

# Mitigating third-party provider cybersecurity risks: navigating the Australian legal framework

 FROM OUR BLOG

A&O Shearman on data

---

**READ TIME**

 7 mins

**PUBLISHED DATE**

 Aug 4 2025

Cybersecurity breaches originating from third-party providers (TPPs) are an escalating concern for Australian businesses. As supply chain risks grow, there is a mounting public expectation that the entity that commissioned the collection of personal information remains accountable for its protection, even when such personal information is handled and managed by a TPP.

Despite recent political commentary in Australia regarding the tightening of privacy laws, there is no current legal requirement for businesses to store data, including any personal information, in-house. As a result, organizations

are increasingly relying on TPPs to manage their data as TPPs can be highly cost-effective and often provide superior specialist services. To maximize the benefit of using TPPs, robust legal risk management is essential.

## Ministerial misstatements on outsourcing cybersecurity obligations

Recent statements by government officials have highlighted a misconception regarding liability for cybersecurity obligations. The minister for cybersecurity, the Hon Tony Burke MP stated that:

“[Y]ou can’t outsource your cyber security obligations. Your obligations to your customers, the people who work with you, all the data that you hold, the obligation is the same. And so if you choose to outsource in some way... no business should think that they are then outsourcing their obligation... The obligation is probably... more complex when you start using more third-party companies. And that’s something that needs to be borne in mind.”<sup>1</sup>

Similarly, shadow minister for cybersecurity, the Hon Melissa Price MP said that companies should reconsider whether they use third parties to store data:

“Although the use of third-party platforms might be common practice for many businesses, surely the time has come for valuable data to be stored in-house.”<sup>2</sup>

Although politically newsworthy, these statements reflect an inaccurate understanding of the current legal framework and business realities. While there may be an increasing public expectation that the original data collector remains responsible, legally, in Australia the responsibility for TPPs is more nuanced and not absolute. However, these comments may signal an interpretative shift of the Privacy Act 1988 (Cth) (Privacy Act) and may also foreshadow legislative reform.

## The Australian regulatory framework

Under the Privacy Act, APP entities<sup>3</sup> must comply with the Australian Privacy Principles (APPs). Two principles are particularly relevant to TPP risk:

- ◆ APP 11 (Security of Personal Information) requires an APP entity to take reasonable steps in the circumstances to protect personal information from misuse, interference, loss, unauthorized access, modification or disclosure.<sup>4</sup>
- ◆ APP 8 (Cross-Border Disclosure) requires an APP entity to take reasonable steps to ensure the overseas recipient of personal information does not breach the APPs.<sup>5</sup>

APP 11 does not specifically reference TPP arrangements, and the prevailing view has been that if a TPP is itself an APP entity, the primary entity is not liable for the actions of that TPP, provided the primary entity itself complies with the APPs. Unlike the European Union's General Data Protection Regulation (GDPR), which distinguishes between controllers and processors (and applies stricter obligations on controllers), the Privacy Act applies the same obligations to both entities.<sup>6</sup>

Currently, only APP 8 imposes explicit liability on APP entities for the actions of TPPs. Liability can still arise for a collecting entity if an overseas party with no Australian link mishandles data, under s 26WC of the Privacy Act.

Further, the new statutory tort<sup>7</sup> for serious invasion of privacy, in force since June 10, 2025, has increased the risk landscape. It provides individuals with a direct legal avenue for redress in the event of a serious privacy breach, separate from the APP regime. Such a claim has yet to be made in court.

## Potential for regulatory change: interpretation and reform

These political statements and recent regulatory action indicate a strong trend towards greater accountability for TPP arrangements. The Government's Response to the Privacy Act Review Report<sup>8</sup> from 2023 (Government Response to the Review Report) further demonstrates an intention to tighten privacy laws.

The Privacy and Other Legislation Amendment Act 2024 (Cth) introduced the first tranche of reforms to the Privacy Act, including the new APP 11.3 which came into force on June 10, 2025. APP 11.3 requires all APP entities to implement "technical and organizational measures" as part of their obligation to take "such steps as are reasonable" to protect personal information. This has clarified that the interpretation of APP 11.1's "such steps as are reasonable in the circumstances" goes further than just "technical measures."

However, the scope of "organizational measures" has yet to be tested in court. It is arguably open to the interpretation that liability extends to TPPs. It could be argued that "organizational measures" covers contracts and contracting processes such as due diligence and could go so far as active TPP oversight both throughout the duration of the contract and upon its completion.

The possibility of a broad interpretation of APP 11 is not far-fetched. In the recent case Commissioner Initiated Investigation into Regional Australia Bank Limited (Privacy) [2025] AICmr 89, the privacy commissioner found that Regional Australia Bank (RAB) was liable for privacy breaches arising from a software fault caused by its TPP, Biza Pty Ltd (Biza). The commissioner determined that RAB was liable for Biza's conduct under s 84(2) of the Competition and Consumer Act 2010 (Cth) (Competition and Consumer Act). Despite the finding that RAB could not have done more to protect itself, RAB was held liable due to the agency implications of s 84(2).

Although this case related to the Competition and Consumer Act, and the Privacy Act has no similar agency provision, the case demonstrates the OAIC's willingness to try to attribute liability to organizations for TPP failings. It is arguable the OAIC could similarly interpret the APP 11.3 requirements to hold businesses liable for TPP actions, if an entity fails to act reasonably in its contracting, due diligence and even TPP management processes.

The government has not announced when the next tranche of reforms from the Government Response to the Review Report will be implemented. However, in light of the growing seriousness and frequency of supply chain data breaches, there is a real possibility of rapid [knee-jerk] legislative reform.

A further proposal that may be implemented from the Government Response to the Review Report is Proposal 22.1, which suggests including a GDPR-like controller and processor distinction. This was agreed to in principle. Under the GDPR, processors are required to have a security standard “appropriate to the risk.”<sup>9</sup> In a recent interview,<sup>10</sup> Carly Kind, the Australian privacy commissioner, stated that proposed changes to Australia’s privacy laws will bring them closer to the GDPR, but may go even further with the proposed “fair and reasonable” test.<sup>11</sup> This test would require APP entities to demonstrate that their “collection, use and disclosure”<sup>12</sup> of personal information is objectively fair and reasonable, moving away from a model that relies primarily on individual consent. There is a question of whether a fair and reasonableness test of “use and disclosure” of personal information, encompasses an entity’s dealings with a TPP.

The commissioner’s recent determinations and commentary signal a continued shift towards greater accountability for businesses and individuals’ control over their personal information.

Additionally, the financial services industry provides examples of higher standards, often exceeding those required by the Privacy Act. The Australian Prudential Regulation Authority (APRA)’s standards CPS 234 and CPS 230, specifically address third party cyber risks and mandate robust information security and operational risk management practices. These provide a framework that other industries or the general legislation may choose to follow.

## Best practice: how to get ahead

In both the current and anticipated regulatory environment, supply chain risk is one of the biggest threats to Australian businesses. Existing contracts that businesses have in place with TPPs may not provide sufficient protection from liability. For many, exclusive in-house data storage is neither practical nor economically viable. Most organizations lack the resources and expertise to maintain the same level of security as specialist providers.

Our view is that best practice in TPP risk management covers the entire vendor lifecycle, including the following:

- ◆ Due diligence processes: involving thorough assessment of potential vendors, including their security posture and compliance history
- ◆ Vendor onboarding: establishing clear service level agreements (SLAs), secure system integration, and initial security testing
- ◆ In-flight governance: regular monitoring of data retention and deletion practices, key performance and risk indicator reporting, audits and remediation planning, and annual penetration testing.
- ◆ Offboarding: ensuring clear data migration and deletion requirements, access management, and termination of SLAs

With the right processes and contracts in place, businesses can better protect themselves and their customers from TPP cyber risks, noting that no system is infallible. Now is the time for organizations to assess their current TPP risk management frameworks, identify any gaps, and implement improvements where necessary.

## Footnotes

1. <https://minister.homeaffairs.gov.au/TonyBurke/Pages/tv-interview-abc-afternoon-briefing-02072025.aspx>.

2. <https://www.afr.com/companies/transport/qantas-boss-vanessa-hudson-says-hackers-too-good-for-its-defences-20250704-p5mcjd>.

3. Section 6 of the Privacy Act 1988 (Cth) defines APP entity.

4. Australian Privacy Principle 11, Schedule 1 of the Privacy Act 1988 (Cth).

5. Australian Privacy Principle 8, Schedule 1 of the Privacy Act 1988 (Cth).

6. It has been proposed to implement a similar distinction in the Privacy Act 1988 (Cth); however, this has only been “agreed to in principle.” See Government’s Response to the Privacy Act Review Report, Proposal 22.1.

7. Schedule 2 of the Privacy Act 1988 (Cth).

8. <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.

9. Article 32 of the General Data Protection Regulation (EU) 2016/679.

10. <https://www.themaybe.org/podcast/regulating-privacy-in-an-ai-era-w-carly-kind>.

11. <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>, page 8.

12. <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>, page 8.

## Related capabilities

Data privacy and data protection

Cybersecurity

### SUBSCRIBE

## Interested in this content?

Sign up to receive alerts from the A&O Shearman on data blog.

**SIGN UP** →

**Register or update your preferences**



