Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Interpreting the legislation – Information Privacy Act 2009

Disclosing personal information out of Australia

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009* in a general way.

This guide is not legal advice and additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

Overview

Agencies must comply with the *Information Privacy Act 2009* (Qld) (**IP Act**) when handling personal information. Section 33 of the IP Act regulates the disclosure of personal information outside of Australia.

Section 33 only applies to disclosure, and not to any other movement of personal information out of Australia, e.g., an agency sending personal information to an officer travelling overseas.

Any disclosure of personal information must also comply with Queensland Privacy Principles 6 (QQP 6), which means overseas disclosure must satisfy both QPP 6 and section 33.

What is disclosure?

Disclosure is defined in section 23(2) of the IP Act. Personal information is only disclosed if:

- the agency gives it to an entity who does not already know it and is not in a position to find it out; and
- the agency ceases to have control over who will know that information in the future.

See ***Key privacy concepts – disclosure*** for more information.

What if the agency retains control

Section 33 sets out when personal information can be disclosed overseas. This includes where two of the four circumstances in section 33(d) can be satisfied. Section 33(d)(i) and (iv) involve a consideration

of how the overseas recipient will handle the personal information and any privacy rules which apply to it.

If the agency satisfies 33(d) by, for example, entering into a contract that limits what can be done with the personal information, then giving it to the recipient may not be a disclosure, as the agency has not lost control over who will know the information in the future.

If giving personal information to the overseas recipient is not a disclosure, section 33 does not apply. However, agencies should ensure that other privacy obligations are met, e.g., ensuring personal information is appropriately secured in compliance with QPP 11.

When can personal information be disclosed outside Australia?

Section 33 allows disclosure outside Australia if:

- 33(a) – the individual has agreed
- 33(b) – the disclosure is authorised or required under a law
- 33(c) – the agency is satisfied on reasonable grounds that the disclosure 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).

The individual agrees to the disclosure – 33(a)

An agency can only disclose personal information under section 33(a) if the individual agrees. This aligns with QPP 6.1(a). If an agency is permitted to disclose under 6.1(a), it will be able to disclose overseas under section 33.

Agreement in section 33 has the same meaning as consent. This means to be valid; 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 disclosure.

Agreement must not be confused with informing the individual of the QPP 5 matters when collecting their information. Even if the individual was advised under QPP 5 that their information might be disclosed overseas, unless the statement is very clear it may not be sufficient to constitute agreement.

See *QPP 6* – ***Use and disclosure with consent*** and ***Key Privacy Concepts – consent*** for more information.

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

An agency can disclose personal information where it is required or authorised by law. This aligns with QPP 6.2(b). If an agency is permitted to disclose under 6.2(b), it will be able to disclose overseas under section 33.

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 disclosure of the personal information, meaning the agency cannot refuse to disclose it, or it may simply **authorise** the disclosure, meaning the agency has a discretion to disclose 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 disclosing the personal information.

See ***QPP 6 – use or disclosure authorised or required by law*** for more information.

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

Agencies can disclose personal information overseas to prevent or lessen a threat, but there must be a sufficient link between the disclosure and the prevention or lessening of the threat. Disclosure in these circumstances would generally be to an entity with the capacity and authority to act on the threat.

This aligns with QPP 6.2(c), Permitted General Situation (PGS) 1(a). If an agency is permitted to disclose under 6.2(c), PGS 1(a), it will be able to disclose overseas under section 33.[1]

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 disclosures, even if those disclosures are intended to reduce serious threats to life or health.

See ***QPP 6 – use or disclosure to lessen or prevent a threat*** for more information.

Disclosure under section 33(d)

Section 33(d) allows personal information to be disclosed to an entity outside Australia if **any two or more** of the following apply. Unlike the rest of section 33, it does not align with QPP 6. Agencies must identify what provision of QPP 6 permits the disclosure generally before relying on 33(d).

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

[1] Note there is an additional requirement in 6.2(c), PGS 1(1) that it must be impracticable or unreasonable to obtain the individual's consent. While this does not apply to section 33(c), it is best practice to seek consent where it is practicable to do so.

effectively upholds principles for the fair handling of personal information that are substantially similar to the QPPs.

There are three parts to 33(d)(i):

- What kind of fair handling principles apply to the entity
- Are they capable of being effectively upheld; and
- Are they substantially similar to the QPPs.

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 of the overseas jurisdiction to determine if this section applies.

What kind of fair handling principles apply to the entity

The entity must be subject to fair handling principles which are contained in a law, binding scheme, or contract. These could include where the entity is:

- 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; or
- a bound contracted service provider under section 35.

The entity 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 disclosed 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 disclosed information
- the agreement is unenforceable at law.

Can the principles be effectively upheld

The fair handling principles which apply to the entity must be capable of being effectively upheld. This includes where:

- the fair handling principles can be enforced; and

- individuals have rights they can exercise if the principles are breached.

It may be necessary to undertake a detailed examination of the fair handling principles and their framework to determine the extent to which they are capable of being upheld. Mechanisms which allow the individual to seek redress against the entity in the event of a breach are an important part of establishing this. Principles with no provision for compliance, investigations, complaints, or an obligation to comply will generally not be considered capable of being effectively upheld.

Where a contract is being relied on, it may be challenging to determine if its fair handling principles can be effectively upheld. If the recipient is a bound contracted service provider under section 35, and the service arrangement is a contract, the principles are more likely to be capable of being effectively upheld.

However, where the entity is not a bound contracted service provider, this section may be difficult to satisfy. The individual whose information is being disclosed is not a party to the contract, which means they have no right to take action under the contract if the entity breaches its fair handling principles.

Contractual provisions which may make the fair handling principles capable of being upheld include those which:

- 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; and
- require the entity to take appropriate steps to promote compliance within the entity body.

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

Whether there is a substantial similarity between the QPPs and the fair handling principles is a question of fact, to be determined taking into consideration all the circumstances.

Agencies should compare the QPPs with the other overseas requirements and assess the importance of any similarities or differences, taking into account the relevant QPPs and the objects of the IP Act.

Some minor variation between the two is acceptable, but the principles binding on the entity cannot be significantly weaker than the QPPs.

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

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

Disclosure under this section does not need to benefit the individual. Some functions of an agency which relate 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 disclosure of personal information must be necessary for the performance of the function, and the function must relate to the individual.

Necessary

When considering whether the disclosure 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 disclosing the personal information that would not be significantly more onerous, it may be difficult to satisfy this section.

The agency's functions

The disclosure must relate to the functions of the agency that is disclosing the information, not the function of the entity 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 disclosure 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.

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 disclosed

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 disclosed must fall within the function, even if disclosing 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 disclosing personal information to the service provider's servers in another country.

Agency D wants to disclose 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 disclosed, because the function relates only to those officers.

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

> *the disclosure 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.*

In order to satisfy this section, the disclosure must be for the benefit of the **actual** individual that the information is about. The disclosure 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 disclosure 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.

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 discloses will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the QPPs.*

If the agency has taken reasonable steps to ensure that the information being disclosed will not be handled contrary to the QPPs, this section

will be satisfied. 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, but information can only be *disclosed* if the agency ceases to have control of it. This may limit the actions an agency can take and when it can take them.

Agencies should take the reasonable steps required by section 33(d)(iv) before the information is disclosed. The steps can be technical, practical, or administrative, and need not be legally enforceable. What steps are reasonable will depend on the circumstances and the nature of the personal information.

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

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

Published 12 June 2024 and Last Updated 5 June 2024