

Information Act 2002 Guideline

Special rules – Privacy



February 2021

Publicly available information

The Privacy scheme doesn't apply to:

- archives that are publicly available; or
- materials in collections of libraries, art galleries and museums that are on public display or publicly available for reference or study purposes (s12).

Information Privacy Principles 2 and 4-10 don't apply to information in publications generally available to the public (s68). However, IPP 1 (Collection) and IPP 3 (Data Quality) do apply.

Information on a public register must be kept in compliance with the IPPs to the extent that it is reasonably practicable to do so given the requirements imposed by or under an Act for keeping the register and making it available for public inspection (s68).

Old information (pre-July 2003)

The Privacy scheme applies to all personal information collected after 1 July 2003.

It also applies to personal information collected before that time if the organisation handles the information at any time after that time (s14).

Courts and tribunals

The *Information Act 2002* does not apply to:

- a court in relation to its judicial functions;
- a tribunal in relation to its decision-making functions;
- a coroner in relation to an inquest or inquiry;

- a judge in relation to a preliminary examination (s5(5)).

The IPPs don't apply in relation to a proceeding or other matter before a court or tribunal (s69).

Health and Safety

An organisation will not breach IPP 2 by using or disclosing personal information if it reasonably believes that the use or disclosure is necessary to lessen or prevent (IPP2.1(d))

- a serious or imminent threat to the individual's or another individual's life, health or safety; or
- a serious or imminent threat of harm to, or exploitation of, a child; or
- a serious threat to public health or public safety.

Emergency situation or public health emergency

An organisation may collect, use or disclose personal information in a way that would otherwise contravene the Information Privacy Principles during an emergency situation or a public health emergency, if the information is being collected, used or disclosed for certain purposes (s81A).

Permitted purposes are defined under s81A. They are:

- coordinating operations for the response, management or recovery;
- identifying individuals who may be injured missing or dead as a result of the emergency situation or public health emergency, or are otherwise involved;

- assisting individuals involved in the emergency situation or public health emergency in obtaining services; and
- assisting with law enforcement in relation to the emergency situation or public health emergency.

A public health emergency is declared under the *Public and Environmental Health Act 2011* and an emergency situation is defined under the *Emergency Management Act 2013*.

Law enforcement agencies

A law enforcement agency is not required to comply with an IPP if the agency believes on reasonable grounds that non-compliance is necessary for the purposes of one or more of its or another law enforcement agency's functions (s70).

Section 70 sets out a non-exclusive list of law enforcement functions, which extends to executing orders or decisions of a court or tribunal, locating missing persons and providing services in emergencies.

The definition of "law enforcement agency" is broad. It includes other state, territory and Commonwealth police forces and the Australian Crime Commission. It also includes organisations that perform a law enforcement function as one of a number of functions. For example, a municipal council has numerous functions, many of which do not involve law enforcement.

The context of s70 makes it clear that the exception only excuses non-compliance in relation to the performance of law enforcement functions — not unrelated other functions of the organisation.

Use for, or disclosure to, a law enforcement agency

An organisation (whether or not it is a law enforcement agency) will not breach IPP 2 by

using or disclosing information if it reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency (IPP 2.1(g)):

- (i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
- (ii) enforcing a law relating to the confiscation of proceeds of crime;
- (iii) protecting public revenue;
- (iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
- (v) preparing for or conducting proceedings before a court or tribunal or implementing the orders of a court or tribunal.

If an organisation uses or discloses personal information under IPP 2.1(g), it must make a written note of the use or disclosure.

An organisation will not breach IPP 2 by disclosing information to ASIO or ASIS, as long as it is a properly authorised request in accordance with IPP 2.1(h) or (i).

Nothing in IPP 2 requires an organisation to disclose personal information to a law enforcement agency. It does not override any existing legal obligation not to disclose information.

However, it is not intended to deter public sector organisations from lawfully co-operating with law enforcement agencies in the performance of their functions.

The exception relates to IPP 2 only. Organisations must still comply with other IPPs. In particular, IPP 9, dealing with transfers of personal information outside the Territory must be complied with.

Unlawful activity

An organisation will not breach IPP 2 by using or disclosing personal information if it has reason to suspect that unlawful activity has been, is being or may be engaged in and uses or discloses the information (IPP 2.1(e)):

- as a necessary part of its investigation of the matter; or
- in reporting its concerns to relevant persons or authorities.

Statistics and Research

An organisation will not breach IPP 2 by using or disclosing personal information if it is:

- necessary for research or compilation of statistics in the public interest;
- not published in a way that identifies the individual;
- not practicable to obtain the individual's consent;
- believed the recipient would not disclose the information.

The exception only applies to statistics and research. Organisations must still comply with other IPPs.

If the information is health information see [Guideline IPP 2.1\(ca\)\(iv\) and s86\(1\)\(a\)\(iv\) Use and Disclosure of Health Information.](#)

Authorised variation from IPPs

An organisation can apply to the Information Commissioner to authorise collection, use or disclosure that would otherwise be in breach of IPP 1, 2 or 10. For more, see [Authorising Departure from the IPPs.](#)

An organisation can apply to establish a Code of Practice that may supplement, vary, or act in place of, the IPPs.

This guideline is produced by the Information Commissioner to promote awareness and understanding about the *Information Act 2002*. It is not a substitute for the Act. You should read the relevant provisions of the Act to see how it applies in any particular case.

Any views expressed in this guideline about how the Act works are preliminary only. In every case, the Commissioner is open to argument by a member of the public or a public sector organisation that a different view should be taken.