大成 DENTONS

# 2nd annual Dentons Data Summit:

## The return to work and employer collection of personal information

June 10, 2020

dentons.com

# Meet our presenters

Eleni Kassaris
Partner, Vancouver
D+1 604 629 4982
E eleni.kassaris@dentons.com

Chloe A. Snider
Partner, Toronto
D+1 416 863 4674
E chloe.snider@dentons.com

Kelly Osaka
Partner, Calgary
D+1 403 268 3017
E kelly.osaka@dentons.com

Chelsea Rasmussen
Senior Associate, Toronto
D+1 416 862 3464
E chelsea.rasmussen@dentons.com

# Health and safety measures on return to work

- General duty to take all precautions reasonable in circumstances under OHS legislation across Canada
- Public health guidance likely considered a “reasonable precaution”
- But: Safety precautions must be balanced against privacy interests

# What are employers implementing on return to work?

- Active screening (questionnaires)
  - Currently recommended by public health authorities
  - Public health guidance may create a reasonable purpose for collection, but the information collected must itself be reasonable
  - Screening questions should be based on current health guidance
- Temperature and thermal screening
  - Blanket health-related testing is generally not permissible
  - It is more acceptable to test individuals on a case-by-case basis where an organization has reasonable cause to require a particular person to have their temperature checked
  - However, in the exceptional circumstances of COVID-19, it is likely that an organization's occupational health and safety obligations may justify temperature screening

# What are employers doing? (cont'd)

- Contact tracing
  - Organizations should not promote or recommend a contact tracing app without understanding how it incorporates privacy principles
  - Organizations should inform individuals about how their information may be used and of the privacy risks associated with the use of contact tracing apps
  - Organizations which are using a third-party contact tracing app should have detailed and specific agreements in place that include provisions in respect of data sharing, data use, and data security
- Consider "old school", easier to implement solutions: Logbook

# Privacy related regulatory and litigation risks

- **Security safeguard** obligations are higher for **sensitive personal information**
  - Limit the individuals who have access to the information;
  - Ensure that all electronic and physical storage is protected.

- **Regulatory risk**:
  - Any individual (employee, customer, activist) can make a compliant to the Privacy Commissioner against a business – they do not have to be affected by the conduct to complain
  - Mandatory breach reporting of any breaches of security safeguards involving personal information that pose a real risk of significant harm

- **Litigation risk**:
  - Increased risk from data breaches and employee privacy incidents
  - Risk of higher damages because of heightened sensitivity of personal information

# Guiding principles for collecting personal information of employees

- Before implementing any new COVID related policies involving the collection, use, or disclosure of personal information an employer should consider:
  - **Necessity**: there must be a clearly defined purpose for the use of the measure that is necessary for the employer to fulfill its obligations;
  - **Proportionality**: the measure should be targeted so as to be reasonably proportionate to the privacy of the individual employee;
  - **Effectiveness**: the measure should be shown empirically to be effective at addressing the issue; and
  - **Minimal Intrusiveness**: the measure should be the least invasive alternative available

- This means:
  - **do not** engage in over collection of personal information; and
  - **do not** use the personal information for secondary purposes.

# Ways to mitigate risk from a privacy incident

- **Privacy impact assessment**
  - When onboarding a new process or technology engage in a systematic evaluation of the proposed initiative
  - Analyze the risks to privacy and how to manage those risks
- **Update privacy policies and training**
  - Provides notification to employees of new policies for return-to-work
  - Demonstrates due diligence
- **Update incidence response plan**
  - Increases incident response time and enhances effectiveness of response
  - Ensures that the plan is up-to-date when office may be inaccessible and employees are working remotely
  - Reduces regulatory and litigation risks

# Implementing screening: what should an employer consider?

- Provide notice or, where necessary, get consent
- Give information about why you are collecting information and how it will be used
- Assure employees that their information will be protected (and protect it)
- Collect the information discreetly and respectfully, respond to the information respectfully
- Only share the information with necessary personnel
- Consider if there are less intrusive ways to collect the necessary information (logbooks?)
- Do not keep information indefinitely

# Can an employer disclose an employee's positive diagnosis for COVID-19?

- A positive diagnosis in the workplace may, depending on provincial legislation and orders, trigger reporting requirements to:
  - Labour / workplace safety boards,
  - Workers' compensation boards,
  - Public health bodies,
  - Workplace health and safety member(s), and/or
  - Union (if applicable).
- Objective of disclosure is limited to providing potentially exposed employees with sufficient information to protect themselves from the risk.
  - Where possible, avoid disclosing information that might (alone or together with publicly available information) identify the specific individual(s) who may have caused the potential workplace exposure risk.

# What about monitoring employees at home?

- Work at home is an extension of the workplace – if you are not monitoring people in the main workplace, you should not implement new forms of monitoring at home
- If evaluate new forms of monitoring for work at home then:
  - Notify employees about the program and what information is collected
  - Avoid continuous, real-time collection of personal information, such as keystroke logging or screen capturing
  - Avoid collecting more information than necessary.
  - Implement training and policies for the employees who will manage tracking tools
  - Log access to the system and periodically review to ensure proper use
  - Periodically evaluate the effectiveness of the program, including whether there is a less intrusive way of addressing the issues

# Ways to mitigate risk with return-to-work

- **Protecting confidential information at home**
  - Employees working remotely or transitioning back to the office should be reminded to:
  1. Print as few documents as necessary (or none) when working from home;
  2. Do not put any documents with confidential information into the garbage
  - Follow best practices when engaging in online video conferencing to protect confidential information

- **Protecting electronic devices**
  - Laptops should be password-controlled and any data stored on a hard drive should be encrypted
  - Employees should be encouraged not to view confidential information on laptops or cell phone while in public

# Questions?

Eleni Kassaris
Partner, Vancouver
D+1 604 629 4982
E eleni.kassaris@dentons.com

Kelly Osaka
Partner, Calgary
D+1 403 268 3017
E kelly.osaka@dentons.com

Chloe A. Snider
Partner, Toronto
D+1 416 863 4674
E chloe.snider@dentons.com

Chelsea Rasmussen
Senior Associate, Toronto
D+1 416 862 3464
E chelsea.rasmussen@dentons.com

# Thank you