Office of the Victorian Information Commissioner

Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

25 September 2025

5 Pillars Team
The Productivity Commission

By email only: 5pillars@pc.gov.au

Dear 5 Pillars Team,

Thank you for the opportunity to make a submission to the Productivity Commission's (**PC**) consultation on the 5 Pillars interim reports.

The Office of the Victorian Information Commissioner (**OVIC**) is a Victorian integrity agency with oversight of privacy, freedom of information and information security in Victorian Public Sector (**VPS**) organisations. This oversight is enabled by both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

OVIC's submission will address 2 of the 5 pillar interim reports: Harnessing data and digital technologies (**data interim report**) and Building a skilled and adaptable workforce (**workforce interim report**) and will cover the following:

- Improving understanding of privacy regulation in Australia, and its relationship with productivity and innovation
- Evaluating the proposed compliance pathway against existing privacy regulation
- Data sharing and information governance practices
- Artificial intelligence (**AI**)
- The use of educational technology (**edtech**) and generative artificial intelligence (**genAI**) in schools.

If you would like to discuss this submission any further, please contact Fathia Tayib, Senior Policy Officer, via fathia.tayib@ovic.vic.gov.au.

Yours sincerely

Sean Morrison
Information Commissioner

OVIC submission to the Harnessing data and digital technology interim report

Privacy regulation in Australia

The primary privacy regulation in Australia is the *Privacy Act 1988* (**Privacy Act**), administered by the Office of the Australian Information Commissioner (**OAIC**).

There are 13 Australian Privacy Principles (**APPs**) in the Privacy Act. The APPs govern how federal public sector agencies and private sector organisations with an annual turnover of $3 million or more must collect and handle personal information. The APPs are generally considered to be flexible principles and outcomes-based.

With the exception of South Australia,[1] each of Australia's states and territories have also enacted privacy legislation that applies to their respective public sectors. While there are some differences between Australia's privacy laws, each contain privacy principles similar to those in the Privacy Act.

Privacy as a human right

OVIC notes that the data interim report appears to place the interests of businesses ahead of the human right to privacy. Privacy is recognised as an individual human right globally.[2] In Victoria, the right to privacy is listed under section 13 of the *Victorian Charter of Human Rights and Responsibilities Act 2006*.

Privacy is not limited to information privacy. Information privacy relates to how an individual can, in certain situations, determine for themselves when, how and for what purposes their personal information is handled by others. The right to privacy also includes the freedom from intrusion and interference.

Privacy is critical to the realisation of other human rights, such as freedom of expression, freedom of thought and freedom from discrimination. The right to privacy is not absolute. Some limitations are permitted where they are reasonable and justified, such as sharing personal information in the interest of public safety and welfare.[3]

The data interim report portrays the right to privacy as a potential impost on a business.[4] However, a robust privacy regime empowers individuals to care about their privacy, and in turn strengthens our

[1] South Australia's privacy regime is based in whole of government policy, rather than enacted through legislation. See the State Records of South Australia website for further information: https://www.archives.sa.gov.au/managing-information/privacy-in-south-australia.
[2] For example, see Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.
[3] For example, Information Privacy Principle 2 in the PDP Act outlines specific circumstances in which disclosing personal information is permitted.
[4] As an example, on page 54, the report lists the costs of protecting privacy, but does not consider the benefits in doing so.

democracy. Australians expect businesses and governments to handle their personal information securely and with care,[5] and proactively protecting individuals' privacy can provide an advantage to businesses.[6]

Productivity, innovation and privacy regulation

OVIC's view is that privacy regulation does not inherently stifle or hamper innovation, in the same way road rules do not prevent drivers from reaching their destination. Regulating a particular sector can enable innovation to evolve in a more responsible and sustainable manner while preventing harm.

If privacy laws are enforced well, it creates incentives and competition for new and innovative products and services that define themselves by their focus on privacy by design and being upfront and ethical in the collection, use and disclosure of personal information.

Productivity is not limited to economics – it is also linked to the health and wellbeing of society.[7] A singular focus on the economic benefits of productivity may lead to a lopsided benefit triangle between organisations, individuals and employees, where organisations are advantaged to the detriment of the other two groups.

OVIC does not share the view that the Privacy Act, and other privacy laws such as the PDP Act, prevent the use of data or the creation of innovative products. Strong privacy protections and practices are not a barrier to innovation. OVIC encourages organisations to build privacy protections into products, services and programs in a meaningful and practical way – from the outset. Privacy by design allows the evolution of processes, procedures and technology, while prioritising individuals' rights, welfare and safety.[8]

Proposed dual regulation pathway

OVIC is of the view that the Privacy Act is generally principles and outcomes-based, providing flexibility to organisations and businesses in how they take steps to protect privacy. For some aspects of privacy law, more prescriptive controls may be necessary to ensure a minimum standard of protection is achieved, so that individuals enjoy fair and equal rights.

The proposed solution to introduce an alternative compliance pathway does not seem necessary as a response to the issues with the Privacy Act identified in the data interim report.[9] The standard for privacy protection under the APPs is a minimum standard. The proposed alternative pathway may lead

[5] The Australian Community Attitudes to Privacy Survey (2023) notes that 4 in 5 Australians place a high importance on how their data is collected, used and protected when choosing a product or service. See https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023.
[6] Robert Waitman, 'Companies worldwide recognize business benefits of privacy', International Association of Privacy Professionals, 19 February 2019, https://iapp.org/news/a/companies-worldwide-recognize-business-benefits-of-privacy.
[7] 'Employee wellbeing is key for workplace productivity', Gallup, https://www.gallup.com/workplace/215924/well-being.aspx.
[8] See OVIC's guidance on privacy by design for more information: https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-by-design/.
[9] Data interim report, chapter 3.

to the erosion of the minimum standard, leading to poor privacy outcomes for organisations and individuals.

Before moving to propose solutions to overhaul existing legislation and processes, the PC may consider a review of the APPs to clearly identify which aspects of the principles they believe are overly burdensome and not achieving privacy outcomes. Where regulation does not improve privacy outcomes for individuals, and is costly for organisations, then this is a potential focus area for reform. However, the data interim report provides no irrefutable evidence that the Privacy Act is creating these issues. The report does not thoroughly identify which aspects of the APPs are both costly to implement and do not improve privacy outcomes for individuals.

Evaluating the proposed alternative pathway against the current Privacy Act and APPs

APPs

The PC's interpretation of 'outcomes-based' vs 'prescriptive' or 'controls-based' appears to misunderstand the premise and nature of the APP framework. The APPs are outcomes-based and are a mix of prescription and flexibility-based principles in how to achieve the intended outcomes of the Privacy Act.

The APPs allow individuals to understand what is expected of organisations – helping to address the potential power imbalance between companies and individuals, government and citizen.

The APPs set the standard for what we expect of government and the private sector in a healthy functioning democracy – that is, what is expected of organisations that are collecting, using and disclosing an individual's personal information.

The outcomes the APPs seek to achieve include organisations being open and transparent, making sure collection, use and disclosure of personal information is lawful, fair, reasonable, and not entirely unconstrained, intrusive or exploitative. They also seek to minimise harm to individuals, through measures such as information accuracy and security.[10]

Privacy outcomes

OVIC is concerned about the PC's position that privacy controls 'dampen innovation',[11] noting that the concept of reasonable proportionality is a key aspect to enabling organisations to innovate and achieve a legitimate purpose, while balancing the potential privacy harms to an individual.

The Privacy Act, and other privacy laws such as the PDP Act, allow organisations to innovate. However, it requires them to understand and consider privacy from the outset as opposed to viewing it as a constraint.

[10] For example, in a family violence context, it is critical that organisations are relying on accurate information when contacting victim survivors, and not disclosing information (such as their location) to perpetrators that could endanger the victim survivor.
[11] Data interim report, page 58.

Moving to an outcomes-based approach of regulation, as the PC suggests, is likely to result in a more complex environment for individuals to navigate, as there will be greater variation between organisations.

OVIC queries the notion that businesses are best placed to make privacy-related decisions in the best interests of their customers, without the structured rules to guide those decisions. Organisations currently rely on the APPs and guidance to identify best practices and standards for compliance.

OVIC notes the opportunity costs of complying with the Privacy Act mentioned in the data interim report.[12] However, it is equally important to identify the costs of not complying with privacy regulations. For example, the data interim report lightly touches on the harms that can arise from privacy breaches[13]. Furthermore, it fails to expand on the full scale of privacy harms that might impact individuals and organisations, downplaying their seriousness. Such harms can include economic loss, embarrassment and humiliation, physical and autonomy harms, discrimination, intimidation, loss of trust and reputational damage in organisations and institutions. It is not only the individuals whose personal information was compromised that suffer as a result of a privacy breach, but businesses, too.[14]

OVIC notes that the PC attributes certain issues with privacy compliance to failings of the Privacy Act. For example, businesses unnecessarily seeking consent from individuals, or providing hard to read and understand privacy policies to individuals.[15] In OVIC's view, these issues are not the fault of the Privacy Act, but rather, a poor understanding and application of the APPs by organisations. For example, the Privacy Act does not necessitate that privacy policies be written in complex language and are overly long.

The data interim report fails to mention how the proposed alternative pathway will resolve the over-compliance issue or reduce privacy concerns raised by individuals.

Right to erasure

The data interim report recommends that the government not introduce a right to erasure, given the high compliance burden that is expected for organisations, and the uncertain benefits this right would provide for individuals.[16] OVIC supports the inclusion of a right to erasure in the Privacy Act.[17] There is a strong public interest in providing individuals with the ability to make a request for the deletion of their personal information, particularly given the increasing community support for such a right.[18]

---

[12] Data interim report, pages 54-55.
[13] Data interim report, page 62, figure 3.2 (scenario 2).
[14] For example, telecommunications company Optus has experienced ongoing damage as a result of its 2022 cyber-attack: https://www.abc.net.au/news/2025-08-08/optus-sued-by-privacy-regulator-alleged-failures-22-cyber-attack/105628586.
[15] Data interim report, pages 55-57.
[16] Data interim report, page 67.
[17] See OVIC's submission to the Attorney-General's Department's Privacy Act review discussion paper, December 2021: https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf.
[18] The Australian Community Attitudes to Privacy Survey (2023) notes that 93% of Australians believe they should have a right to request a business delete personal information held about them:

However, public sector agencies are required to keep certain information due to various public recordkeeping legislative requirements. The right to erasure would need to be appropriately limited by the *Archives Act 1983* for federal public sector agencies, the *Public Records Act 1973* for Victorian public sector agencies or other relevant legislation requirements, or where the terms of services allow.

Data sharing and information governance practices

The data interim report suggests that privacy laws make it difficult for organisations to share data.[19] OVIC notes that in most instances privacy laws only regulate a subset of the information held by an organisation.[20] Privacy laws only apply to the collection, use and disclosure of personal information - they do not prevent organisations from making use of other data they hold and from using or sharing de-identified information. Privacy laws also allow for sharing personal information where it is appropriate.

OVIC is of the view that organisations should practice data minimisation and refrain from purpose creep – that is, to use the personal information it holds beyond its original intended purpose.

The data interim report fails to identify and discuss the issue of poor data governance and management by organisations. This issue prevents organisations from understanding what information they hold, being able to share data and use it within their organisations (beyond just personal information), and the uptake of new technologies, like AI. Poor data governance practices are not a result of complying with the Privacy Act. OVIC suggests that this issue warrants further examination in terms of its impact on productivity.

Artificial intelligence

The data interim report recommended a review of existing laws for potential AI-related expansions before considering the development of AI-specific laws.[21] OVIC supports the idea of reviewing existing legislation and frameworks across Australia that already apply to AI (for example, information privacy and security frameworks).

The data interim report has failed to include the cost of preparing data for use in AI tools. Many organisations hold data that is inaccurate, poorly formatted or requires extraction from legacy systems. It is unclear how many organisations are capable of the significant monetary and resource investment required to uplift their data management systems.

https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023.

[19] Data interim report, page 32.

[20] Victoria's PDP Act also includes a requirement for certain public sector organisations to ensure the security of *public* sector information. This includes, but not limited to, personal information (Part 4, PDP Act). This obligation extends to contracted service providers of an organisation.

[21] Data interim report, pages 19-20.

OVIC submission to the Building a skilled and adaptable workforce interim report

The workforce interim report briefly outlines the data privacy risks associated with edtech and genAI tools.[22] OVIC notes that some states have allowed the use of genAI in schools.[23]

OVIC is of the view that children, parents and guardians should be made aware of the risks and benefits of these tools. OVIC recommends that children and parents are provided detailed notices of collection and privacy policies outlining how their personal information is being used, disclosed, handled, stored and disposed of by schools and third-party vendors. Failure to provide this information may lead to privacy incidents or complaints. OVIC also recommends the development of age range-specific guidance on the use of genAI and edtech tools.[24]

[22] Workforce interim report, page 23.
[23] Workforce interim report, page 18, figure 1.6.
[24] See OVIC's submission to the OAIC's Children Code consultation, August 2025, https://www.oaic.gov.au/__data/assets/pdf_file/0030/255972/Office-of-the-Victorian-Information-Commissioner.PDF.