大成 DENTONS

Dentons Data COVID-19

Restarting Your Business - Privacy and Data Toolkit

NOTE: Dentons Data: Restarting Your Business - Privacy and Data Toolkit has been developed to assist our Canadian clients with some of the data-related issues they may face as provinces and businesses begin to open up during the COVID-19 pandemic. Please note that the information provided in this Toolkit does not constitute legal or professional advice or a legal opinion. Each business will need to create its own plans having regard to the nature of its business, the jurisdiction in which it operates, and the information, orders and guidance provided by government and public health authorities. This Toolkit will provide businesses with some of the background information on privacy obligations to help rebound, restart and move forward. If you have any questions, please reach out to one of the members of the Dentons' Transformative Technology and Data Strategy group.

Contents

Introduction

As we have repeatedly been told, these are extraordinary times and many Canadian legal regimes are adapting to this crisis on the fly. Privacy laws are no different. The Office of the Privacy Commissioner of Canada (OPC) has recognized that the pandemic calls for a flexible and contextual application of privacy laws and that measures that would otherwise not be reasonable in ordinary circumstances may be justified under the current circumstances.

Businesses and other organizations will soon face new considerations as we proceed through various return-to-work stages, which will be in place for an unknown period of time. This Dentons Data: COVID-19 Restarting Your Business Privacy and Data Toolkit addresses many of the privacy and data issues that organizations will face in the coming year as lockdown restrictions fluctuate, ease, and possibly restrict again as necessary in order to prevent the spread of the virus.

We have developed this toolkit as a companion to our **Labour & Employment Return to Work Toolkits** to help organizations navigate the "flexible and contextual" privacy requirements as they return to operations.

To do so, this toolkit will cover the following topics:

Entry to premises – screening

a. General considerations

b. Active screening (questionnaires)

c. Temperature and thermal screening

d. Biometric identifiers

e. Contact tracing apps

f. Vendors and others

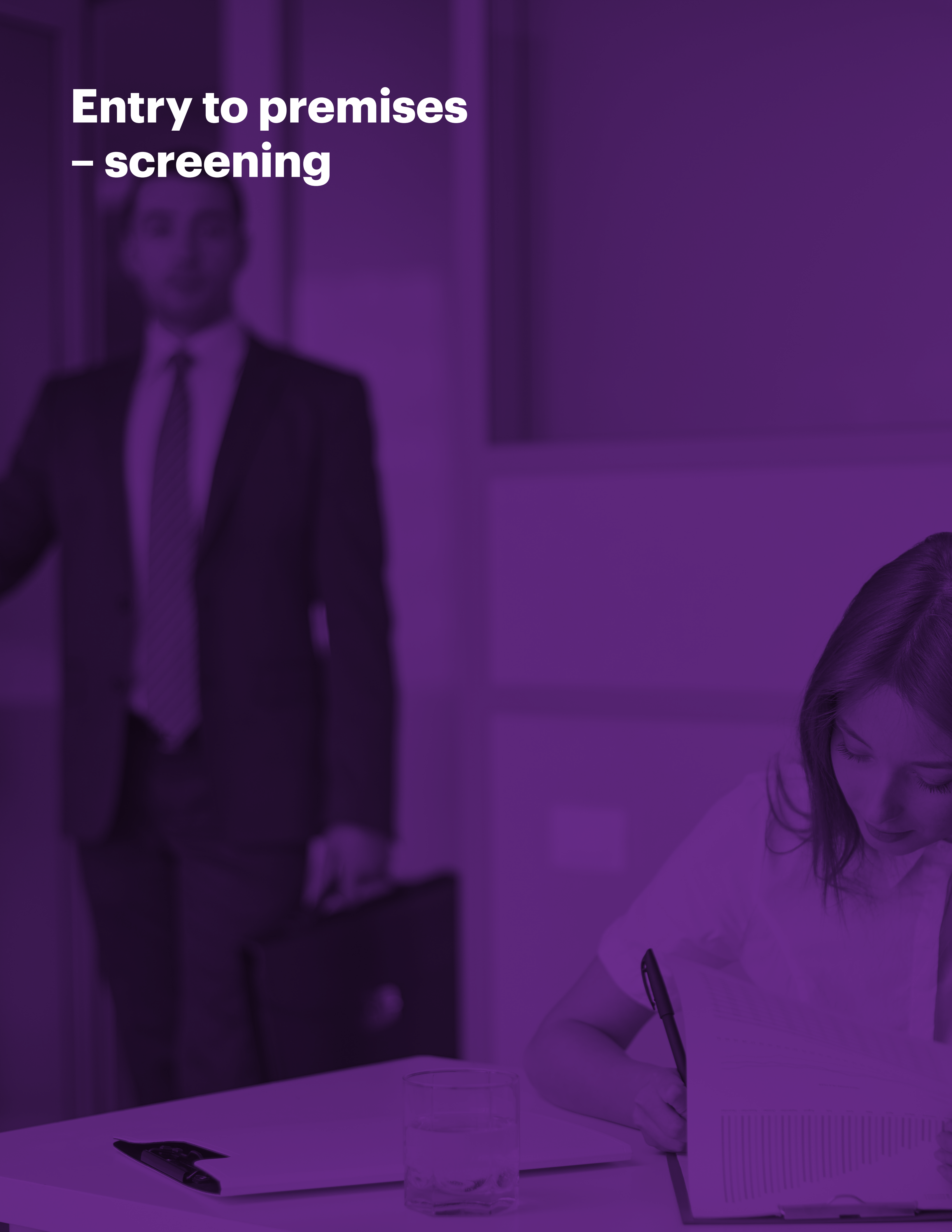
Disclosure of employee (and others) COVID+ status

Mobility of employees, customers and vendors

Online video conferencing platforms

Employee monitoring

Entry to premises – screening



Organizations may consider implementing screening, including questionnaires, temperature screening and biometric identifiers, as a way to identify and prevent potentially infected individuals from entering their premises. The purpose of such screening is typically to inhibit the spread of COVID-19 or to identify individuals who have been in the premises in order to assist with contact tracing for epidemiological purposes or to identify others who may have been infected (or both).

COVID-19 screening necessarily involves the collection, use and disclosure of some amount of personal information and therefore engages individuals' rights under Canadian privacy laws. Regardless of the specific form of the screening, certain privacy obligations will apply.

Organizations are legally responsible for ensuring that their premises are safe. Safety considerations, however, do not create a blanket override of individual protections under Canadian privacy laws. There is a balance to be struck between safety and privacy. Any safety precautions that involve the collection, use and/or disclosure of personal information must be reasonably justifiable in the circumstances and must be undertaken with consent (or fall into one of the very narrow exceptions to consent).

The majority of workplace and business safety requirements specifically relating to COVID-19 are derived from guidelines and recommendations from public health bodies in various Canadian provinces. As such, they may not themselves have legal force, but may nonetheless constitute "reasonable precautions". As such, these types of guidelines and recommendations serve to create a benchmark. An unexcused failure to implement these types of guidelines and recommendations can create risk for an organization, and for its employees, customers and clients.

When developing policies, procedures, training and communication materials regarding screening processes, organizations should use current, correct messaging from a trusted source. Staying current may prove challenging – the information may change weekly, or even daily, and organizations will need to be diligent, and adjusting their practices accordingly. It is best to follow guidance from federal, provincial and local government agencies with respect to privacy, public health and occupational health and safety. Any screening program should be reinforced by the use of signage (preferably infographics) placed in strategic locations in the premises, wherever possible.

In addition to privacy and data issues, note that there may be issues under human rights, employment or occupational health and safety legislation to be taken into account when undertaking various types of screening or collecting health information. For further information about these issues, please see our Employment & Labour Return to Work Toolkits or contact a member of the Dentons' Employment & Labour group.

A. General considerations

Two key considerations for meeting privacy obligations when implementing a screening program are privacy impact assessments (PIAs) and information governance practices. PIAs help organizations formulate effective and compliant initiatives before personal information is collected and information governance practices help organizations comply with privacy obligations once personal information is in their hands.

(i) Privacy impact assessments

Before undertaking any screening measures involving the collection, use and disclosure of personal information, it is prudent (and may be required for some public sector organizations) to conduct an appropriate PIA. A PIA is a systematic evaluation of a proposed initiative, technology or information handling practice that identifies and analyzes the relevant risks to privacy and forms the basis for how these risks should be managed, including what measures should be implemented to mitigate the risk to an acceptable level.

The scope and content of a PIA will vary depending on the nature of an organization's operations, but a PIA should review the intention, rationale and efficacy of the proposed initiative, identify risks and risk tolerance, identify the purpose to prevent the expansion of uses of personal information beyond the intended purpose, create (or confirm) policies, identify roles within the organization that are responsible for handling personal information, and establish a retention schedule and process for the information being collected.

(ii) Information governance

The first step of proper information governance is controlling what information enters an organization's hands. Screening should collect only the personal information that is reasonably necessary to accomplish its purpose. Collecting more personal information than you reasonably need for the stated purpose is not only a violation of Canadian privacy laws, it can materially increase the risk to an organization that a breach will occur and - should a breach occur – may increase the chance of litigation and amount of damages.

Once personal information has been collected, it should only be kept for as long as it serves its purpose or is required to be kept by law. After that, it should be securely destroyed. In order to document its practices or compliance, an organization may create meta-records; for instance, records that document that individuals were screened, but that no positive results arose.

Organizations are required by Canadian privacy laws to implement appropriate measures to protect personal information under their control, be they physical (e.g., locked storage), technical (e.g., password-protected databases) or administrative (e.g., privacy practices or confidentiality agreements). What is appropriate depends on the nature and form of the personal information. The more personal information an organization holds and the longer it holds it, the greater the risk of a breach (and the possible damages should one occur).

Organizations should have documented information governance policies, including how long certain types of information will be kept. An organization's existing privacy policies will likely be the best place to start as employees will be familiar with existing general privacy practices. The policies should include provisions for secure destruction (or robust anonymization, if appropriate) of the personal information.
Such policies should also allow for exceptions (such as litigation holds).

B. Active screening (questionnaires)

Current public health guidelines indicate that organizations should screen all individuals prior to entering the premises (including employees, contractors, visitors, etc.) for COVID-19 by collecting information through questions. This guidance may create the reasonable purpose for collecting personal information, but the information collected must itself be reasonable and screening must otherwise comply with Canadian privacy laws.

Screening questions should be based on current health guidance (in other words, the known symptoms at the time), and other, non-medical screening factors (such as, to the best of their knowledge, they have not been in contact with someone with a confirmed or probable case of COVID-19), updated as necessary.

It remains to be seen whether public health officials, or provincial ministries of labour, will recommend that organizations continue active screening even after the government relaxes the current restrictions that are in place. In any event, organizations which serve vulnerable populations (for example, hospitals and long-term care homes) should strongly consider maintaining screening until the threat of COVID-19 has subsided.

Since the purpose of this type of screening is generally simply a gating mechanism to enter the premises, there is generally no need to collect any information (e.g., no need to identify the individual, no need to record or retain the information). Organizations that require ID (e.g., bars) should be careful to separate the identification step from the initial COVID screening step.

C. Temperature and thermal screening

Temperature screening involves screening an individual to take their temperature and. depending on the mechanism used, can be disruptive and potentially invasive. Thermal screening, an aggregate screening technique that displays colour-coded thermal images of people to identify those with elevated temperature, can also be used. It is less invasive and less disruptive than temperature screening. In either case, however, there is a collection of an individual's health information, which is generally considered sensitive personal information.

Medical examinations or health-related tests like temperature testing are generally acceptable only if the testing or examination is reasonably necessary for a reasonable and legitimate purpose and is undertaken with consent. In normal circumstances, it is generally not permissible to require blanket health-related testing such as temperature screening as that would constitute an unnecessarily invasive action. It would be 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 (i.e. a reasonable belief that a particular person is symptomatic).

However, in the exceptional circumstances of COVID-19, it is likely that an organization's obligations under applicable occupational health and safety legislation to take all reasonable precautions for the protection of the health and safety of its employees or others on the premises may justify temperature screening in these circumstances – particularly where the organization serves a vulnerable population. Essential businesses that are required to remain open by government order despite increased risk may also be justified in implementing more rigorous screening.

As the economy reopens, and non-essential businesses and organizations begin to open, they may think about introducing temperature or thermal screening as a condition of entry for customers. In the circumstances of COVID-19, this may be reasonable; however, organizations thinking of adopting this approach should have clear signage indicating that temperatures will be taken (so people can elect not enter the premises). Alternate means of delivery of goods or services should also be considered (for instance, those not wishing to have their temperature taken and are therefore barred from entry, can still access the good or service online or via curbside delivery).

As a result, as a best practice, organizations that conduct temperature or thermal screening during COVID-19 should conduct such screening in conjunction with other active screening measures as set out above, and where possible should be conducted by a third party or individual with appropriate training and personal protective equipment. Ideally, the location of any temperature screening will be curtained off or separated, so those who have elevated temperatures will not be open to view by others awaiting entry.

Bear in mind that an individual's temperature may be elevated for a reason related to a different, non-communicable medical condition that does not pose an unreasonable risk to health and safety on the premises. In other words, a person with an elevated temperature should not be told they may have COVID-19, but rather that the screening guidelines prohibit entry to anyone with a temperature above X degrees.

Once again, since the purpose of temperature or thermal screening is simply a gating mechanism to entry, there is likely no need to record identifying information. Records may be kept in aggregate (the number of individuals screened, the number of persons refused entry, etc.).

Once the COVID-19 pandemic is over and business operations have resumed, it will likely be difficult to justify the invasive action of temperature screening in most organizations, again with the exception of long-term care homes and other workplaces that serve vulnerable populations.

D. Biometric identifiers

Biometric identifiers, such as fingerprints, retinal scans or facial recognition can be effective tools for identifying individuals present in an organization's premises, but similar to temperature screening, biometric information is sensitive personal information. Organizations will almost always require express consent of the individual to collect such information.

Before considering the use of biometrics (such as automated facial recognition technology, retina scans, fingerprints, hand scans), organizations should consider whether they are necessary, effective, and proportional to the potential privacy risks, and whether there is a less privacy invasive way to identify or authenticate an individual.

Because biometric information is also generally immutable, organizations collecting such information will not only need a strong rationale for collecting it, they will also need robust security to protect it, and rigorous information governance on the storage, retention and destruction of such information.

Organizations that have rapidly implemented online payments in response to COVID-19 should revisit their data handling processes, particularly if the payment process uses biometric identifiers for authentication.

E. Contact tracing apps

Contact tracing is the process of identifying individuals who have been in contact with someone who has been diagnosed with COVID-19, notifying those individuals that they may be at risk, and identifying who they have been in contact with to contain the spread of the virus.

Generally, contact tracing apps make use of mobile devices' Bluetooth capabilities to log the devices that have been in close proximity through the exchange of personal identification numbers. This information is resident on the device and nothing is done with it until the user tests positive. When a user of the app tests positive, they can upload their log of personal identification numbers to a public health service to be used for contact tracing and automatic notification. In short, information about nearby devices that would ordinarily be detected through Bluetooth, but not retained, would now be retained for the purpose of contact tracing.

Governments around the globe, including Canada, are working to implement contact tracing apps, but there are also a number of apps designed for use in the private sector. The federal, provincial and territorial privacy commissioners jointly issued principles for the use of contact tracing apps for governments, which are not binding on private sector organizations, but provide a useful framework for implementing or selecting contact tracing apps for use in the private sector:

- Consent: The use of apps must be voluntary. There must be reasonable and articulated purposes for the tracing program and consent must be meaningful (i.e., informed) for all purposes.
- Necessity and proportionality: The use of contact tracing apps must be science-based, necessary for a specific purpose, tailored to that purpose and likely to be effective.
- Purpose limitation: Personal information must be used for its intended purpose (i.e., preventing disease transmission) and for no other purpose.
- De-identification: De-identified or aggregate data should be used whenever possible, unless it will not achieve the defined purpose.
- Time-limitation: Any personal information collected during the pandemic should be destroyed when the crisis ends.
- Transparency: Individuals should be fully informed about the information to be collected, how it will be used, who will have access to it, where it will be stored, how it will be securely retained and when it will be destroyed.
- Accountability: Organizations should monitoring and evaluate the effectiveness of contact tracing.
- Safeguards: Appropriate legal and technical security safeguards, including strong contractual measures with developers, must be put in place to ensure the security of the data.

Organizations should not promote or recommend a particular contact tracing app without investigating and understanding how it incorporates the above principles. Organizations that require individuals to download and use a contact tracing app before entering the premises should inform individuals about how their information may be used and of the privacy risks associated with the use of contact tracing apps. If such a program is implemented, measures should be taken to document compliance, if not expressly, then through adequate communication and training.

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.

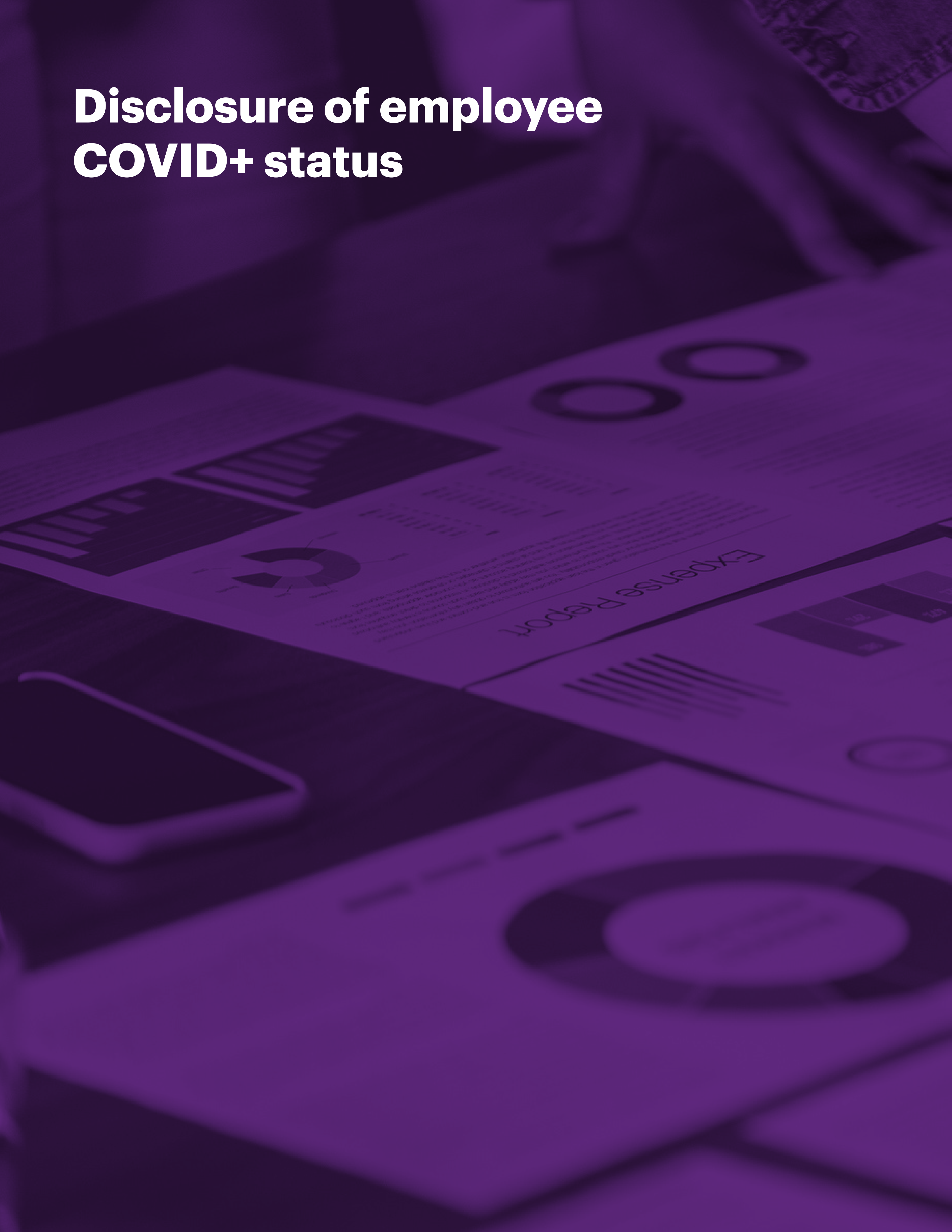
As with temperature screening, organizations that choose to make the use of a contact tracing app a condition of entry should ensure that those who do not wish to download or use the app have an alternate means to access the goods or services (e.g,. online, or curbside pickup).

F. Vendors and others

While the above has mostly focused on employees and customers, with the opening up of businesses and other organizations, the supply chain also opens up – which means organizations will have vendors and other suppliers entering their environment, and leaving to go to another organization's environment. These multiple contacts make vendors and other similar supplies a potential vector for infection. Organizations should consider how they will address these concerns with respect to such itinerant populations. Many of the above concerns apply equally to these relationships, and businesses should develop a plan for managing and screening vendors and others.

> **"The ethics of public health information, data protection, and data privacy must be considered at all levels of contact tracing activities, in all training activities for contact tracing, and when implementing contact tracing tools."**
>
> *World Health Organization, Contact tracing in the context of COVID-19*

Disclosure of employee COVID+ status



As part of meeting their legal obligation to provide a safe workplace, organizations should instruct employees not report to work if they are ill and they should not be allowed in the workplace if they are known to be ill. However, privacy issues naturally arise when an organization requires an employee to disclose information about their medical diagnosis or health status.

Responding to a confirmed COVID-19 diagnosis will require contact tracing to limit the workplace hazard and may trigger reporting requirements under provincial occupational health and safety legislation or public health guidelines. Organizations are also required to consult with workplace health and safety committees on workplace safety matters.

Canadian privacy laws contain exceptions that allow organizations to disclose personal information if necessary to respond to an emergency, but disclosing the name of an infected or possibly infected employee is not necessary to achieve health and safety objectives in response to a positive test. Organizations should designate an individual outside of employees' direct reporting chain to receive positive test reports and measures should be implemented to protect the infected individual's identity. Disclosure of the positive test (or presumptive positive status) should be made to other employees or customers on a non-identifiable basis only (e.g., "an employee in our Hamilton store tested positive on X date"). Sufficient information that allows people (or work colleagues) to work backwards to identify someone will be identifying information. For instance, telling colleagues that "someone on the production floor tested positive and their last day of work was X date" may provide enough information that colleagues will be able to determine who it is, particularly if there are only two or three employees to choose from.

Note that in ordinary circumstances, it is not advisable for employers to seek diagnostic information as it is not necessary for the employer to assess whether the employee is fit for work, and it will be difficult to support requiring disclosure of medical diagnostic information after the pandemic.

As always, the health status of an employee, vendor employee or other person with whom an organization has come into contact should be treated as sensitive personal information and not shared without a clear statutory basis for doing so. Such information will also need to be carefully protected (e.g., encrypted) to prevent accidental loss or disclosure, or employees who "snoop" through workplace systems.

Organizations should also carefully consider how long they should keep this information.

> **"Responding to a confirmed COVID-19 diagnosis will require contact tracing to limit the workplace hazard and may trigger reporting requirements under provincial occupational health and safety legislation or public health guidelines.**

Mobility of employees

As governments begin to lift lockdown restrictions and employees return to work, employees may need to transport their employer's records to and from their employer's office space. Fluid working arrangements whether at the office or at home create the opportunity for privacy breaches. The purpose of this section is to set out how employees should protect the privacy and confidentiality of their employer when working outside the office.

Removing paper records from the office

Employees should only remove records containing personal information from the office when it is absolutely necessary for the purposes of carrying out their job duties. If possible, only copies should be removed with the original left in the office. Of course, where possible, employees should try to work from electronic records and leave all physical copies in the office.

Paper records containing personal information should be securely packaged in folders, carried in a locked briefcase or sealed box and kept under the constant control of the employee while in transit. When an employee travels by car, paper records should always be locked in the trunk. If possible, paper records should never be left unattended in a car trunk while the employee goes elsewhere. When an employee travels by public transportation, they should never open or review paper records or electronic files.

If records containing personal information or other confidential information are being left behind in an office, they should be locked away, and other security measures should be taken. With fewer employees in the workplace, offices are becoming targets of thieves, some of whom are simply stealing valuables, but others of whom are seeking to steal identity information.

Protecting confidential information at home

Dumpster diving is a method used by malicious actors to gather data by going through the garbage. It does not require the use of technology as paper files are of great value, too. Information obtained through dumpster diving can also be used to design sophisticated social engineering emails that appear to be coming from your client or a member of your team working on the same matter.

While the exact scope of disposal regulations may vary to some degree, the critical practices to implement in a home office are twofold: 1) print as few documents as necessary and 2) do not put ANY documents with confidential client or personal information into the trash. An employee can use a home shredder if they are sure that they can meet applicable security standards for home shredding based on the type of data in their printed documents. Otherwise, they should find a secure place to store these printed materials until they can safely bring them back to the office or otherwise properly dispose of them.

While it may seem unnecessary, a clean desk ensures the confidentiality of client and personal data. It is worthwhile noting that family members are third-party strangers to a business' clients, and the "clean desk" practice can prevent accidental disclosures.

Designating an area in the home (and/or using headphones) so that an employee can make work related phone or conference calls helps to assure that no one accidentally overhears a confidential conversation. A designated area will also assist in protecting the client and organizational data as a whole.

And remember, the easiest step an employee can take towards responsible document management may be to give up with the old habit of printing every document for review. Finally, an added consideration for some organizations may be in respect of any trade secrets they have. Generally, trade secrets (a form of confidential information) are protectable only where reasonable measures are taken to protect confidentiality, and therefore taking these steps to protect confidential information at home is important.

Electronic devices

Access to laptop and home computers should be password-controlled, and any data on the hard drive should be encrypted. Other reasonable safeguards, such as anti-virus software and personal firewalls, should also be installed. Employees should only use software that has been approved by their organization.

Laptops should be kept under the constant control of the employee while in transit. If it is necessary to view confidential information on a laptop screen when working at locations outside the office, ensure that the screen cannot be seen by anyone else. Confidential information should never be viewed on a laptop screen while travelling on public transportation.

When working at home, a laptop or home computer should be logged off and shut down when not in use. For added protection, they should be locked to a table or other stationary object with a security cable. Laptops used for work purposes should not be shared, including with other family members or friends.

Similar principles apply to wireless devices such as cell phones. Access to such devices should be password-controlled and any stored data should be encrypted. To prevent loss or theft, a wireless device should be carried in a locked briefcase or closed purse and kept under the constant control of the employee while in transit. If it is absolutely necessary to view confidential information on a wireless device while in public or when travelling on public transportation, ensure that the display panel cannot be seen by anyone else.

Many organizations have had to implement mobile payments or online payments processes rapidly. To protect themselves, and their customers, organizations should take this opportunity to review their payment handling processes. For instance, for curbside pickup, are customers handing their cards to your employees? What security measures do you have in place to prevent card swaps or other misuse of card information? Are employees handing the point-of-sale terminal to customers? If so, are you keeping an eye out for them being swapped for lookalike terminals used to steal payment card information?

Reporting requirements

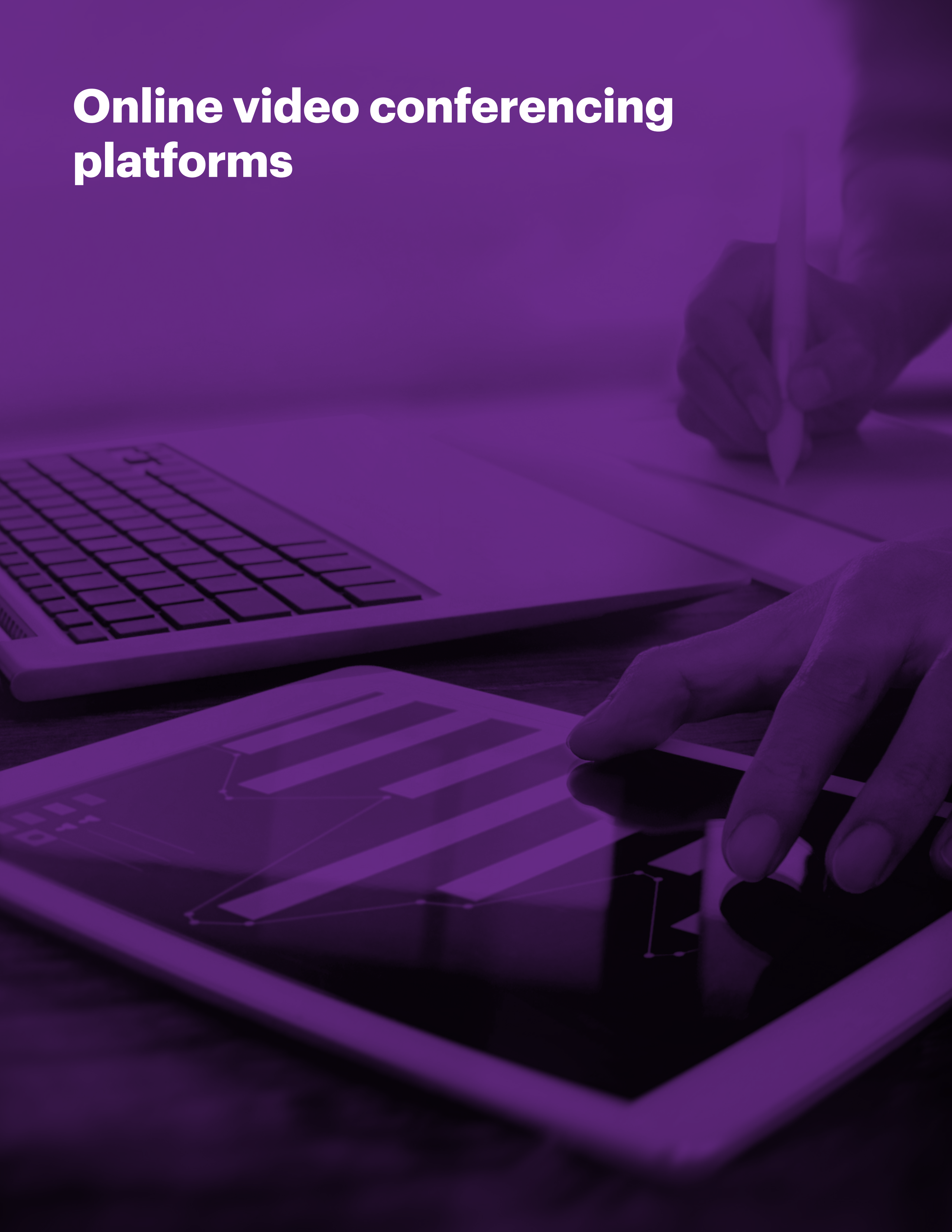
The loss or theft of personal information or a personal device containing confidential employer information should be reported immediately to an employee's manager. The employer along with their legal counsel will make an assessment on whether any notification is necessary to impacted parties and/or to regulators.

The loss, unauthorized access, or theft of customer personal information may trigger breach reporting and notification requirements. Organizations already dealing with the COVID-19 crisis do not need to be managing a data crisis on top of it; a review of privacy practices, employee refresher training are all a good idea.

Organizations should also be reviewing their incident response plans and updating them to reflect:
(a) the working-from-home environment (your plan likely contemplated everyone being in the office or workplace) and (b) any employee changes due to layoffs, furloughs, or COVID-related leaves.

“Organizations should also be reviewing their incident response plans and updating them to reflect: (a) the working-from-home environment (your plan likely contemplated everyone being in the office or workplace) and (b) any employee changes due to layoffs, furloughs, or COVID-related leaves.”

Online video conferencing platforms



As organizations adjust to working remotely and shifting their operation into the digital realm, many have turned to online video conferencing platforms for virtual meetings with colleagues and clients. There are many online video conferencing platforms including Zoom, Google Hangouts, Skype, Slack, Cisco Webex, BlueJeans and Microsoft Teams, among others. Below is a summary of the major privacy implications arising from the use of these online video conferencing platforms as well as some advice concerning best practices for their use.

Personal data

Many online video conferencing platforms collect a considerable amount of personal data including, but not limited to:

- Information commonly used to identify an individual, such as their name, user name, physical address, email address, phone numbers and other identifies.
- Information about an employee's job, such as their title and employer.
- Credit/debit card or other payment information.
- Social media profile information (when an individual uses a social media platform to log in).
- Information about an individual's device, network, and internet connection, such as their IP address(es), MAC address, other device ID such as Unique Device Identifier (UDID), device type, operating system type and version and client version, etc.
- Information about an individual's usage of the online video conferencing platform.
- Other information uploaded, provided or created while using the online video conferencing platform.

Given the amount of personal data that may be collected by an online video conferencing platform, it is important for businesses and individuals to review and understand their platform's privacy policies and terms of use. In particular, businesses and individuals should review and understand how the online video conferencing platform may collect, use, store and disclose personal data from those who set up accounts or simply use their platform. Businesses should ensure their chosen online video conferencing platform's privacy policies and terms of use align with internal policies and outside obligations with respect to privacy and data handling. In certain situations, businesses may need to amend their internal policies to permit the use of online video conferencing platforms.

Organizations that are now providing their services online via such platform should consider updating their privacy policies to reflect this new development, and the likely new uses of personal information.

Recordings

Many online video conferencing platforms allow a host to record a video conference call and to save the recording to the platform's server or their own personal device. Participants on a call are notified when a host decides to record and, if a participant does not want to be recorded, are provided with an option to ask the host to stop recording or leave the call. If a host chooses to save a recording to their online video conferencing platforms' server, the host should first ensure that the platform's privacy policies and terms of use align with its internal policies and outside obligations with respect to privacy and data handling. Most online video conferencing platforms will assign a recording a default file name that a stranger can easily predict and then search for. Hosts should therefore consider renaming all recording to decrease this risk. If a host chooses to save the recording locally, they will want to ensure that where they choose to store that data meets the requirements of their organization's privacy policy.

Risk of infiltration

Recent media reports have noted vulnerabilities related to third-party infiltration or hijacking of online video conferencing platforms, sometimes referred to as "Zoom-bombing". Such infiltration is possible when meetings are configured without password protection or a "waiting room" mechanism by which participants would be positively identified and granted entry. This situation can be exacerbated by publishing links to online video conferencing meetings in open forums or on social media. Beyond the obvious risk to confidentiality, infiltrations of this sort can result in reputational damage, loss of credibility, disrupted business and the need to re-establish secure communications. To decrease the risk that a video conference could be infiltrated by a third party, hosts should ensure meetings are private and only accessible to invited participants. Also consider protecting video conferencing calls with a password, if possible, especially if you intend to discuss sensitive, confidential or personal information. Consider training employees on the proper use of these services to prevent these types of incidents.

File sharing

The use of link and file sharing through online video conferencing platforms presents a set of risks similar to those present when opening links or files from emails. If a conference has been infiltrated by a malicious actor, they may be able to convince meeting participants to click on a malicious link or open an infected document file that they provide. If possible, exchange files over a more secure platform than a third-party online video conferencing platform.

Best practices

Below are tips on how to utilize online video conferencing programs while protecting personal, client and business information:

- Choose an online video conferencing platform with appropriate security features. Factors to consider include: the level of encryption, the ability to require passwords or other methods of authentication in order to join a video conference call, etc. Also consider how the data is handled – some platforms may route data outside Canada or store shared data on servers they control.
- Set rules and expectations concerning the types of discussions that may take place on a given platform (for example, confidential material should never be shared over an online video conferencing platform). Refrain from unnecessarily disclosing confidential or personal information during your videoconference. If the parties intend to discuss personal or private information, consider disabling your participants' ability to record the call. Also consider developing policies for videoconferencing, and making employees and others aware of them.
- Ensure all parties using the online video conferencing platform are aware of and comfortable with any data sharing done by the software owner in order to realize a profit (i.e., selling data analytics for marketing purposes). Consider obtaining the client's consent prior to utilizing online video conferencing platforms to communicate with them, specifically advising them of the collection and possible use of their data by the service provider. Confirm this consent in an email.
- Follow news stories about your online video conferencing platform. Numerous reputable websites and sources publish stories related to privacy and security vulnerabilities of the various online video conferencing platforms.
- Review your own company's privacy policy to ensure it permits the use of online video conferencing – revisions to the policy may be required in order to utilize these services.
- When signing up for a new account with an online video conferencing platform, do not sign in using one of your existing social media accounts. It is recommend that individuals use an email address and unique password to access the platform in order to limit the amount of personal data collected.
- Ensure meetings are private and only accessible to invited participants to help prevent unwanted guests from joining. If possible, protect your video conferencing calls with a password, especially if you intend to discuss sensitive personal information. This will also help prevent unwanted guests from joining the call.
- Be cognizant of your surroundings during the call. This includes where you sit (who and what is visible in the background can reveal a lot of information that you may not want to share) and who can hear your call (you may need to wear headphones to isolate yourself in a separate room to prevent other people from overhearing your conversation).
- If you install a video conferencing app on your phone, tablet or computer, make sure you review its permissions and maintain its most up-to-date version. Developers regularly release updates to refine a tool's functionality and address new security vulnerabilities.
- If you are using a web browser for the video call, it would be best to open a new window with no other browser tabs. Preferably, close other applications to avoid inadvertently sharing notification pop-ups (such as new incoming emails) with other participants and the video conferencing.
- Before recording a meeting, even locally, obtain the participants' consent to do so. Do not record meetings to the provider's cloud unless it complies with your company's internal privacy policy.

Employee monitoring

With remote working arrangements expected to continue, organizations will be looking for ways to monitor employees who are no longer in the office under the direct supervision of their managers. There are a number of employee monitoring tools available to employers, but not all tools will be appropriate for an organization's operations and care should be taken in determining whether the use of such tools is permissible, and in selecting the right one. While employers have the right to monitor the activities of their employees and safeguard their IT systems and confidential information, Canadian privacy laws impose limits on the scope of technological monitoring.

IT security software can lead to personal information over-collection about employees, particularly where employees are using personal devices or computers to access their work systems while working from home. Accordingly, organizations should consider conducting a PIA and have their privacy officer work with the IT and procurement teams in developing the program or selecting a security or monitoring tool.

Assuming a rigorous PIA review process has determined that the use of employee monitoring tools is reasonably justified, organizations should consider the following best practices for implementing security programs and protocols:

- Employees should be notified that the program is in place and what information is being collected when they access the organization's systems. The notice (usually in the organization's terms of use policy) should set out the purpose of the collection, how the system works, how the information will be used and whom employees can contact for more information.
- Avoid continuous, real-time collection of personal information, such as keystroke logging or screen capturing. These practices should be reserved for targeted investigations where wrongdoing is reasonably suspected.
- Avoid collecting more information than necessary. Catch-all programs will result in collecting more personal information than necessary, in contravention of Canadian privacy laws.
- Implement training and policies for the employees who will be using tracking tools. The training should include not only technical and security training on how to use the software, but also privacy training. To the extent it does not compromise security, make the training materials and policies available to employees as a transparency measure.
- Log access to the system and periodically review the logs to ensure the system is being properly used.
- Periodically evaluate the effectiveness of the program, including whether there is a less intrusive way of addressing the issues the program was implemented to manage.

As the OPC has indicated, a flexible and contextual approach to privacy laws during this pandemic may permit the broader use of employee monitoring tools, provided there is a legitimate rationale, but organizations must consider whether the reason for the proposed monitoring is reasonable and whether their objectives can be met another way. Despite the difficulties with remote working, monitoring software is not a substitute for personal management.

In addition, the implementation of such tools and programs may be reasonable now, but may no longer be reasonable as the country and the economy open up. Organizations should not assume that what is permissible now will be permissible in the future, and should pay close attention to developments.

Key contacts

Kirsten Thompson
National Lead of the Transformative Technology and Data Strategy group
D +1 416 863 4362
kirsten.thompson@dentons.com

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

Chantal Bernier
Of Counsel
D +1 613 783 9684
chantal.bernier@dentons.com

Elizabeth Allum
Associate
D +1 403 268 3003
elizabeth.allum@dentons.com

Taylor Buckley
Senior Associate
D +1 604 648 6522
taylor.buckley@dentons.com

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

Karl Schober
Senior Associate
D +1 416 863 4483
karl.schober@dentons.com

Chloe Snider
Partner
D +1 416 863 4674
chloe.snider@dentons.com

Dentons, which has offices in 183 locations in 75 countries, has been at the forefront of the global legal response to COVID-19 since the beginning of the crisis. For further information on COVID-19 legal matters around the world, our Dentons COVID-19 (Coronavirus) Hub can be found here: **https://www.dentons.com/en/issues-and-opportunities/covid-19-coronavirus-hub**. Our 10,000 lawyers around the world are ready to assist with your global concerns.

ABOUT DENTONS

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in the New Dynamic.

dentons.com

This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content.
Please see dentons.com for Legal Notices.

CSBrand-30922-Return-to-Work-Toolkit-Dentons-Data-10 — 27/07/2020