The Australian Privacy Commissioner is not waiting for another reform

Australian data privacy is at crossroads. The newish Privacy Commissioner has a clear vision. With the new enforcement powers granted to her in the first of several promised reform packages late last year and with an increased budget, the Office of the Australian Information Commissioner (**OAIC**) is well equipped to pursue that vision.

Australian data privacy is a relatively complex set of general and sectoral laws at federal and state level. At its core are the Australian privacy principles which somewhat resemble those in the European General Data Protection Regulation (**GDPR**).

The Privacy Commissioner recently explained her strategic focus in using enforcement action to advance data privacy jurisprudence in courts and give more specific guidance back to entities about exactly what the law requires. In other words, the Commissioner is putting meat on the bone of the principle-based law, to match the rising expectation of the public and emerging good practices in corporate governance.

This will result in a cultural change in how data privacy compliance is perceived by boardrooms across Australia, which remain dominated by ill-informed defensive compliance approaches and misguided resistance by business leaders. This is all about the change.

Consent not essential

Consent (or rather implied consent) is often seen as the prevalent basis for the handling of personal information under the Privacy Act 1988 (Cth). However, in a recent interview,[1] the Privacy Commissioner described the Privacy Act as unique and "*not heavily contingent on consent the way the GDPR is*". The Commissioner sees this as a positive feature rather than a weakness of the privacy regime. In her view, consent is overused and it often fails to provide effective protection to individuals.

In fact, Australian law requires consent only in specific circumstances, for example, to use sensitive personal information, send unsolicited direct marketing or to use personal

[1] Australian Privacy Commissioner Carly Kind breaks down new rules in Australia's Privacy Act, Vision by protiviti, April 2025 (link).

information for a new purpose. In other situations, for example, if data use could be seen as unfair, it is prudent to collect consent to mitigate the risk of non-compliance. However, seeking blanket consent for all data use or incorporating consent in a privacy policy will do little to advance an organisation's legal compliance or the data privacy of individuals.

Necessity and fairness

Instead, "necessity" and "fairness" protect the individual from excessive data use. This resembles a human rights approach and indeed Australia's data privacy is founded on the commitments under the International Covenant on Civil and Political Rights 1966. The Commissioner has elaborated on these concepts in recent OAIC determinations.

An organisation must not handle personal information unless this is "necessary" for its functions or activities. In a recent determination, referring to the objects of the Privacy Act, the Commissioner reiterated the requirement for each organisation to balance its interests and peoples' rights where there may be a conflict.[2] Accordingly, to establish "necessity", the proposed data use and the benefits gained must be proportionate to any necessary interference with peoples' rights.

Another requirement is "fairness". Certainly, any personal information obtained by deception or in an intrusive way, will not be fair. However, fairness is an open-textured and evaluative criterion which should be construed beneficially as per the Privacy Act's objects.[3] A person's reasonable expectations and any impact on the individual will play a role in the assessment of when specific data use may or may not be fair. Any data collection from public sources in breach of the underlying terms and conditions could be unfair and unlawful.[4]

With these requirements Australian data privacy aligns with some of the most advanced data privacy regimes, such as the GDPR.

Regulatory strategy underpinned by new enforcement powers

The recent reform granted the Privacy Commissioner significant monitoring and investigatory powers under the Regulatory Powers Act 2014. Subject to a warrant issued by a judicial officer, entry, search, examination, testing, recording, operating equipment,

---

[2] Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy) [2024] AICmr 230 (29 October 2024).
[3] Commissioner Initiated Investigation into Master Wealth Control Pty Ltd t/a DG Institute (Privacy) [2024] AICmr 243 (18 November 2024).
[4] AHM' and JFA (Aust) Pty Ltd t/a Court Data Australia (Privacy) [2024] AICmr 29 (12 February 2024).

and seizure are some of the investigatory tools available to the Commissioner in investigating an offence or civil penalty under the Privacy Act and various other laws.

Until now, the Commissioner has rarely enforced civil penalties under the Privacy Act. However, the lower tiers of civil penalties introduced in the recent reform make it significantly easier to issue penalties for technical infringements and non-serious interference with data privacy. Penalties are no longer reserved for serious and repeated contraventions.

Small infringements such as the lack of a compliant privacy policy may attract the streamlined infringement notice procedure yielding a penalty of up to AUD$66,000. The Commissioner calls this an exciting development. Any excessive data collection or data use for a secondary purpose without obtaining prior consent will likely attract the mid-tier penalties of up to AUD$660,000. A lack of systems and procedures in place or a lack of staff training would also sit under this penalty tier. Serious interference with privacy could attract penalties of up to the greater of AUD$50m, 3 times the benefit or 30% of adjusted annual turnover for corporates.

Future developments

The Commissioner is not hung up on any further data privacy reform, which may or may not happen. A lot can be done without it. But one of the services she is hoping to provide in future, if supported by a legislative mandate, is to offer an innovation or advice hotline where organisation can sense-check their compliance approaches to new data privacy problems.

In the meantime, the Commissioner will focus on shaping the Australian compliance culture with a new enforcement posture, focusing on education and awareness-raising rather than any punitive objective. She welcomes the growth of the Australian privacy community and with it, the increase in good privacy practices.

Next steps

Broadly displaying good governance will likely put organisation in a good compliance position. However, Australian data privacy is unique and deserves separate attention.

The necessary compliance steps and documentation will depend on the circumstances of each organisation, but, by way of example, these might include:

- **Data privacy governance**
- **Compliance plan**

- **Privacy assessments**
- **Data Privacy Policy** as an internal guideline
- **Staff training**
- **Staff Privacy Policy**
- **Data rights and complaints procedure**
- **Information security policy**
- **Acceptable use policy**
- **Contracts** such as data sharing agreement, client terms, employment contracts, service agreements, etc., with appropriate data privacy clauses
- **Due diligence**, for example, on inbound technology services
- **Privacy Policy and Fair Collection Notice(s)** (published)
- **Monitoring and audits**
- **Other reasonable practices, procedures and systems**