大成 DENTONS

2nd annual Dentons Data Summit: Navigating data and privacy in the new normal

June 8, 2020

dentons.com

大成 DENTONS

2nd annual Dentons Data Summit:

Managing a privacy program in the post-COVID environment

June 8, 2020

dentons.com

Meet our presenters

Kirsten Thompson
Partner, Toronto
D+1 416 863 4362
kirsten.thompson@dentons.com

Luca Lucarini
Associate, Toronto
D+1 416 863 4735
luca.lucarini@dentons.com

The highlights

1. **Privacy programs and pandemics: the challenges of change and uncertainty**
   - Risk landscape
   - Enforcement landscape

2. **What you know….and what you don't**
   - Data inventories
   - Privacy Impact Assessments (PIAs)

3. **Operational privacy**
   - Framework
   - Customers returning to physical
   - Payments

The highlights

4. Managing information security risk

- Physical files and electronic devices
- Telecommunications/videoconferencing

5. Incident response plans

6. Privacy policies

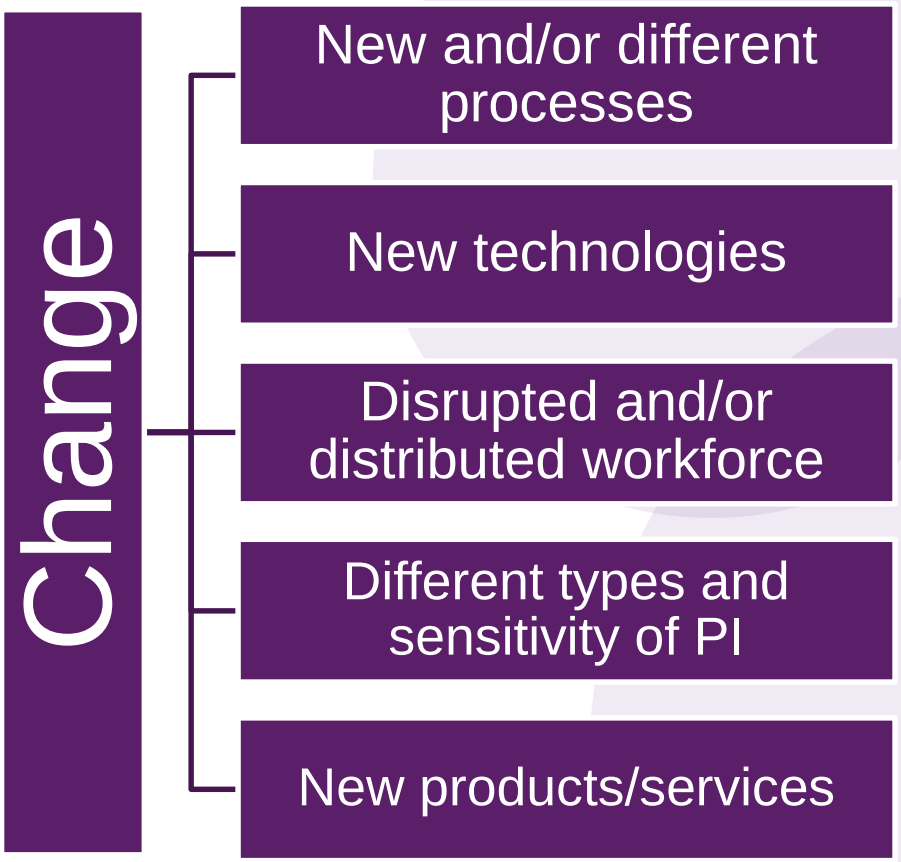
大成 DENTONS

1. Privacy programs and pandemics

Privacy programs and pandemics

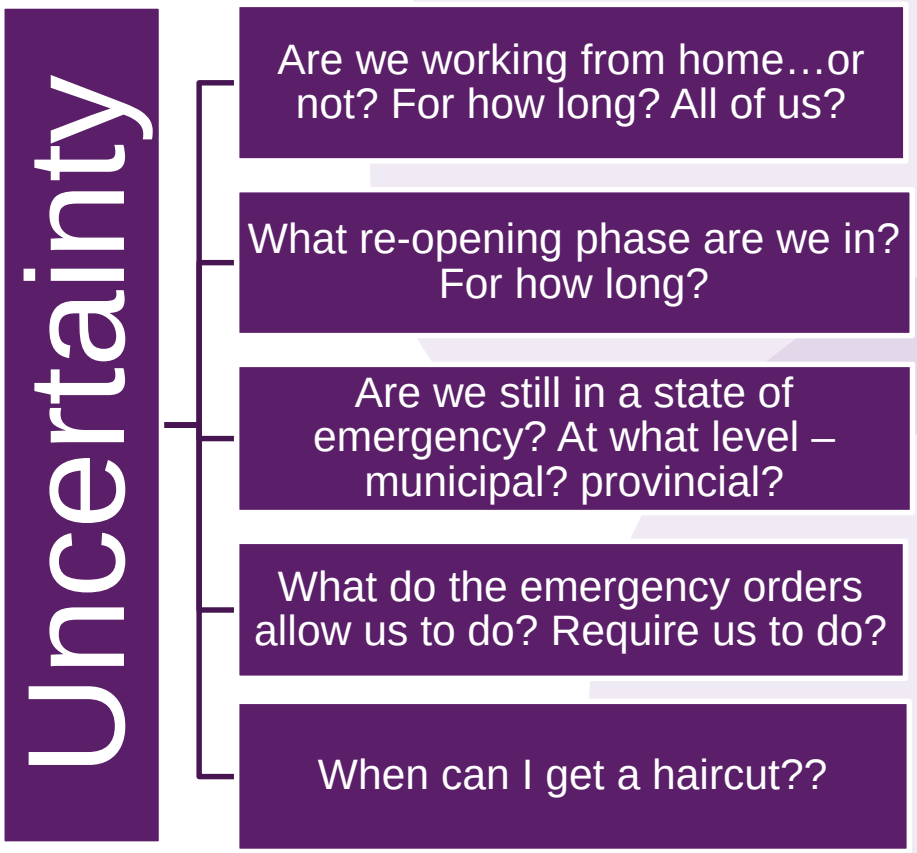
大成 DENTONS

Risk landscape: change and uncertainty



Privacy programs and pandemics

Risk landscape: change and uncertainty



Privacy programs and pandemics

大成 DENTONS

Enforcement landscape: Privacy laws continue to apply

- Office of the Privacy Commissioner of Canada ("**OPC**"):

> *The OPC will continue to protect the privacy of Canadians, while adopting a **flexible and contextual** approach in its application of the law.*
>
> OPC Guidance (March 20, 2020)

- Privacy Commissioner of Alberta ("**AB OIPC**"):

> *…orders issued under public health legislation could require the collection, use and disclosure of certain personal information relating to employees and customers.*
>
> *If you need to collect, use or disclose employee personal information in an emergency, you should communicate to your employees the **specific legislative authority** that is engaged to do so.*
>
> AB OIPC Guidance (undated)

大成 DENTONS

2. What you know…and what you don’t

What you know/don’t know

- Risk mitigation is impossible unless you understand the risk
- To understand the risk, you have to understand what you’re dealing with

What you know/don't know

- **Data inventory:** an internal assessment about the data an organization has collected, the location where the data is stored, how long it is being retained, and with whom it has been shared (internally and externally with third-parties), etc.
- Best practice (not required under Canadian law; arguably required under GDPR to support Art. 30 compliance)
- Can be done for all types of data across the enterprise

Pro Tip: Scale down. If you don't already have a data inventory process in place, consider just doing one for COVID-related measures, and just for personal information.

What you know/don't know

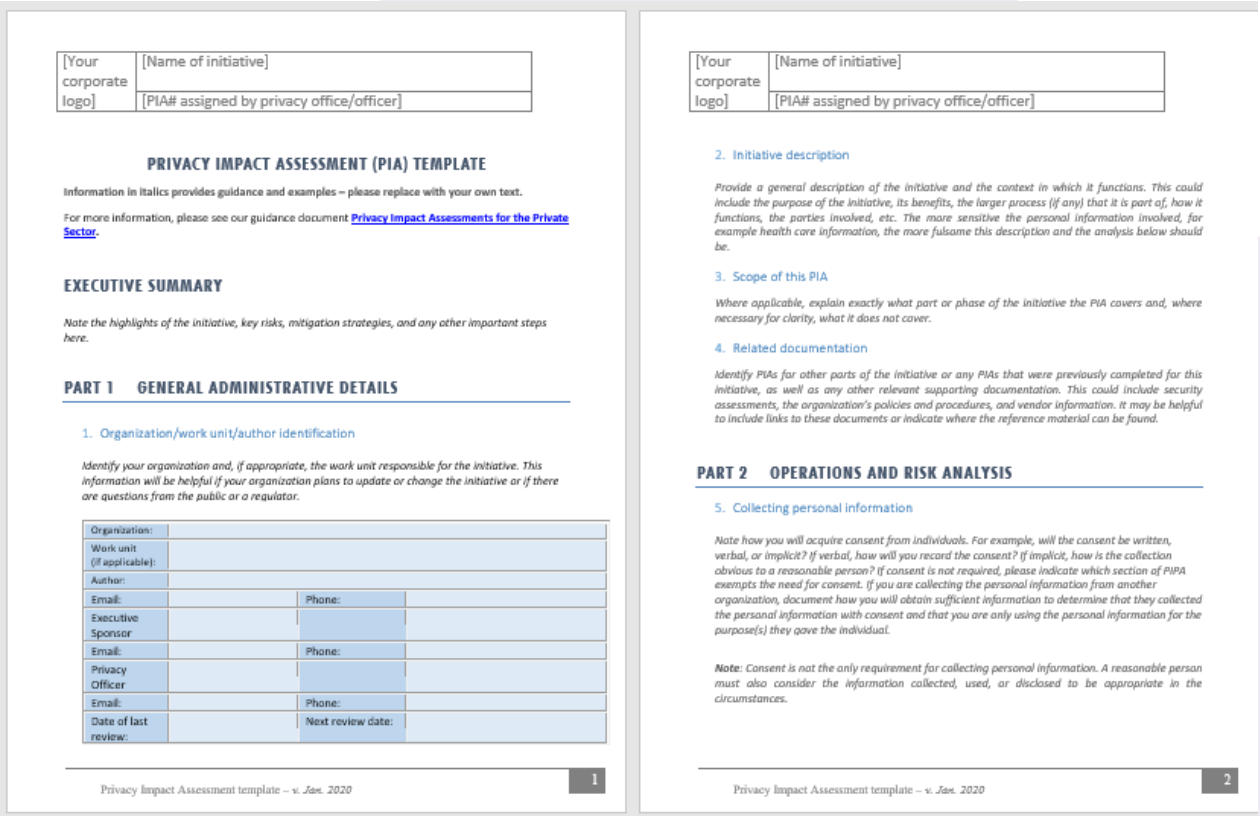
For each process involving personal information ("**PI**"), track what PI is to be collected, used or disclosed ("**C/U/D**"), the specific purpose for C/U/D of PI, whether the PI is sensitive, how long it will be retained, what (if any) regulatory requirements are attached to the PI, etc.

EXAMPLE DATA INVENTORY FOR CLUBS

Method of collecting personal data	What personal data is collected	Data Subject(s)	When is this data collected	Volume of Personal Data	Why is this data collected? (see notes section below *)	Where is data stored?	Security measures already taken?	Retention period and when are any updates carried out	Data Controller? Joint Data Controller? Data Processor? (see notes section below **)	Has a suitable privacy notice been issued?	Person responsible for handling data
1.Club Membership Form	Personal information requested from our members • Name • Address • Date of birth • Emergency contact name • Emergency contact number x 2 • Medical history / conditions that the club should be aware of • Email	All members Parents/carers of junior members (u16 year olds)	When they join the club (anytime throughout the year)	100 club members plus any new that join	To be able to communicate with members regarding club matters (consent) To be able to submit the required personal information on grading sheets sent to HQ to enable them to process gradings (consent) To be able to ensure the safest and most appropriate service to members by understanding any specific needs they may have or medical conditions that could	In a club file that is the responsibility of the club head coach Club coach responsible for the security of the file during the session	Office where file located is kept locked	Held until the individual leaves the club when their record is then deleted Club request new form completion at the start of each year (January)	Data controller	Privacy notice is displayed on our club website and handed out along with our club membership forms	Club head coach or lead coach at session

What you know/don't know

- The data inventory becomes the basis for a Privacy Impact Assessment in respect of each new process
- **Privacy Impact Assessment** ("**PIA**"): a process of analysis that helps to identify and address potential privacy risks that may occur in the operation of a new or redesigned project



[Your corporate logo]	[Name of initiative]
	[PIA# assigned by privacy office/officer]

PRIVACY IMPACT ASSESSMENT (PIA) TEMPLATE

Information in italics provides guidance and examples – please replace with your own text.

For more information, please see our guidance document Privacy Impact Assessments for the Private Sector.

EXECUTIVE SUMMARY

Note the highlights of the initiative, key risks, mitigation strategies, and any other important steps here.

PART 1 GENERAL ADMINISTRATIVE DETAILS

1. Organization/work unit/author identification

Identify your organization and, if appropriate, the work unit responsible for the initiative. This information will be helpful if your organization plans to update or change the initiative or if there are questions from the public or a regulator.

Organization:			
Work unit (if applicable):			
Author:			
Email:		Phone:	
Executive Sponsor			
Email:		Phone:	
Privacy Officer			
Email:		Phone:	
Date of last review:		Next review date:	

Privacy Impact Assessment template – v. Jan. 2020 1

[Your corporate logo]	[Name of initiative]
	[PIA# assigned by privacy office/officer]

2. Initiative description

Provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. The more sensitive the personal information involved, for example health care information, the more fulsome this description and the analysis below should be.

3. Scope of this PIA

Where applicable, explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

4. Related documentation

Identify PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative, as well as any other relevant supporting documentation. This could include security assessments, the organization's policies and procedures, and vendor information. It may be helpful to include links to these documents or indicate where the reference material can be found.

PART 2 OPERATIONS AND RISK ANALYSIS

5. Collecting personal information

Note how you will acquire consent from individuals. For example, will the consent be written, verbal, or implicit? If verbal, how will you record the consent? If implicit, how is the collection obvious to a reasonable person? If consent is not required, please indicate which section of PIPA exempts the need for consent. If you are collecting the personal information from another organization, document how you will obtain sufficient information to determine that they collected the personal information with consent and that you are only using the personal information for the purpose(s) they gave the individual.

***Note**: Consent is not the only requirement for collecting personal information. A reasonable person must also consider the information collected, used, or disclosed to be appropriate in the circumstances.*

Privacy Impact Assessment template – v. Jan. 2020 2

What you know/don’t know

- Data inventories / PIAs will form the basis of an organization’s ability to identify and respond to risks such as over-collection and retention, improper secondary uses etc.
- PIAs allow you to make a considered business decision about the level risk you as an organization are willing to accept – and may help you also identify risk mitigation strategies

大成 DENTONS

3. Operational privacy

1. Framework for introducing new measures

As a general rule, when implementing a new process or technology, an organization should consider the balance of factors:

Necessity: there must be a clearly defined necessity for the use of the measure, in relation to a pressing societal concern (in other words, some substantial, imminent problem that the new measure seeks to treat).

Proportionality: that the measure (or specific execution of an invasive power) be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the privacy rights of the individual being curtailed.

Framework for introducing new measures

Effectiveness: that the measure be shown to be empirically effective at treating the issue, and so clearly connected to solving the problem.

Minimal intrusiveness: that the measure be the least invasive alternative available (in other words, ensure that all other less intrusive avenues of investigation have been exhausted).

Case study

WidgetCo. is re-opening its widget factory. As part of its re-opening process, it plans to institute temperature checking of its workers. However, WidgetCo. is concerned that it will need to train screeners, manage shifts and lineups, etc., and processes will generally bog down.

FaceScan Inc. sells an automatic temperature screening device (*RightFace, RightTime*) that simply requires a worker to briefly stand in front of a camera. The device takes the worker's temperature and scans their face so that a record of their temperature is created. WidgetCo. is impressed by how efficient this is.

Should WidgetCo. go ahead and buy *RightFace, RightTime*?

2. Customers returning to premises

- COVID C/U/D: Is it reasonable? Is it required?

  See guidance from AB OIPC *Pandemic FAQ on customer lists* (https://www.oipc.ab.ca/resources/pandemic-faq-customer-lists.aspx)

  See BC order re: retention of customer information (https://www2.gov.bc.ca/assets/gov/health/about-bc-s-health-care-system/office-of-the-provincial-health-officer/covid-19/covid-19-pho-order-nightclubs-food-drink.pdf) and guidance from the BC OIPC *Collecting personal information at food and drink establishments during COVID-19* (https://www.oipc.bc.ca/guidance-documents/2421)

- Where practical, organizations should notify customers of COVID-19-related collection of PI (in relation to a screening program, customer lists, etc.) using clear, visible signage (preferably infographics).

Customers returning to premises

- Where practical, organizations should notify customers of COVID-19-related collection of PI (in relation to a screening program, customer lists, etc.) using clear, visible signage (preferably infographics)

- Organizations should apply data minimization principles to customer screening activities
  - **Example:** if a questionnaire must be completed, the questions should be limited to current health guidance and other non-medical screening factors

Customers returning to work premises

- Ideally, use a third party screener instead of an employee. If not practical, what steps can you take to minimize intrusiveness?
  - requiring an **NDA/confidentiality** agreement specific to this engagement
  - **training** the employee
  - **private screening** area
  - ensuring the employee is **not screening his/her direct or skip level reports** (ideally, the screener would be from a wholly different business unit).

Customers returning to work premises

- Organizations should avoid scenarios where individuals are forced to consent to collection of (potentially sensitive) PI in order to access the premises
  - **Example:** an organization that implements temperature screening as a condition of entry to premises should consider making available alternatives for those who refuse. Curbside pickup, online orders, etc. are viable alternatives.

- Organizations should avoid recording (collecting) PI in the course of screening activities
  - Least risk approach

3. Payments

- Organizations are now accepting payments using credit cards in potentially insecure ways (e.g. accepting payments over the phone for curbside pickup) should implement procedures addressing the collection and recording of credit card information

- If online payments are a new thing, you may need to update your privacy policy to reflect this

- Payment card information is sensitive personal information – do you existing security safeguards measure up?

Payments

- PCI-DSS (Payment Card Industry Data Security Standard)
  - Ensure **you** continue to be PCI-DSS compliant
    - See: PCI-DSS, *Protecting Payments While Working Remotely* (https://blog.pcisecuritystandards.org/protecting-payments-while-working-remotely)
    - See: PCI-DSS, *Protecting Telephone-Based Payment Card Data* (https://www.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf?agreement=true&time=1584466730777)
  - Ensure **your providers** continue to be PCI-DSS compliant

大成 DENTONS

4. Managing information security risk

File and device management

大成 DENTONS

Don’t forget about the basics

- **Physical files**
  - If physical files containing PI were left behind in workplace, are they secure? What about computers?
  - Minimize paper in the home environment; avoid transport back and forth
  - Secure disposal at home, not just out with the garbage/recycling

- **Electronic devices**
  - Password protect, encrypt
  - Avoid viewing personal information collected and used for work in public
  - Avoid use of personal email
  - Always securely store devices

Telecommunications / videoconferencing

Introducing a new platform

- **Assess risk:** Conduct privacy-impact and IT security assessments before introducing new technology.

- **Evaluate service agreements:** What are the service provider's information handling practices?
  - While many service agreements will be non-negotiable, assessing the service provider enables you to:
    - Decided whether the service fits your risk profile;
    - Scope out internal standards and procedures; and
    - Account for the service provider's practices in your privacy notice.

Telecommunications / videoconferencing

Introducing a new platform

- **Incorporate standards into your policies addressing:**
  - **Scope of discussions**: What types of meetings (e.g. internal, external, confidential etc.) will take place on the platform?
  - **Recording meetings**: Will recording of videoconferencing be implemented - and under what circumstances? Where are recordings stored?
  - **Notice:** How will external meeting participants be made aware of the service provider's information-handling practices?
  - **Authentication**: How will you identify meeting participants? (e.g. 'waiting-room' and user identification features).

Telecommunications / videoconferencing

Further guidance on videoconferencing:

- Office of the Privacy Commissioner, *Privacy tips for videoconferencing services. (*May 1, 2020)
- Canadian Centre for Cybersecurity, *Alert: Considerations when using video-teleconference products and services* (April 3, 2020)
- UK National Cyber Security Centre, *Video conferencing services: using them securely* (April 21, 2020)
- Australian Cyber Security Centre, *Web Conferencing Security*, (April 2020)

大成 DENTONS

5. Incident response plans

Incident response plans

大成 DENTONS

Breach reporting: an update

- The privacy commissioners may be experiencing delays in responding to requests (Office of the Privacy Commissioner of Canada, March 20 Announcement).
  - Organizations are **still obligated to comply with breach reporting requirements**.
- **Timing**: In the event that you suffer a privacy breach – you are still obligated to report and/or notify within the statutory timeframe (provided you meet the threshold for reporting / notification)
  - PIPEDA: "as soon as feasible" (Section 10.1(2)).
  - Alberta's *Personal Information Protection Act*: "without unreasonable delay" (Section 34.1)

Incident response plans

Breach reporting: an update

- **Real risk of significant harm** (“**RROSH**”) remains the threshold for reporting:
  - Be judicious in the application of the RROSH test.

- **Recordkeeping obligations continue**: Can you comply remotely?

Incident response plans

大成 DENTONS

Your incident response plan

- **Changing employment conditions:** Can you execute your incident response plan in the context of:
  - Work-from-home?
  - Employee layoffs, furloughs or leaves? (i.e. are individuals crucial to your incident response plan available?)
- **Scope of your plan**
  - Provide guidance for scenarios involving the loss or theft of company devices or physical files in the possession or remote workers
  - Clarify internal reporting procedures for when an employee discovers a breach while working remotely

Incident response plans

大成 DENTONS

Your incident response plan

- **Training**
  - Ransomware attacks are **on the rise** in the time of COVID-19
    - **Ransomware is especially problematic in the remote working/online sales environment: everything will be shut down**
  - Ensure that employees are equipped to deal with evolving threats – for example phishing tactics.

大成 DENTONS

6. Privacy policies

Privacy notices

Currency of privacy notices

- **PIPEDA Principle 8**: Individuals must be able to acquire information about an organization's information handling practices "without unreasonable effort".
- If your privacy program has been changed due to COVID-19, any such changes **must be reflected in your privacy notice.**

- **New source of jeopardy: Canada's Competition Bureau**
- On May 19, 2020, the Bureau announced it had signed a consent agreement settling a false or misleading claim about the extent to which users of a digital platform could control access to their personal information.
- The agreement related to the platform's privacy statements, and provided for a fine of **$9 000 000** in addition to the Bureau's costs.
- **This development materially changes the risk environment for organizations.**

Questions?

Kirsten Thompson
Partner, Toronto
D+1 416 863 4362
kirsten.thompson@dentons.com

Luca Lucarini
Associate, Toronto
D+1 416 863 4735
luca.lucarini@dentons.com

Thank you