



Australian Government

Office of the Australian Information Commissioner

Draft Guidelines

Requirements to collect personal information for contact tracing purposes

The Office of the Australian Information Commissioner and state and territory privacy regulators have produced the following draft guidelines to support a nationally consistent approach to requirements for businesses and venues to collect contact information.

The guidelines can be used by governments when drafting requirements and designing methods to require collection of contact information from individuals by a business or venue. This includes collection via digital check-in services such as apps and QR codes.

As domestic borders open, harmonisation of requirements to collect personal information would ensure personal information is handled consistently. This supports businesses and venues to develop solutions to meet the requirements, and individuals to confidently provide accurate personal information for contact tracing purposes. Protecting personal information is central to maintaining public trust and promoting compliance with health orders and contact tracing processes.

Currently state and territory orders have some common requirements, but others differ. These draft guidelines suggest ways to harmonise these requirements.

We are seeking feedback on the draft guidelines from Chief Medical Officers, health departments, digital check-in providers, businesses and venues, and the community.

Data minimisation

State and territory orders that require contact details to be collected for contact tracing purposes should be limited to the minimum information necessary for that purpose.

This means that a business or venue should only be required to collect:

- a first name or pseudonym (where practicable)
- a contact phone number or email address, and
- the time and date of attendance at venue.

Security

Contact information should be required to be protected from disclosure to other customers and securely stored by the business or venue, or their chosen provider (where the business or venue is using a third-party digital check-in service).

Reasonable steps should be required to be taken to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure. This includes using reasonable physical and/or ICT controls to limit access to the information.

In line with community expectations, the information should be stored in Australia.

Contact information collected by a business or venue should be required to be securely transmitted to the relevant health department for contact tracing purposes. Where a third-party digital check-in service is used, it is preferable for the contact information to be securely transmitted directly from the provider to the health department, rather than via the business or venue.

Purpose limitation

Information that is collected by a business or venue solely for contact tracing purposes should be required to:

- only be used and disclosed to health authorities for contact tracing purposes
- not be used or disclosed for any other purpose, such as direct marketing.

Where a business or venue collects information for more than one lawful purpose that must be clearly explained prior to collection.

Retention/deletion

Information that is required to be collected by a business or venue for contact tracing purposes should be required to be securely destroyed after a maximum of 30 days.

Regulation by the Privacy Act

Personal information collected by a business or venue for contact tracing purposes should be protected by an enforceable privacy law to ensure that individuals have redress if their information is mishandled:

- A business or venue operating a digital check-in service should choose a third-party provider that is covered by or has opted in to coverage of the *Privacy Act 1988* (Privacy Act).
- Digital check-in providers which are not already covered by the Privacy Act should opt in to coverage (s6EA).

If a business or venue has developed its own digital check-in service, and it is not already covered by the Privacy Act, it should opt in to coverage (s6EA). States which are implementing government-developed digital check-in services, and which do not have enforceable privacy laws, should consider opting in to coverage of the Privacy Act (s6F).

This would extend rights and protections to residents of other states and territories where their information is being shared with a state which does not have privacy protections in place.

Information on how to opt in to the coverage of the Privacy Act can be found on the [OAIC website](https://www.oaic.gov.au).