Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D20/20654

19 November 2020

Fiona Patten MLC
Chair
Legislative Council Legal and Social Issues Committee

By email only: contacttracinginquiry@parliament.vic.gov.au

Dear Chair

Inquiry into the Victorian Government's COVID-19 contact tracing system and testing regime

Thank you for your invitation of 6 November 2020, to make a written submission to the Legal and Social Issues Committee's (**the Committee**) inquiry into the Victorian Government's COVID-19 contact tracing system and testing regime (**the Inquiry**). In addition, I appreciated the opportunity to appear before the Committee alongside Ms Rachel Dixon, Privacy and Data Protection Deputy Commissioner on 16 November 2020.

As you would be aware, my office, the Office of the Victorian Information Commissioner (**OVIC**) is the primary regulator for information privacy, information security and freedom of information in Victoria, administering the *Privacy and Data Protection Act 2014* (Vic) and the *Freedom of Information Act 1982* (Vic).

This submission adds additional context to the matters raised at our appearance before the Committee, with a particular focus on the collection, use and disclosure of personal information pursuant to the *Workplace Directions (No 9)*[1] (**Workplace Directions**) issued by the Chief Health Officer under the *Public Health and Wellbeing Act 2008* (Vic).[2]

The privacy frameworks operating in Victoria

In Victoria, three pieces of legislation operate to regulate and protect the information privacy of individuals:

1. *Privacy and Data Protection Act 2014* (Vic) (**Victorian Privacy Act**): The Victorian Privacy Act only applies to the Victorian public sector (**VPS**) – that is, Victorian state and local government agencies and organisations. The Information Privacy Principles (**IPPs**)[3] contained in the Victorian Privacy Act regulate the collection, use and disclosure of personal information by those agencies and organisations. 'Personal information' under the Victorian Privacy Act means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or

[1] https://www.dhhs.vic.gov.au/workplace-directions-no-9-pdf.
[2] Issued under section 200(1)(d) of the *Public Health and Wellbeing Act 2008* (Vic).
[3] The IPPs are contained in Schedule 1 of the Victorian Privacy Act and set out the obligations of the Victorian public sector in relation to the handling of personal information.

not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include health information.[4]

2. *Health Records Act 2001* (Vic) (**HR Act**): The HR Act applies to the VPS, as well as private sector organisations that are not subject to the *Privacy Act 1988* (Cth) and who provide health services. The Health Privacy Principles (**HPPs**)[5] contained in the HR Act regulate the collection, use and disclosure of health information. 'Health information' can broadly be described as personal information that also concerns an individual's physical, mental or psychological health, a disability, or personal information collected to provide a health service.[6]

3. *Privacy Act 1988* (Cth) (**Commonwealth Privacy Act**): The Commonwealth Privacy Act applies to Commonwealth government agencies and organisations, and all private sector businesses with an annual turnover of more than $3 million. It does not apply to the VPS. Where the Commonwealth Privacy Act applies, the Australian Privacy Principles (**APPs**) must be complied with when collecting, using and disclosing personal information.[7] In the Commonwealth Privacy Act 'Personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not.[8]

Sharing personal information and other data

While complexities exist in identifying whether information is considered health or personal information – and subsequently, which of the Victorian Privacy Act or HR Act applies to that information – in my view, the Victorian Privacy Act has not been a barrier to the appropriate sharing of personal information within government throughout the COVID-19 pandemic. In particular, I note that under the IPPs, personal information can be disclosed or shared where an organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to public health, public safety or public welfare.[9] Noting personal information is permitted to be shared and disclosed to respond to the current pandemic under the IPPs, protections from inappropriate use or disclosure nonetheless continue to apply under the IPPs.

My office was consulted on the development of the VPS COVID-19 Data Sharing Policy[10] and the VPS COVID-19 Data Sharing Heads of Agreement.[11] Together, these documents established a framework for sharing information for the purpose of enabling the Victorian Government to respond to and recover from the impacts of COVID-19.

This framework includes specific obligations and protections when handling personal information. For example, personal information must be removed from the data to be shared, unless it is necessary for fulfilling a specific purpose and is legally permitted to be shared; and shared data must be destroyed after the purpose for its collection or sharing has been fulfilled.

The Workplace Directions

The Workplace Directions require all employers operating within Victoria (with limited exceptions) to request the personal information of employees, customers and other persons (collectively **'visitors'**) who attend their premise for longer than 15 minutes. This record-keeping requirement is set out in clause 7 of the Workplace Directions and requires the visitor's first name and phone number to be requested, along with the time and date of their attendance to be recorded.

[4] Defined in section 3 of the Victorian Privacy Act.
[5] The HPPs are contained in Schedule 1 of the HR Act and set out the obligations of the Victorian public sector in relation to the handling of health information.
[6] 'Health information' is defined in section 3 of the HR Act.
[7] The APPs are contained in Schedule 1 of the Commonwealth Privacy Act.
[8] Defined in section 6 of the Commonwealth Privacy Act.
[9] See IPP 2.1(d)(ii) and the equivalent provision under HPP 2.1(h)(ii) of the HR Act.
[10] https://www.vic.gov.au/victorian-public-service-covid-19-data-sharing-policy.
[11] https://www.vic.gov.au/victorian-public-service-covid-19-data-sharing-heads-agreement.

2 of 5

Encouragingly, clause 10 of the Workplace Directions sets out certain protections when personal information is collected by an employer in accordance with the obligation in clause 7. These protections include:

- only collecting the first name and phone number of the visitor – clause 10(a)(i);
- using reasonable endeavours to protect the personal information from use or disclosure except where requested for contact tracing – clause 10(a)(ii);
- using reasonable endeavours to notify a visitor that their personal information is being collected for contact tracing purposes – clause 10(a)(iii); and
- destroying the personal information as soon as reasonably practicable following 28 days after the visitor's attendance – clauses 10(a)(iv) and 10(b).

Victorian Government operated check-in system

As OVIC understands it, the Victorian Government has developed and is currently piloting its own check-in system to assist Victorian premises to meet the record-keeping requirements of the Workplace Directions and provide a mechanism by which visitors can record their attendance. The check-in system comprises a web-based portal for businesses to register for a quick response code (**QR code**) provided by Service Victoria, and a digital check-in system that allows a visitor to scan the QR code provided by Service Victoria. Service Victoria has also incorporated the check-in process into their app. This process allows a visitor to provide their first name and phone number without disclosing it to the business they are visiting.

Scanning the QR code provided by Service Victoria and checking in at premises can be done with a visitor's phone camera (without the Service Victoria app), or alternatively using the Service Victoria app. Importantly, visitors have a choice in what method they use, and a Service Victoria account is not required for a visitor to use the Victorian Government provided check-in system. OVIC views this choice for individuals as an important element of the design of the check-in solution.

The Victorian Government, through the Department of Premier and Cabinet, has consulted with OVIC on the development of its check-in system, and has demonstrated a commitment to ensuring that the system is designed with privacy and security-enhancing features. OVIC welcomes this approach and has appreciated the opportunity to provide feedback on the system from a privacy perspective.

Privately operated check-in systems used by businesses

Alongside the Victorian Government check-in system, employers continue to have a choice to use alternative check-in systems offered by the private sector. Private sector check-in systems use a variety of methods including QR codes, phone apps, web-based, and paper check-in systems.

To assist with rapid contact tracing, OVIC understand the Victorian Government plans to provide the private sector with access to an application programming interface (**API**) to enable information collected by private check-in providers to be easily shared with Department of Health and Human Services (**DHHS**) contact tracers. In the event a case of COVID-19 is detected, the API will facilitate the direct transfer of the name and phone number of all other visitors who were checked-in at the premise during the period in which the infected visitor was present.

Privacy and information security considerations of the check-in systems

The Victorian Government operated check-in system has a number of privacy and information security enhancing features when contrasted with private sector check-in systems. These include:

3 of 5

- In addition to the protections contained in clause 10 of the Workplace Directions, the Victorian Government operated system is subject to the Victorian Privacy Act and regulatory oversight by my office. As such, visitors who use this system are provided the privacy protections, complaint pathways and enforcement mechanisms contained within the Victorian Privacy Act.

- The personal information is stored by the Victorian Government on local servers, and cannot be used or accessed by businesses. This means the personal information will not be used or accessed for secondary purposes such as marketing or profiling. The personal information will only be accessed by DHHS for contact tracing purposes, where required.

- Visitors using the system are only asked to provide their first name and phone number, ensuring only the minimum amount of required personal information is collected.

- Service Victoria will delete the personal information after 28 days have passed, ensuring the personal information is not stored indefinitely.

Privately operated check-in providers and the businesses that use them or other manual check-in methods may lead to several unfavourable privacy and information security implications when contrasted with the Victorian Government's check-in solution. These may include:

- While the Victorian Government operated system and privately operated systems will supplement each other and ensure broad coverage, the Victorian Government should be cautious in ensuring it does not endorse or promote the use of private sector systems. There is potential for the Victorian Government to be seen to inadvertently endorse private providers who choose to utilise the API for the transfer of data collected to DHHS. This may be problematic where the privacy and security practices of private check-in system providers are not as robust as those found in the Victorian Government's check-in solution.

- Businesses and privately operated check-in systems with a turnover of more than $3 million are subject to the obligations contained in the Commonwealth Privacy Act, and to oversight by the Office of the Australian Information Commissioner (**OAIC**). However, where they have a turnover of less than $3 million, they are not subject the Commonwealth Privacy Act. As a result, many private check-in providers and businesses are not subject to any privacy laws, and the way in which personal information is collected, used and disclosed is therefore largely unregulated. This means visitors do not have a legislated right to seek redress by complaining to an oversight authority if their personal information is inappropriately used or disclosed by a private check-in provider or the business they visited.

- Businesses are required to comply with the limited use and disclosure restrictions contained in clause 10 of the Workplace Directions. However, as there is no specific oversight authority, the ability to ensure businesses comply with the Workplace Directions is limited.

- Given the jurisdictional complexities outlined, private check-in providers and businesses may not be fully aware of their obligations under the Commonwealth Privacy Act, where they exist. Additionally, many businesses are unlikely to be aware of the limits on the use and disclosure of personal information contained in the Workplace Directions. As such there is a heightened risk that:

    - Private check-in providers will permit, or businesses will choose to over collect personal information. For example, collecting email and residential addresses. As previously noted, clause 10(a)(ii) of the Workplace Directions requires businesses to only collect a visitor's first name and phone number.

    - Personal information will be used for marketing, profiling or other purposes outside of contact tracing, whether or not these other purposes are communicated to individuals at the time they

4 of 5

provide their personal information. As previously noted, clause 10(a)(ii) of the Workplace Directions require personal information to be protected from use or disclosure except for contact tracing purposes. Compliance with the Workplace Directions may therefore require the private providers to modify their apps or services to limit collection and use. It is unclear whether there is any way to compel them to do so.

Transparency and maintaining public trust

Key to the effectiveness of any contact tracing system is establishing and maintaining public trust in that system. To achieve this the Victorian Government needs to be proactive in ensuring businesses operate in accordance with the Workplace Directions and are aware of their obligations under those directions. If personal information is misused, it has the potential to impact the public's trust and their willingness to provide accurate contact details, undermining the entire contact tracing system.

This requires both the Victorian Government and businesses to openly communicate with the public, and be transparent when telling individuals how their personal information will be used and protected.

Thank you again for the opportunity to appear before the Committee and make a submission in relation to this Inquiry. I have no issues with my submission being published on the Committee's website without further reference to me.

If you have any questions about this submission, please don't hesitate to get in touch with me directly [redacted] or my colleague, Cliff Bertram, Principal Policy Officer, [redacted]

Yours sincerely

[redacted]

Sven Bluemmel
Information Commissioner

5 of 5