information and privacy commission new south wales

Fact Sheet **Updated November 2019**

Guidance: Transborder Disclosure Principle – section 19(2)

Privacy and Personal Information Protection Act 1998

This Fact Sheet is prepared under s 36(b) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) which provides the Privacy Commissioner with a general function "to prepare and publish guidelines relating to the protection of personal information and other privacy matters, and to promote the adoption of such guidelines".

The PPIP Act s 19(2) sets out requirements when agencies are disclosing non-health 'personal information' to a recipient who is a Commonwealth agency, or who is outside the NSW jurisdiction.[1]

Transborder rules

Any disclosure must first meet the applicable standard disclosure rule (or an exemption to that rule); and then, if the disclosure is going to a recipient who is outside the NSW jurisdiction (or to a Commonwealth agency within NSW), it must *also* meet the additional criteria set under the applicable transborder rule (or an exemption to that rule).

The standard disclosure and transborder rules differ, depending on the type of 'personal information' at issue. The inter-relationship between the different disclosure rules is outlined in the table below:

Type of personal information	Standard disclosure rule	PLUS: Additional rule if recipient is outside the NSW jurisdiction or a Commonwealth agency
Health information[2]	HPP 11	HPP 14
Sensitive information[3]	s19(1) PPIP Act[4]	s19(2) PPIP Act
Non-health, non-sensitive personal information	s18 PPIP Act	s19(2) PPIP Act

For example, the disclosure of financial information (which is neither 'health information' nor 'sensitive information') to a recipient in another country would first need to satisfy s18 of the PPIP Act (or be able to claim an exemption to s 18), and then *also* s 19(2) of the PPIP Act (or be able to claim an exemption to s 19(2)).

What does the transborder principle require?

Section 19(2) provides a number of grounds under which a transborder disclosure can be made. The full text of s 19(2) is in Attachment A.

Satisfying s 19(2)(a): subject to a law, binding scheme or contract

The Privacy Commissioner does not determine which other jurisdictions might be considered to offer "a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles."

The rationale for this decision is that if there is a similar privacy law in another jurisdiction, the recipient may not be bound to comply with that law due to specific exemptions. Recipients might decide to later opt out of a self- regulatory binding scheme. Further, judgments as to the adequacy of privacy rules applying to another organisation can be subject to disagreement from the courts.[5]

Agencies must make their own enquiries on a case-by-case basis, and where necessary seek legal advice.

The Privacy Commissioner urges caution when seeking to rely on this provision.

Satisfying s 19(2)(b): express consent

Consent cannot be a condition of receiving a good or service from an agency. If a person has no practical alternative but to provide certain information in order to receive a service, an agency should not suggest they are seeking the person's consent.[6] In these circumstances the agency must still be open about how it will handle a person's information by notifying the person about relevant matters when it collects their information (s 10 of the PPIP Act).

Express consent means consent that is clearly and unmistakably communicated.[7] It must be *"precise as to*

the kind and, possibly, the exact contents of the information to which the consent relates".[8]

This provision requires the subject of the information to expressly consent to the disclosure being made *to a recipient in a jurisdiction outside NSW*. This is distinct from any consent obtained to make the disclosure in the first place (e.g. in order to comply with s 18). This would likely require the individual to first be warned that the recipient is outside the NSW jurisdiction, and might *not* be bound by privacy principles that could be enforced by the individual.

Satisfying s 19(2)(c) or (d): necessary for a contract

Even if the subject individual has entered into a contract with the agency which necessitates disclosure to a recipient who is outside the NSW jurisdiction, notice to the individual should have been provided under s 10 of the PPIP Act, prior to entering the contract, that such a disclosure is likely to take place.

Satisfying s 19(2)(e): benefit the individual, but impracticable to obtain consent, and if notified would likely consent

NCAT has found that 'impracticable' means "impossible in practice".[9]

The fact that seeking consent is inconvenient or would involve some effort or expense is not of itself sufficient to warrant it 'impracticable'.

Some examples of where it might be impracticable to seek consent include if:

- the subject is deceased, or
- the age and / or volume of the information is such that it would be very difficult or even impossible to track down all the individuals involved, or
- there are no current contact details for the individuals in question and there is insufficient information to get up-to-date contact details.[10]

Satisfying s 19(2)(f): necessary to lessen or prevent a serious and imminent threat

This provision is to be narrowly construed, and only permitted in very limited circumstances.[11]

Any threat must be both 'serious' and 'imminent'. A 'serious' threat could include a potentially life-threatening situation, or one that might result in an illness or injury without timely decision or action.[12] 'Imminent' means "likely to occur at any moment; impending".[13]

The proposed disclosure must also be 'necessary' to prevent the threat from being realised. The decision should be based on whether the proposed disclosure will lead to the intended outcome, that is, whether disclosure will lessen or prevent a serious threat.[14]

Satisfying s 19(2)(g): take reasonable steps

Exactly what will constitute 'reasonable steps' will differ according to the nature of the personal information, the risk of harm to the individual if there is a breach, and the safeguards already offered by the recipient.

However, it is expected that at a minimum, this provision would require a public sector agency to enter into an enforceable contract with the recipient, with at least the following features:

- a requirement on the recipient to handle the personal information in accordance with the IPPs in relation to its collection, storage, use, disclosure and data retention
- a mechanism by which the public sector agency can enforce these terms against the recipient if necessary
- a mechanism for handling or referring privacy complaints
- a mechanism for handling data breaches, including notification to the agency, and
- a requirement on the recipient to bind any sub-contractors to the same terms.[15]

Additional steps that might be appropriate could include requiring the recipient to provide evidence to the agency of the way in which the recipient's personnel (and any sub-contractors) have been made aware of their privacy obligations, or the conduct of site visits or audits of the recipient's information handling practices.

Satisfying s 19(2)(h): permitted or required by law

This provision is similar in terms to the exemption found at s 25 of the PPIP Act If another NSW or Commonwealth statute, or the order of a court or tribunal such as a subpoena,[16] specifically requires or authorises a disclosure to take place, that other law will override the general prohibition against disclosure in s 19(2).

What exemptions are there to the transborder principle?

As with most of the IPPs, there are numerous exemptions to s 19(2). These may be found elsewhere in the PPIP Act, in the PPIP Regulation, in Privacy Codes of Practice, or in temporary public interest directions made by the Privacy Commissioner.

Examples include the 'other law' exemption at s 25 of the PPIP Act, and the research exemption at s 27B of the PPIP Act.

Note that there are some exemptions which relate only to s 18, or only to s 19(1), which will not assist in relation to s 19(2). Examples include the exemption relating to investigative agencies at s 24 of the PPIP Act, and the exemption relating to credit information at s 27C of the PPIP Act.

Is outsourcing to a cloud storage provider affected by the transborder principle?

The transborder rule only applies to *disclosure*, not *use*. The provision of personal information to a contracted cloud data storage provider may be considered a 'use', rather than a 'disclosure', so long as certain conditions are met.

In a discussion about privacy responsibilities when considering the use of cloud computing, the NSW Government *Cloud Policy* states:

"The collection, storage, access, use and disclosure of personal information is governed by PP/PA and HR/PA. Where the use of cloud computing requires the transmission or storage of personal information, including health information, agencies must ensure that their arrangements comply with relevant privacy and disclosure requirements. ...

If an agency shares with or transfers personal information to a contracted cloud service provider and the cloud service provider simply holds the data and acts according to the instructions of the agency, ***then disclosure will not be considered to have occurred****. If the cloud service provider uses the data provided for its own purposes, this may be unauthorised access, use, modification or disclosure".*[17] *(emphasis added)*

A similar view has been expressed by the Australian Privacy Commissioner, in the context of the equivalent federal 'transborder disclosure' privacy principle.[18]

As a general rule

When in doubt about its ability to comply with any of the other criteria set out in s 19(2), a public sector agency seeking to disclose non-health personal information to a Commonwealth agency, or to a recipient who is outside the NSW jurisdiction, should follow s 19(2)(g), and take reasonable steps to ensure that the information that it plans to disclose will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles.

As noted above, the 'reasonable steps' would at least include contractual arrangements.

Disclaimer

This document is intended as a guide for public sector agencies regulated by the *Privacy and Personal Information Protection Act 1998* (NSW) (the PPIP Act), as to the Privacy Commissioner's views on the interpretation of sections 18 and 19.

This guide is not legally binding, and does not constitute legal advice. Agencies should also be guided by interpretations of the PPIP Act by the NSW Civil & Administrative Tribunal (NCAT) and higher courts, and by their own legal advice.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.

---

[1] It is the location of the recipient, rather than where the disclosure occurs, that is the pertinent fact in determining whether this section applies; see *Bevege v Commissioner of Police, NSW Police Force* [2014] NSWCATAD 22.

[2] As defined at s.6 of the HRIP Act

[3] Sensitive information is information about "an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities"; see s.19(1) of the PPIP Act.

[4] Section 19(1) "overrides s.18(1)(c) if one of the categories of sensitive information mentioned in s 19(1) is in issue". *Director General, Department of Education and Training v MT* (GD) [2005] NSWADTAP 77 at [73].

[5] For a summary of the unravelling of the 'Safe Harbor' binding scheme, which had been relied on by multinational companies for the past 15 years to authorise transborder disclosures from the European Union to the United States, see http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection, accessed 21 October 2019.

[6] Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004, p.7.

[7] Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004, p.10; see also Privacy NSW, *Handbook to Health Privacy*, 2004, part 1.3.

[8] Vice Chancellor, *Macquarie University v FM* (GD) [2003] NSWADTAP 43 at [97].

[9] *ALZ v WorkCover NSW* [2014] NSWCATAD 49.

[10] Privacy NSW, *Statutory Guidelines on Research*, 2004, pp.8-9.

[11] *MT v Director General, NSW Department of Education & Training* [2004] NSWADT 194 at [195].

[12] Information and Privacy Commission NSW, *Use and Disclosure of Genetic Information to a Patient's Genetic Relatives: Guidelines for organisations in NSW*, October 2014, p.4

[13] *FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78 at [56].

[14] Information and Privacy Commission NSW, *Use and Disclosure of Genetic Information to a Patient's Genetic Relatives: Guidelines for organisations in NSW*, October 2014, p.4

[15] This expectation is in line with the Australian Privacy Commissioner's guidelines on interpreting the equivalent federal transborder disclosure provision; see Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.0, February 2014, para 8.15.

[16] *AYT v Sydney Local Health District* [2014] NSWCATAD 29.

[17] NSW Government, digital.nsw, *Cloud Policy*, April 2018, Version 2.1, p.8; available from https://www.digital.nsw.gov.au/sites/default/files/Cloud%20Policy%20%28for%20publication%29-%20April%202018.pdf, accessed 13 November 2019.

[18] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.0, February 2014, para 8.14.

Checklist: Transborder Disclosure Principle – s 19(2)

Am I intending to disclose information outside the NSW jurisdiction?

No ↓

Section 18 Limits on disclosure of personal information applies.

Yes ↓

Does an exemption under s 19(2) apply to allow disclosure of the personal information? ↓

Section	Question	Things to consider in making decision:
s 19(2)(a)	Is the intended recipient subject to a law, binding scheme or contract that would be substantially similar to NSW privacy laws?	**Is the recipient subject to a law or binding scheme?** ☐ Is the recipient bound by a privacy or data protection law that applies in the jurisdiction of the recipient or subject to a scheme or privacy code that is enforceable? OR ☐ Is the recipient exempt from complying, or is authorised not to comply, with part, or all of the privacy or data protection law in the jurisdiction? ☐ Can the recipient opt out of the binding scheme without notice and without returning or destroying the personal information? **Is the law or scheme substantially similar?** ☐ Does the law or binding scheme the recipient is subject to provide a comparable level of privacy protection as NSW privacy laws such as comparable definition of personal information, rules regarding collection and disclosure of personal information, right of access, etc? (the IPPs useful baseline for this review) **Is the law or scheme enforceable?** ☐ Is the privacy protection mechanism accessible to the individual whose information is being shared? ☐ Are NSW citizens able to enforce their rights in the jurisdiction? o What access to justice do NSW citizens have if their privacy is breached in the recipient's jurisdiction? o Is there an equivalent of the NSW Civil and Administrative Tribunal? o Do citizens from NSW have standing in the jurisdiction or is residency a requirement? o What is the process for return or destruction of personal information if the regime is no longer deemed equivalent?
s 19(2)(b)	Is there express consent from the individual to release the information?	☐ Is there a clear oral or written statement of consent in relation to disclosure of information *to a recipient in a jurisdiction outside of NSW*? ☐ Is the consent informed, made voluntarily and not as a condition of receiving a good or service from an agency? ☐ Has the individual been notified about the consequences of having their information disclosed to a recipient outside NSW? ☐ Has the individual at any time withdrawn their consent to make a transborder disclosure of information?

Section	Question	Things to consider in making decision:
ss 19(2)(c) and (d)	Is disclosure necessary for performance of a contract/or pre-contractual measures in the interests of the individual?	☐ Was/will a contract be entered into between the individual and the agency for services? OR ☐ Was/will a contract be entered into between the agency and a third party in the interest of the individual? ☐ Is there a specific provision in the contract that requires, or grants discretion to, the agency to disclose the type of personal information? ☐ Has a notice been provided to the individual prior to entering the contract that a disclosure to a recipient outside NSW is likely to take place? ☐ Does the fulfilment of the contract or a pre-contractual term require information to be disclosed to another jurisdiction?
s 19(2)(e)	Is disclosure of benefit to the individual?	☐ In disclosing the information to another jurisdiction will the individual obtain a benefit from this disclosure? ☐ Is it impracticable to obtain the consent of the individual to that disclosure? (examples have been provided in the main body of this Fact Sheet) ☐ Would consent likely to have been given (in the general course of events given the benefit it would be unlikely that consent would be withheld)?
s 19(2)(f)	Is disclosure necessary to lessen/prevent a serious and imminent threat?	☐ Is there a serious and imminent threat? ☐ Will the disclosure of information prevent a serious and imminent threat (e.g. prevent death, serious injury or illness)?
s 19(2)(g)	Have reasonable steps been taken?	☐ What is reasonable in the circumstances? Consider: ○ The nature and sensitivity of personal information ○ The agency's previous relationship with the recipient and whether there has been disclosure in the past ○ Possible consequences for an individual if the information is mishandled ○ Existing safeguards implemented by the recipient to protect the privacy of the disclosed information ☐ Have contractual arrangements been entered into with the recipient? (Suggested in the body of the Fact Sheet)
s 19(2)(h)	Is the disclosure permitted or required by law?	☐ Is the disclosure required or permitted by another law, whether a NSW law or a law of the recipient's jurisdiction? ☐ Is the disclosure required by a legal instrument (such as a court or a subpoena) issued in NSW, or, in the recipient's jurisdiction showing an intention to have effect in NSW?

ATTACHMENT A

S19(2) PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998

A public sector agency that holds personal information about an individual must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the public sector agency reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles, or

(b) the individual expressly consents to the disclosure, or

(c) the disclosure is necessary for the performance of a contract between the individual and the public sector agency, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the public sector agency and a third party, or

(e) all of the following apply:

  (i) the disclosure is for the benefit of the individual,

  (ii) it is impracticable to obtain the consent of the individual to that disclosure,

  (iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the disclosure is reasonably believed by the public sector agency to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or

(g) the public sector agency has taken reasonable steps to ensure that the information that it has disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles, or

(h) the disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law.