Office of the Information Commissioner
Queensland

Interpreting the legislation – *Information Privacy Act 2009*

Sending personal information out of Australia

This guideline does not reflect the current law.

It reflects the *Information Privacy Act 2009* as it existed prior to 1 July 2025.

It has been provided for the use of agencies and Ministers dealing with privacy complaints or compliance issues that occurred before 1 July 2025, and for bound contracted service providers to whom the pre-1 July 2025 IP Act continues to apply.

1.0 Overview

The *Information Privacy Act 2009* (Qld) (**IP Act**) explicitly regulates the transfer of personal information **outside of Australia**.

Once personal information has left an agency[1] and passed into the possession of someone who is not subject to the IP Act, the protections under that Act are lost. Transfer outside of Australia must only be done in accordance with section 33.

2.0 Transfer outside Australia

Section 33 of the IP Act sets out when an agency may transfer personal information outside of Australia. There are four circumstances in which such a transfer may occur:

- 33(a) – the individual has agreed
- 33(b) – the transfer is authorised or required under a law
- 33(c) – the agency is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of any individual, or to public health, safety and welfare
- 33(d) – if two or more of the criteria in 33(d) apply (see below).

[1] In this Guideline references to an 'agency' include Ministers and bound contracted service providers, unless otherwise specified.

Hint: transfer versus transit

Section 33 of the IP Act sets limits on transferring personal information overseas. But how does it apply to email which may go through a lot of different countries as it makes its way to its destination?

When you send an email it travels out of your agency's network and through a number of routers until it reaches its destination. Those routers may be located in Australia or they may be located overseas; it's impossible to know which it will be when you hit the send button.

The view of the OIC is that, when an agency sends email to another Australia-based email address, if personal information is routed through another country and immediately directed back to Australia it has not been transferred overseas.

Note that this does not apply when sending email to non-Australia based email addresses, such as Gmail or Hotmail.

The definition of *privacy principles* in schedule 5 of the IP Act makes the obligation to comply with section 33 of the IP Act a privacy principle. The obligations in section 33 do not replace the Information Privacy Principles (**IPPs**) or the National Privacy Principles (**NPPs**). Rather, they add an additional layer of factors that must be met when transferring information overseas.

For example:

- Where the transfer constitutes a disclosure and the agency is subject to the IPPs, it may disclose only if permitted by IPP 11 and comply with the obligation in IPP 11(3) to take all reasonable steps to ensure the recipient will not use or disclose the personal information for a purpose other than that for which it was provided.

- Where health information is being transferred overseas by a health agency for research or statistic compilation, the obligation in NPP 2(1)(c)(iii) applies, requiring the agency to reasonably believe the recipient will not disclose it.

Whenever personal information is transferred by an agency to a third party there is a risk that the personal information may not be appropriately protected. This is a particular concern when it is transferred overseas, given the practical difficulties of enforcement in a non-Australian jurisdiction.

Hint

Transfers under 33(a), (b), (c) and parts (d)(ii) and (iii) do not expressly require that the personal information be subject to privacy protections. However, the IPPs or NPPs may require that the information be protected.

3.0 The individual agrees to the transfer – 33(a)

An agency may transfer personal information outside of Australia if they have the agreement of the individual the information is about. The agreement must be fully informed, voluntary, specific, current and given by an individual with the legal capacity to do so. The individual should also be told of any privacy risks that could result from the transfer.

Agreement must not be confused with notice given under the privacy principles relating to collection. It is unlikely that the purpose of collecting personal information would ever be solely to transfer it outside of Australia, though the transfer may be contemplated at the time of collection.

Even if the individual was told in the collection notice that their information might be transferred out of Australia, their agreement will still need to be sought under this section.

Hint

See *Key Privacy Concepts – agreement and consent* for further discussion on what constitutes valid agreement under the IP Act.

4.0 The transfer is required or authorised under a law – 33(b)

Generally, the law in this section must be legislation and it must apply to the agency that holds the information. The Act and section on which the agency is relying must be clearly identified.

The law may **require** the transfer of the personal information, meaning the agency cannot refuse to transfer it, or it may simply **authorise** the transfer, meaning the agency has a discretion to transfer it or not.

Implied legal authority may be relied upon where the law clearly requires or authorises a function or action, and it is impossible to give effect to the law without transferring the personal information.

5.0 The transfer is necessary to lessen or prevent a serious threat to life, health, safety or welfare – 33(c)

There must be a sufficient link between the transfer of the personal information and the prevention or lessening of the threat. Transfer of this kind would normally be to an entity with the capacity and authority to intervene to reduce the threat, where the intervention cannot occur without the personal information.

This section should only be used in emergency or extraordinary situations where time is of the essence. It should not be used to justify regular or ongoing transfers, even if those transfers are intended to reduce serious threats to life or health.

6.0 Transfer under section 33(d)

Section 33(d) allows personal information to be transferred to an entity outside Australia if **any two or more** of the following apply.

6.1 33(d)(i) – recipient subject to equivalent privacy obligations

> *the agency reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs or, if the agency is a health agency, the NPPs.*

The application of privacy laws and schemes can be complex, and those in overseas jurisdictions may be significantly different from the Queensland IP Act. It may be necessary to seek legal advice about the privacy laws or schemes, and/or their application to the entity to which the information is proposed to be transferred.

The key elements in satisfying 33(d)(i)are:

- the form and content of the obligation
- the extent to which the law, binding scheme or contract can be effectively upheld
- the similarity of the law, binding scheme or contract to the privacy principles in the Queensland IP Act.

Hint

Information about a jurisdiction's privacy laws is often available on websites maintained by oversight or government bodies in different jurisdictions. Additionally, more general lists are often maintained by international privacy bodies. While these can be out of date and their accuracy cannot be guaranteed, they can be a good starting point.

6.2 Is the recipient subject to a law, binding scheme or contract?

As a general rule, this may be satisfied where the recipient is, for example:

- bound by a privacy or data protection law that applies in the recipient's jurisdiction
- required to comply with some other law that imposes data collection and handling obligations in respect of personal information, such as taxation or criminal laws, which often include provisions that authorise or prohibit certain uses and disclosures
- subject to an industry scheme or privacy code enforceable against its participants, whether participation is voluntary or not, as long as the recipient is participating in the scheme or code
- a bound contracted service provider under section 35.

The recipient is unlikely to be considered subject to a law, binding scheme or contract where, for example:

- the recipient is exempt from some or all of the data protection law or regulation
- there is an existing or proposed authority, such a public interest waiver or direction, which means the recipient will not have to comply with some or all of the law or scheme
- the information being transferred is not protected under the privacy or data protection law
- the recipient is able to opt out of the binding scheme without notice and without returning or disposing of the transferred information
- the agreement is unenforceable at law.

Hint

Where privacy law coverage in the recipient's jurisdiction is poor, sketchy or non-existent, and there is no applicable industry scheme or code in place, agencies may be able to adequately bind the recipient by way of a contract.

The discussion in *Contracted service providers under the IP Act* may be helpful.

Where personal information is being transferred to a bound contracted service provider located overseas the principles to be upheld will be identical to the privacy principles in the IP Act.

6.3 Does the relevant law, binding scheme or contract effectively uphold the fair handling principles?

The fact that fair handling principles exist in the recipient's jurisdiction may not be enough to satisfy this. The principles must be **capable of being effectively upheld**.

Capable of being effectively upheld is not defined, but includes, for example:

- that the privacy protections can be enforced
- that individuals have rights they can exercise if the privacy obligations have been breached.

A detailed examination of the principles and their framework should be conducted, to determine the extent to which they are capable of being upheld.

Hint

Principles that exist but contain no provisions relating, for example, to compliance, investigations, complaints or obligations to comply will generally not be considered 'capable of being effectively upheld'. It is important that there are mechanisms which allow the individual to seek redress against the recipient if a breach should occur.

Where a contract is being relied on to satisfy this section determining if its principles can be effectively upheld may be difficult.

- If the recipient is a bound contracted service provider under section 35, and the service arrangement is a contract, the principles will be capable of being effectively upheld.

- Where the recipient is not a bound contracted service provider, this section may be difficult to satisfy. The individual whose information is being transferred is not a party to the contract. This means they will not be able to take any action if the recipient breaches the contract in relation to their personal information.

Provisions that could be included in the contract to make it capable of being effectively upheld are those that:

- establish mechanisms enabling access and correction rights to be exercised
- require complaints to be independently investigated and appropriate redress to be provided for harm arising from a privacy breach
- allow for compliance audits to be undertaken
- require the recipient to take appropriate steps to promote compliance within the recipient body.

Hint

Refer to the Victorian Privacy Commissioner's *Model Terms for Transborder Data Flows of Personal Information* as a starting point.

6.4 Are the fair handling principles substantially similar to the privacy principles?

In order to be substantially similar, the principles in question must have enough in common with the privacy principles in the Queensland IP Act. This will involve a comparison of the content of the two regimes to determine their similarity.

Some variation between the two is acceptable, but the principles binding on the recipient cannot be significantly weaker than the privacy principles under the IP Act.

The approach in this section is based on the Victorian approach, and the Victorian guidelines identify some steps for assessing substantial similarity.

- To help determine the similarity of the two sets of principles, the principles should be compared side by side and the similarities and differences noted.

Hint

Generally, where personal information is transferred from a Queensland government agency to a recipient overseas it should be adequately protected by the recipient and use for legitimate purposes only.

- The importance of any similarities or differences should be assessed. When making this assessment, agencies should consider essential features of the relevant privacy principles and the objects of the IP Act.

- Decide whether there is a substantial similarity between the privacy principles and the principles binding the recipient. This is a question of fact, to be determined taking into consideration all the circumstances.

6.5 33(d)(ii) – transfer is necessary to perform a function

the transfer is necessary for the performance of the agency's functions in relation to the individual.

Transfer under this section does not need to benefit the individual. Some functions of an agency in relation to an individual will not be for their benefit, for example, investigation into the individual's actions where they have allegedly breached an Act which is administered by the agency.

However, the transfer of personal information must be necessary for the performance of the function, and the function must relate to the individual.

6.5.1 Necessary

When considering whether the transfer is necessary, the personal information does not have to be essential or critical to the performance of the function, but it must be more than just helpful or expedient. If there is a way to perform the function that does not involve transferring the personal information that would not be significantly more onerous, it may be difficult to satisfy this section.

6.5.2 The agency's functions

The transfer must relate to the functions of the agency that is transferring the information, not the function of the recipient or any other agency.

Example

Agency A may hold information about Person X which is not held by Agency B. Agency B's functions involve providing a service to Person X that they can only perform if Agency A gives the information they hold to Body Q, which is located overseas. This will not be a valid transfer under this section, as it was done to assist the functions of Agency B, and not of Agency A.

The functions of an agency can be determined by what they are legally permitted to do. If the action is set out in legislation administered by the agency, it will clearly be within its functions. Additionally, the functions of an agency can be set by government policy or Parliamentary direction. Essentially, it must be an action, activity, or obligation that falls within the purpose for which the agency exists and its responsibilities.

If in doubt, reference to the Administrative Arrangements Order in force at the time, the agency's annual report or relevant government policy documents should assist. If still unsure, legal advice should be sought.

6.5.3 Relation to the individual

The function must relate to the individual the information is about. It is not sufficient that information about a group of individuals is transferred overseas to allow an agency to perform a function in relation to only some members of the group. Each and every individual whose information is to be transferred must fall within the function, even if transferring only some of the group's information would make the task significantly more onerous or even impossible.

Example

As part of its functions, Agency D must provide life insurance to some of its officers. It decides that outsourcing this function to an overseas service provider is necessary to perform it. This involves Agency D transferring personal information to the service provider's servers in another country.

Agency D wants to transfer the information of *all* of their officers, even the ones who do not qualify for life insurance, because it will be easier.

Under this section, only the information of the officers who actually qualify for the insurance can be transferred, because the function relates only to those officers.

6.6 33(d)(iii) – transfer is for the individual's benefit

> *the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement.*

Hint

See *Privacy Guideline Section 4 – Key Concepts* for detailed discussion on the concept of practicability and agreement.

In order to satisfy this section, the transfer must be for the benefit of the **actual** individual that the information is about. The transfer may occur without the agreement of the individual, but only where:

- it is not practicable to seek it, and
- the individual would be likely to agree if they were asked.

Example

The transfer of personal information overseas is to assist in identifying and assisting a seriously injured person. It is not practicable to seek their agreement, given they are injured and overseas, but, if they were asked, they would be highly unlikely to refuse.

6.7 33(d)(iv) – reasonable steps have been taken to ensure the information is protected

> *the agency has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is a health agency, the NPPs.*

Generally, circumstances that satisfy 33(d)(i) will satisfy 33(d)(iv).

The focus in 33(d)(iv) is on the actions taken by the agency, rather than the laws or standards binding the receiver. It can be satisfied even where there is no law, binding scheme or contract applying to the recipient.

If the agency has taken reasonable steps to ensure that the information being transferred will not be handled contrary to the privacy principles, this section will be satisfied.

The agency must take reasonable steps, but these could be technical, practical, or administrative, and need not be legally enforceable. What are reasonable steps will depend on the circumstances and the nature of the personal information.

Hint

See *Key privacy concepts – reasonable* for a discussion on what 'reasonable' means.

Reasonable steps could include:

- taking practical steps to limit the amount of information transferred
- entering into an agreement to clarify permissible and prohibited uses and disclosures
- securing the information from the time of transfer until its return or destruction.

For additional information and assistance please refer to the OIC's privacy guidelines or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

Published 30 June 2009 and Last Updated 19 July 2013

Changes to legislation after the update date are not included in this document