COVID-19: Australian guidance on privacy and cybersecurity issues

March 30, 2020

Privacy and cybersecurity implications of COVID-19 – understanding your legal obligations in Australia

Introduction

In Australia, on 18 February 2020, the Federal Government activated its Emergency Response Plan for Novel Coronavirus[1] as its response to the challenge. Many companies are now actively monitoring to contain the virus and are asking their employees to report symptoms and enforce rules relating to isolation.

However, there are a number of privacy issues and laws for companies to bear in mind in responding to and managing risks relating to the COVID-19 pandemic.

First and foremost, any obligations imposed by the *Australian Privacy Act 1988* (Cth) (**Privacy Act**) or the Australian *Spam Act 2003* (Cth) (**Spam Act**) continue to apply.

In addition, there are other applicable workplace surveillance, general surveillance or health records laws imposed on employers which need to be complied with and these vary according to the type of monitoring and personal information collected.

COVID-19 related personal information may include information about:

- Individuals who have travelled to/from certain places, have symptoms or have tested positive or not.
- Employees that have been sent home to self-isolate or which visitors have been denied access to premises.

This information will all be “personal information” within the meaning of that term in the Privacy Act. And much of it will also be “sensitive data” given it is personal information which reveals information about health status. As sensitive data is higher in risk, it is afforded special protection under Australian privacy law.

What about consent to collecting and using COVID-19 personal information?

In summary, under the Privacy Act, consent is not necessary if collection of personal information is required or authorised under by or under an Australian law[2] or if “permitted general situation” exists. [3]

This includes where the collection is undertaken to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

Proposed uses or disclosure of the information for the non-primary purpose will be a secondary purpose and each company will need to assess if that is permitted by an exception to the Australian Privacy Principles under the Australian Privacy Act (**APP**s) – specifically APP 6 which outlines when an entity may use or disclose personal information.

For context, the rules provide:

- An entity can only use or disclose personal information for a purpose for which it was collected (the "primary purpose"), or for a secondary purpose if an exception applies.
- APP 6.2(b) expressly permits secondary uses where the use or disclosure is required or authorised under an Australian law or where a permitted general situation applies, such as where it is unreasonable or impracticable to obtain consent, and it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
- The information handling requirements imposed by some APPs do not apply if a "permitted general situation" exists.
- This exception applies in relation to the collection, use and disclosure of sensitive information.
- The most relevant permitted general situation in the current circumstances is "lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety". [4]
- This permitted general situation applies when an entity is collecting, using or disclosing personal information and it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and the organisation reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.

Can employers disclose information to employees or others?

On 29 February 2020, the Australian Commonwealth Government first published guidance for employers, which they have kept updated. The guidance notes that employers should provide information and brief all employees and contract staff on "relevant information" and procedures to prevent the spread of coronavirus. A key question is what would be considered "relevant information".

Australia's privacy regulator, the Office of the Australian information Commissioner (**OAIC**), provided its own privacy advice for the COVID-19 pandemic.

In summary, the legal position for employers under Australian law is as follows:

- Privacy obligations of most private employers to employees under the Privacy Act in Australia are less stringent because there is an "employee records exemption". [7] This exempts private companies from having to comply with the Privacy Act when they are processing their employees' personal information for a purpose directly related to the employment relationship.

- The exemption does not cover everything however:
  - **Not all information covered**: Not all the information an employer holds that relates to an individual employee would be an employee record – it will depend on the circumstances in any particular case.
  - **Contractors and volunteers not covered by the exemption**: Contractors, subcontractors and volunteers at employers are not covered by the exemption. Employers will need to look at the specific terms of the contracting arrangements to understand their rights and obligations.

Practical guidance: Below is some practical guidance when responding to the need to collect COVID-19 related personal information:

- **Why are you collecting?** Consider why you are collecting and document your reasons for, and methods of, collection of the personal information.

  In many cases, laws relating to handling employee health information will not prevent you from critical information sharing for the purpose of maintaining a safe workplace for employees and visitors.

  Apply common sense. It is reasonable to ask people to tell you if they have visited a particular high-risk country or are experiencing virus symptoms, but do not collect more information than you need.

  Take steps to tell your staff and visitors about how they should handle the information in responding to any potential or actual case of COVID-19 in the workplace.

- **Minimise where possible**: Personal information should be used or disclosed on a proportionate and "need-to-know" basis.

  This does not stop you from telling staff that a colleague or visitor has or may have contracted COVID 19 for information that is reasonably necessary in order to prevent or manage COVID-19 in the workplace.

  Only the minimum amount of personal information reasonably necessary to prevent or manage COVID-19 should be collected, used or disclosed.

  Consider if it is necessary if names need to be disclosed and, if yes, to whom they need to be disclosed and why.

  Collect as little information as is reasonably necessary or directly related to preventing or managing COVID-19. That includes information that the Department of Health says is needed to identify risk and implement appropriate controls to prevent or manage COVID-19, for example:

  - Whether the individual or a close contact has been exposed to a known case of COVID-19.
  - Whether the individual has recently travelled overseas and to which countries.

- **Use the personal information only for the purpose it is collected**: Generally, information should only be used for necessary purposes such as managing the immediate health risk and making decisions as to action required.
- **Do not keep the information for longer than necessary**: Also consider what information is needed to be retained for insurance purposes. Develop protocols/guidance for recommended actions given particular risk scenarios – including who gets notified in the event that someone tests positive. This will require a balancing of the interests of the individuals and the organisation.

  Check if subsequent processing of information for related purposes (such as lessons learnt about planning,

management and business continuity matters) could or should be carried out with anonymised data to the extent possible.

Beware the representations you make about your handling of information in your policies and statements

In October 2019, Australia's consumer protection regulator, the Australian Competition and Consumer Commission (**ACCC**), instituted proceedings in the Federal Court against a global online search provider alleging they engaged in misleading conduct and made false or misleading representations to consumers about the personal location data the provider collects, keeps and uses. The ACCC's case is focusing on representations contained expressly within the provider's privacy policies and also whether the provider made inadequate disclosures to consumer.

The clear message signalled by these proceedings is that organisations should not mislead consumers about the way in which they use personal information.

Specifically, organisations need to be careful to avoid scope creep – where they collect personal information for one purpose but use it for another.

Practical guidance: Below is some practical guidance for handling and disclosing how you are handling COVID-19 related personal information:

- Check your privacy notices/policies as to what they say regarding handling of personal information. Do they need updating? What do they say about the purposes of processing and use? Consider what representations you are making about handling of information in your policies and statements – are they true and accurate? Could they be misleading – either by what is not in them or what is in them?
- Consider where information is collected about non staff (e.g. visitors) and how you let people know about what you are doing. Could the relevant consents be provided on forms used to collect the data or perhaps with a link to the website privacy policies?
- Retain test/health status data only for so long as necessary to identify risk scenarios and to take immediate action. You may need it to follow up with those who have tested positive to ensure they have appropriate support and know when they should self-isolate and when it is safe to return to the office. You may also need it to comply with other legal obligations relating to occupational health and safety.
- If some of this information is generated in hard copy (visitors' confirmation that they have not been exposed to the virus), consider when you can dispose of it and how. If you no longer need it then it can be destroyed or deleted.
- Ensure any reasons for processing and retention of personal information contained in privacy policies are updated to ensure they cover COVID-19 categories of information.

Sharing of personal information

Under the Privacy Act, sharing of COVID-19 data with suppliers, clients and customers should be subject to obligations to keep it confidential and to handle it in line with applicable privacy laws. These obligations are most often set out in the contracts between parties.

The Privacy Act provisions and Spam Act provisions will still apply:

- If the information is to be shared with entities outside Australia, then the recipient will need to keep the information secure and managed in a way which complies with Australian laws. This guidance applies even if the transfers are between recipients of the same corporate group.

- If data sharing is necessary on a controller-to-controller basis (for example, with medical services, healthcare providers or public authorities (such as public health organisations)), carry out proportionate due diligence.
- Take all steps to manage or mitigate the adverse impact on privacy and to maintain compliance with laws.

What about sending information in messages to customers?

It would be a rare individual at present that has not received multiple emails, texts and other electronic messages from a variety of organisations relating to COVID-19. The volume of information messaging about the virus has increased so much that it is inevitable there are opportunistic activities taking place where some companies may be looking to exploit interest and fears about the virus. In other words, they are contributing to a spam spike being reported by providers of spam filter software services.[8]

The COVID-19 pandemic has created an exponential increase in communications and the need for them from organisations that are facing difficulties in complying with their contractual obligations due to factors beyond their control, including the inability to access products and services from suppliers or to operate from their usual premises/workplace.

In sending messages to customers and others, organisations need to be mindful of their obligations under the Spam Act.

- **What is spam – and are you spamming?** Spam is an unwanted email or message that advertises goods or services.

  If the message is not genuinely a message that advertises goods or services but is a message providing emergency management information to customers who may be impacted, then it would not be spam. To be spam, the message must be commercial. That means it must contain one or more of the following:

  - Offers
  - Advertisements
  - Promotions

- **What are the rules if it is spam?** To send (either directly or through another provider) marketing messages, the sender must:
  - First have the permission (express or implied) of the recipient
  - Include its contact details in the message
  - Have a way for the recipient to say “stop” getting messages

The Australian spam regulator, the Australian Communications and Media Authority (**ACMA**), has acknowledged[9] that the COVID-19 pandemic may create real difficulties for organisations to comply with their regulatory responsibilities due to factors beyond their control and so ACMA will,

> “… where warranted … Consider regulatory forbearance on a case-by-case basis … balanced against the potenti risk of consumer harm, the seriousness of any breach of law, efforts of organisations to comply and all other relevant considerations”.

In our view, it is unlikely that ACMA would be lenient in enforcing the Spam Act if a commercial message was sent in

breach of the laws even if it is dressed up as a COVID-19 emergency message.

How to take care of privacy when working remotely

The Privacy Act does not prevent employees from working remotely as a response to COVID-19, however the Australian Privacy Principles will continue to apply.

Practical guidance: To ensure compliance with privacy laws when working remotely, organisations should provide the following guidance to their employees:

- Use reasonable steps are in place to keep personal information secure when working remotely.
- Implement similar security measures for employees working remotely as those that apply in normal circumstances.
- Consider conducting privacy impact assessments to evaluate and mitigate risks to personal information where high privacy risk projects (or initiatives that involve new or changed ways of handling personal information) are being undertaken.
- Let employees know that they are expected to continue to comply with information security policies.
- Increase cyber security measures in anticipation of the higher demand on remote access technologies, and test them ahead of time – for example:
  - All devices, Virtual Private Networks and firewalls should have the updates and the most recent security patches (including to operating systems and antivirus software) and require strong passwords.
  - Multi-factor authentication for remote access systems and resources (including cloud services) is best practice and should be required.
- Ask anyone remote working should be reminded to store devices only in safe locations when not in use.
- Ask employees to check their access is only through trusted networks or cloud services.
- Remind your employees of your policies – including policies that work email accounts (not personal accounts) should be used for all work-related emails that contain personal information when working remotely.

For more information or assistance about managing your privacy obligations, please contact Robyn Chatwood or Ben Allen or your usual member of the Dentons Australia Privacy and Cybersecurity team.

---

1. See https://www.health.gov.au/resources/publications/australian-health-sector-emergency-response-plan-for-novel-coronavirus-covid-19↩
2. According to Australian Privacy Principles APP 3.4(a) under the Privacy Act↩
3. According to Australian Privacy Principles APP 3.4(b) under the Privacy Act↩
4. APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d)↩
5. See https://www.health.gov.au/resources/publications/coronavirus-covid-19-information-for-employers↩
6. See Section 7B(3) of the Privacy Act.↩
7. See https://success.trendmicro.com/solution/000247621-Coronavirus-COVID-19-is-being-used-in-email-Spam-attacks-Malware-and-other-Scams↩
8. See https://www.acma.gov.au/articles/2020-03/covid-19-important-information-industry↩

Your Key Contacts

Robyn Chatwood
Partner, Melbourne
D +61 3 9194 8330
robyn.chatwood@dentons.com

Ben Allen
Partner, Sydney
D +61 2 9035 7257
ben.allen@dentons.com