruction, or loss of use, of personal or health information.
5. Your contractor or business partner c,u,d personal or health information in contravention of one or a combination of privacy legislation

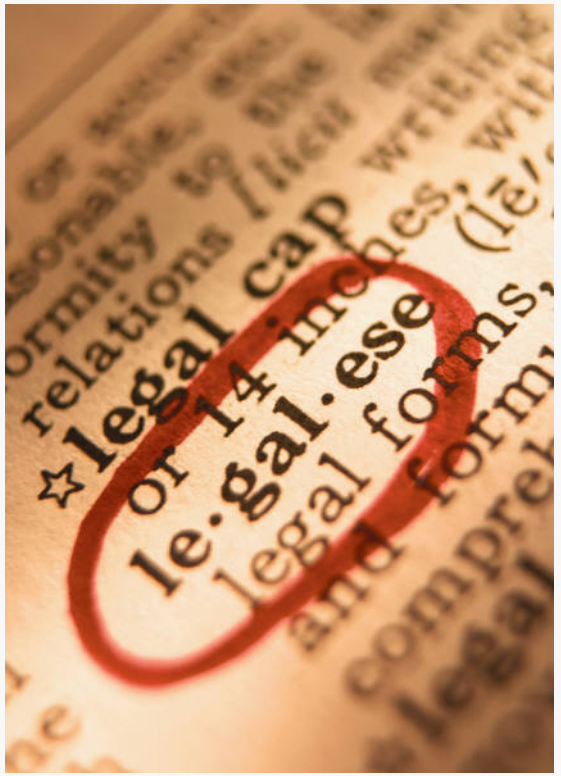
Example Risk Analysis

- Risk:
  - “Snooping”
  - Probability? Impact?

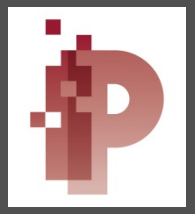
- Mitigation strategies
  - Access controls and permissions
  - Training and awareness
  - Audit of user activity

Characteristics of a Good PIA

- Non-technical
  - Avoid IT, legal jargon
- A living document
  - Include in project library, user documentation
  - Reference for future reviews
- Available to the public
- Available to staff



WHAT TOOLS DO YOU NEED TO CONSTRUCT AND SUPPORT A PIA ?



TOOLS

- Legislation
  - Are you required by law to do a PIA or is it a suggested best practice?
  - Section 69(5) of BC FIPPA

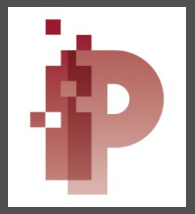
- Internal Policies & Procedures
  - Establish policies and procedures that support compliance with privacy legislation (ie. is there a policy on the management of access requests?)
  - Can be used as guidance during the development of the particular project (are amendments needed)?

TOOLS Continued

- External Guidance Documents
  - BC Ministry of Technology, Innovation and Citizens' Services Privacy Impact Assessment Process
  - Accountable Privacy Management in BC's Public Sector
  - Office of the Information and Privacy Commissioner of Alberta's Privacy Impact Assessment Requirements Publication

CASE STUDY

Group Exercise 1 – Getting the PIA



Case Study – PIA
Exercise 1- “Getting the PIA Started”

- To understand and use the basic building blocks of a PIA

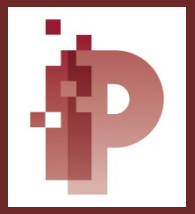
- To identify from the case study, the following:
  - Do I need to do a PIA?
  - Stakeholders or Key players involved
  - What personal information will be handled?
  - Authorities (collection, use or disclosure)

Case Study I Wrap-up

- PIA?
- Stakeholders or Key players:
- Types of Personal Information:
- Authorities:

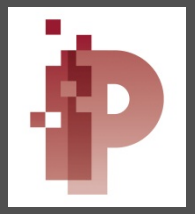
COMPLEX PIA

Definition, Relationships, and Case Study II

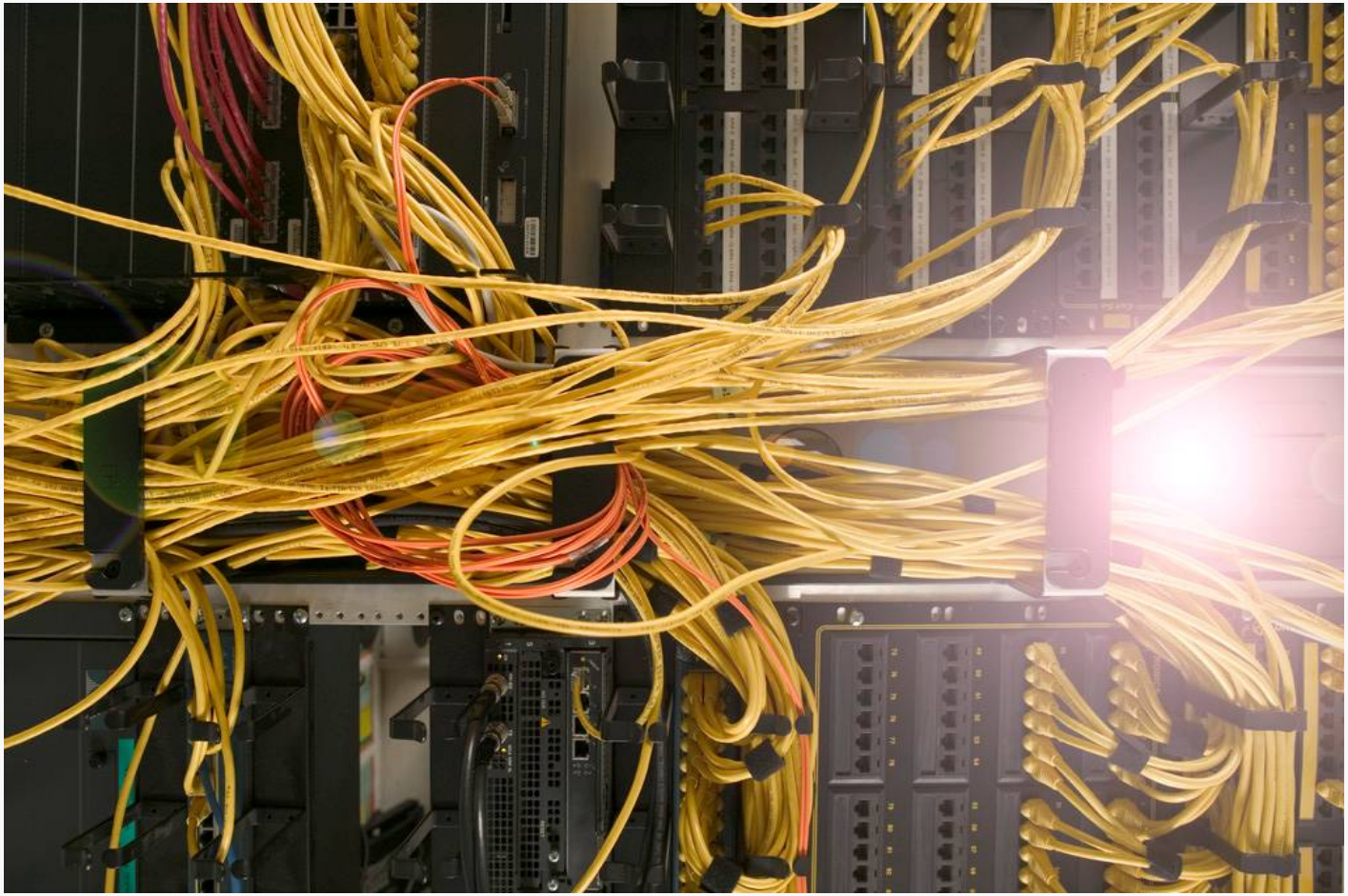


IT JUST GOT COMPLICATED

Defining a complex PIA



How complicated?



Watch for complications

- Outsourcing
- Imported solutions
  - “The vendor says it’s HIPPA-compliant!”
- PIA seen as roadblock
  - Executive buy-in
  - Project team buy-in
- Once PIAs become routine
  - Cookie-cutter approach
- Monitoring
- Multiple parties involved

Multi-party PIAs

- Increased complexity, but not impossible

- Each party may need to write their own organizational management piece
- Do single version of project-specific piece
  - Decide from whose perspective you are writing

Multi-party PIA Continued

- Beware of different jurisdictions
    - Different laws may apply to the different entities
- Your biggest challenges will be sign-off and on-going review
    - If no-one's in charge everyone signs-off

What do you need to consider with a complicated PIA?

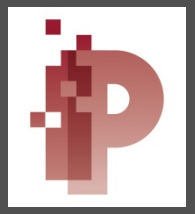
- The person submitting the PIA is authorized to do so.
- All parties are identified, and have signed off on the PIA or there's evidence of endorsement
- The PIA describes:
  - How each party is involved.
  - Who is accountable for what personal information.
  - How changes affecting the PIA will be managed.
  - Who is accountable to update the PIA.
  - How the PIA will be revisited to ensure accuracy.

More Considerations

- Information flows for each party are clear and include legal authorities
- Describe how notification requirements will be met.
- Describe who will receive access or correction requests and how this is made public.
- Describe how privacy breaches will be managed.
- Identify who has custody or control of personal information

MULTIPLE PARTIES

Relationships are important



Parties Relationships

- **Someone needs to be in charge**

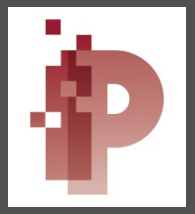
- Parties will have differing interests/perspectives
- There will be varying levels of privacy awareness
- Differing policies and procedures
- Differing legislative requirements

Considerations

- Who has custody and control of the information?
- How are you operating?
- Identify all your stakeholders and information flows and authority
- Who is accountable?
- Who submits your PIA? (someone with authority)
- What consent provisions apply?
- Watch for commitment

CASE STUDY

Group Exercise 2 - Risk Assessment



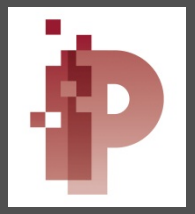
Case Study
Group Exercise 2 – Risk Assessment

Privacy Risk	Description	Mitigation Measures	Policy Reference
What is the risk	Describe the risk	Administrative, technical and physical measures	Refer to policies and procedures that mitigate this risk.
1. Unauthorized access	Snooping by users	Access controls. Training. Confidentiality agreements. Audit logs.	Privacy Policy Manual (Appendix 7) Confidentiality Agreement (Appendix 8)

Group Exercise 2

- General discussion of risks

RECAP



Recap – 5 Stages of a PIA Process

1. Establishing whether you need a PIA
2. Project Description
3. Identifying the key players (relationships), types of personal information, mapping the flows of personal information, and authorities
4. Assessing the privacy risks and developing and implementing mitigation strategies
5. Ongoing review and management of the PIA (remember it's a living document)

PIA Resources

- “Privacy Impact Assessment Requirements for use with the Health Information Act”, available on the internet at www.oipc.ab.ca
- “Early notice and Privacy Impact Assessments to OIPC (BC) under FIPPA, available at www.oipc.bc.ca
- “Accountable Privacy Management in BC Public Sector” available at www.oipc.bc.ca
- “Privacy Impact Process (PIA)” published by the BC Ministry of Technology, Innovation and Citizens’ Services available at www.cio.gov.bc.ca
- http://www.oipc.gov.nl.ca/resources.htm (NF - Privacy Audit)
- www.oipc.sk.ca/resources.htm (SK)
- http://www.ombudsman.mb.ca/compliance-phia.htm (MB)
- http:www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp (CAN – PIA e-learning tool)

A PIA Checklist

- Is there personal information?
- Evidence that the appropriate level of delegated authority submitted the PIA
- A project summary with objectives, rationale, clients, approach, programs, or partners involved
- A list of all parties, their roles and responsibilities

PIA Checklist cont.

- Describes organizational privacy management
- Includes a list of the personal information
- An information flow analysis (with a diagram)
- Identifies legal authorities and purposes (table)
- Describes how notification requirements are met
- Describes the role of consent (if used)

PIA Checklist…cont.

- Describes how incident responses be managed
- Describes how access and correction requests are managed
- Includes an analysis of risks and mitigations
- Describes how monitoring, reviews, and updates will occur
- Describes contracts or agreements with other parties involved in the project
- The policy and procedures related to the project are attached

Office of the Information and Privacy Commissioner of Alberta

410, 9925 - 109 Street
Edmonton, Alberta
T5K 2J8
Phone: (780) 422-6860

Suite 2460, 801 6 Avenue SW
Calgary AB, T2P 3W2
Phone: (403) 297-2728

Toll Free: 1-888-878-4044

www.oipc.ab.ca