

15 September 2025

Productivity Commission

By upload

Dear Ms Wood

Interim Report on Harnessing Data and Digital Technology

The Insurance Council of Australia (Insurance Council) welcomes this important and timely work by the Productivity Commission (the Commission).

The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 85 per cent of total premium written by private sector general insurers. As a foundational component of the Australian economy, the general insurance industry employs approximately 46,000 people, generates gross written premium of \$75 billion per annum and on average pays out \$160 million in claims each working day (\$40 billion paid out per year).

The insurance industry plays a critical role in providing the financial failsafe for Australian households and businesses, which underpins the choices and investments that drive Australia's economic and productivity growth. This role as a financial failsafe means insurance touches almost every household and business across the country. Productivity enhancements delivered within the insurance system percolate through to our customers and supply chains across the economy.

The Australian economy is currently at the start of a digitisation journey and the recommendations made by the Commission are critical to informing the Government's approach to effectively supporting this transition. Insurers are regulated by four separate pieces of legislation that control how insurers collect, manage, use, store, share and govern personal information and data. We acknowledge the importance of handling personal data responsibly and are committed to ensuring integrity in the industry as emerging technologies that use data enter the market.

Below we offer our views on the Commission's interim recommendations on harnessing data and digital technology. Attached you will find more detailed responses to your consultation questions where relevant.

Artificial Intelligence

Artificial Intelligence (AI) is already being adopted across the general insurance system in response to inefficiencies, risk or uncertainties and there are further opportunities for adoption to accelerate productivity.¹ AI in general insurance serves to enhance the consumer experience, lower operational costs and mitigate risk. An uncertain or overbearing regulatory environment will pose a significant challenge to AI deployment and use, limiting benefits delivered to customers. General insurers support the Commission's interim recommendations on AI and urge the Government to leverage existing regulation where possible to manage identified risks.

Data Access Pathways

Insurers support consumers having access to data that relates to them held by businesses, and we understand the benefits accessing this data has to individuals to help them make more informed choices. There are several challenges with the rollout of the Consumer Data Right (CDR) to general insurance that should be considered in any supplementary data access pathway. General insurance

¹ [Ensuring we are better insured: How AI can improve outcomes for Australians - Insurance Council of Australia](#)

data is not transactional and often involves commercially sensitive information that is inferred to determine an asset or individual's risk profile. This data would not be interoperable or comparable between general insurers, given the differences in how insurers identify and assess risk. Insurers currently comply with a range of information management regulations that support consumers with access to their personal information and information used in determining a claim. It's unclear from the Commission's report what consumer benefits would be achieved by applying a data access pathway to general insurance. A data access pathway should therefore not be pursued in general insurance unless there are clearly identified gaps in the current information management regulatory framework, there are clear benefits identified for consumers and there is a net productivity benefit.

Outcomes based privacy regulation

Regarding the privacy regime, the Insurance Council and its members support outcomes-based regulation and support the Commission's recommendation to introduce a defence compliance pathway (similar to Option A outlined in the Commission's interim report). Introducing an outcomes-based test as a defence should act as a safety net for compliance in the case of regulatory action, rather than being added to the legislation as an additional requirement. Insurers support consumers' rights to privacy but note that the Commission has identified that some of the proposals relating to Tranche 2 of the *Privacy Act 1988* reforms are open to being implemented in an overly prescriptive manner. Insurers support the Commission's recommendation not to pursue a right to erasure and would like all remaining recommendations from the Privacy Act Review to be reassessed to determine their alignment with an outcome-based regulatory approach and non-prescriptive requirements, to ensure a net benefit to productivity.

Digital Financial Reporting

Finally, general insurers understand the importance of moving to digital financial reporting and the benefits this would have to leveraging emerging technologies, including AI. Insurers must already comply with ASIC's Financial Reporting Taxonomy and although there are some references to the cost implications experienced internationally, this does not consider the existing operating environment of general insurers subject to Australia's financial services regulatory framework. If mandatory digital financial reporting is recommended in the Commission's final report, general insurers will need significant lead times to implement changes given the current volume of regulatory reform underway and the complexity of updating systems and processes to ensure compliance.

We thank the Commission for allowing us to comment on the interim recommendations and look forward to the final report.

Should you have any questions regarding this submission please contact Brooke Noorbergen, Senior Adviser Strategic Policy, at bnoorbergen@insurancecouncil.com.au.

Yours sincerely



Kylie Macfarlane
Chief Operating Officer & Deputy CEO

Appendix: Harnessing Data and Digital Technology

Insurance industry response to the Commission's interim recommendations

Artificial Intelligence

Draft recommendation 1.1 - Productivity growth from AI will be built on existing legal foundations. Gap analyses of current rules need to be expanded and completed.

The Insurance Council and our members supports this recommendation. Most risk and possible harm associated with artificial intelligence (AI) and its use are being mitigated by existing laws and regulation. Further strengthening the current regulatory framework, built on a regulatory gap analysis, will provide certainty for business and regulators alike. The general insurance industry would welcome the opportunity to collaborate on any gap analysis.

Focusing on strengthening existing legal frameworks rather than creating new frameworks will limit unnecessary costs to the Government and industry associated with building, implementing and maintaining new and additional regulatory infrastructure.

Additionally, the Insurance Council notes that new regulations can often have flow on effects to end-user costs, including for insurance products such as cyber, professional indemnity and directors' and officers' lines.

Draft recommendation 1.2 - AI-specific regulation should be a last resort

Insurers support this recommendation. Any move to AI-specific regulation should only occur after the gap analysis discussed above has found specific AI harms that cannot be regulated by other existing means.

Draft recommendation 1.3 - Pause steps to implement mandatory guardrails for high-risk AI

Insurers support this recommendation. Regulation of high-risk AI should be underpinned by a regulatory gap analysis (as outlined above) and cost-benefit analyses.

Data Access

Draft recommendation 2.1 - Establish lower-cost and more flexible regulatory pathways to expand basic data access for individuals and businesses

The interim report outlines the benefits of Consumer Data Right (CDR) regime which currently applies to the banking and energy sectors. The benefits to consumers outlined are improved operability between systems and reduced duplication in data collection. This ultimately improves competition and supports consumers to better understand their needs to make informed decisions. Insurers support consumers accessing their data held by businesses, however, insurance data is not analogous with other sectors where the CDR has been implemented. The application of a data access pathway to insurance requires further analysis.

In 2023, the Government paused the roll out of the CDR regime to insurance. The Insurance Council at that time outlined several differences in insurance data handling that would make the application of the CDR difficult, costly and potentially ineffective. Unlike basic banking and energy data, insurance data is not transactional and mostly relates to the insured asset (such as a house or car), or the risk, rather than the insured person. Where there is data that relates to individuals, insurers will utilise a range of data from their own modelling or procured from third parties, such as natural hazard data to undertake risk assessments and pricing. This risk information is also collected and assessed at a point in time, usually at inception of the policy (which typically run for 12 months) and is likely to change as time elapses. The risk assessment and pricing data becomes commercially sensitive and is the

intellectual property of the insurer. There are also circumstances where insurers do not own the data and are only the intermediary holding the data. For example, in workers compensation or compulsory third-party insurance, individuals are bound by the terms of the Government, and the Government is the owner of the data.

The Commission rightly points out that any additional data access “...*pathways should begin in sectors where better data access could generate large benefits for relatively low cost; and there is clear value to consumers.*” There are a range of information sharing regulations that require insurers to share personal information with customers in certain circumstances. For example, the General insurance Code of Practice under section 104. requires insurers to provide consumers information that was relied on when deciding on mental health related claims. It’s unclear from the interim report what value would be sought by introducing a supplementary data sharing pathway in insurance. Insurers therefore do not support insurance data being captured by these initiatives until clear consumer benefits are identified and there is a sound net benefit to productivity.

Privacy Regulation

Draft recommendation 3.1 - An alternative compliance pathway for privacy

Insurers support privacy regulation that is outcomes based and would like to see the Government consider the design of all remaining Tranche 2 Privacy Act reform proposals to ensure alignment with this approach. Some recommendations being considered as part of Tranche 2 of the Privacy Act Review propose further prescription, for example, notifying consumers where geolocation tracking data may be accessed and used. Blending prescription and outcomes-based regulation will significantly impact productivity as it will require the double handling of processes to ensure compliance with both the prescriptive and outcomes-based measures. Insurers support the Commission’s proposal to introduce a defence compliance pathway against regulatory action but do not see this as being an alternative.

Information request 3.1

- What are the anticipated costs and benefits of implementing an alternative compliance pathway?

Introducing a defence pathway would have minimal to nil costs for insurers should this be implemented as a defence for regulatory action under the civil penalty regime (including compliance notice and infringement notice powers). This is preferred over alternative models outlined in the interim report which would introduce burdensome costs to reverse previous investments in systems and processes that accommodate existing prescriptive requirements.

- How should an alternative compliance pathway be designed – through the creation of a new defence, a safe harbour, deemed-to-comply standards, or something else? Why?

The defence pathway is the preferred pathway for general insurers. This pathway would have minimal impact on productivity but still uplift consumer protections. The *safe harbour* or *deemed to comply* pathways are not supported as they would require more prescription and move further away from an outcomes-based approach.

- How should requirements for the alternative pathway be framed – as a duty of care, a fiduciary duty, a best interest obligation, or something else? What are the merits and downsides of the different options?

Insurers do not support a best interest obligation for individuals as this is subjective. Insurers support a *duty of care* model as this aligns with an outcomes-based approach that seeks to avoid and mitigate

harm to an individual's personal data. The Commission should consider the impact of their recommendations on industry's ability to use and share personal information in the context of settling insurance claims and investigating fraud. The current APPs allow data sharing for the original collection purpose; a secondary purpose if the individual consents; if it is reasonably necessary for enforcement activities or is required by law. The Commission should continue to support the use of personal data in these ways in its final report.

Draft recommendation 3.2 - Do not implement a right to erasure

The Insurance Council and its members support the Commission's recommendation to not progress a *right to erasure* as recommended by the Privacy Act Review. Insurers note that APP11 requires insurers to not hold personal information unnecessarily. The Commission's interim report acknowledged the concerns raised by stakeholders regarding the rigour of the Government's cost-benefit analysis undertaken on the Privacy Act Review's recommendations. The Commission identified that the costs to implement a *right to erasure* would outweigh the benefits. If the Government pursues the remaining recommendations from the Privacy Act Review, including the *right to erasure*, the Government should ensure all recommendations have a net benefit to productivity. Additionally, the Government should consider the entire ecosystem of data retention policies (such as the CDR or the Attorney General's review of data retention) concurrently to any changes made to the *Privacy Act 1988*, to ensure coordination and minimise the operational burden on insurers to change systems and processes.

Digital Financial Reporting

Draft recommendation 4.1 - Make digital financial reporting the default

Insurers acknowledge that financial reports provide essential information that is used by a wide range of stakeholders for diverse purposes. Insurers support improving efficiency in processes but remain concerned about the timelines for implementation and the cost impost this might have. Although there was international cost comparisons included in the Commission's report, these are drawn from jurisdictions that don't reflect the unique context of Australia's financial services regulatory framework.

Currently, insurers must adopt software capable of producing financial statements in XBRL or iXBRL format, aligned with the ASIC Financial Reporting Taxonomy. This involves tagging each financial data point with the appropriate taxonomy element, validating the report for compliance, and ensuring it meets ASIC's digital lodgement standards. Changing these systems will involve significant cost and effort, as well as requiring appropriate oversight, ongoing controls and auditing. Beyond the technical requirements, it is anticipated that there would need to be changes to processes in how financial information is prepared, reviewed, and disclosed, as well as a possible shifts in governance and oversight processes to accommodate digital formats.

While we recognise that digital financial reporting is likely to deliver long-term benefits in terms of data quality, transparency, and regulatory efficiency, and facilitate the use of emerging technologies, any move to digital financial reporting will require significant lead time for implementation (likely years).

Information request 4.1

- Who should be required to submit digital financial reports? Should implementation be phased?

All listed entities, entities holding public deposits and all large entities meeting/exceeding the threshold criteria defined by the *Corporations Act 2001* that are required to prepare general purpose financial statements.

Phased implementation is appropriate and should start with listed entities.

- Are there other reports that should be submitted digitally?

If digital reporting is implemented for annual financial reporting from insurers, a natural extension would be to include sustainability reporting. Sustainability reporting is an emerging domain, and reporting will evolve over time. Any roll out of digital financial reporting should consider the maturity of the reporting in question and the consistency of the data contained over time.

Other areas could include regulatory returns such as those collected by APRA. Or ASIC half year and end of year financial statements.

- What is needed to support high-quality financial data? How should digital financial reports be submitted and accessed?

Introducing a taxonomy would support quality reporting, providing the data points are standardised. Consideration will need to be given to company specific disclosures as these can vary based on principles-based accounting standards.

Insurers have experience using APRA's Connect platform, which is a centralised data collection tool where insurers can submit financial data. Lessons learnt from this tool could be applied. For example, data collection processes should enable automatic validation checks which clearly identify errors and makes it easy for the user to correct them. Additionally, the bulk provision of documents should be facilitated to avoid the need to individually upload items. Ongoing funding will be required for regulators to continuously improve online reporting tools to minimise the regulatory burden on companies. The Government may also need to consider external assurance of tagging to ensure accuracy.

- Should report preparers be required to prepare their digital financial reports in XBRL format, iXBRL format, either format or a different format?

Should the objective be to fully transition from PDF-based reporting to digital financial reporting, the adoption of iXBRL is recommended. However, if the intention is for digital financial reporting to exist alongside current PDF formats, the XBRL format may be more appropriate. The need for XBRL or iXBRL format should be challenged with the evolution of new AI models and the Commission should consider if tech neutrality is achievable with digital financial reporting.

- How should digital financial reports be submitted? How should they be made available to the public?

Digital financial reports should be accessible to the public (if currently published). Limiting access solely to institutional investors would restrict the broader benefits these disclosures can offer. Wider availability ensures that all key stakeholders - including customers, suppliers, and retail investors - have equitable access to essential information with the same capabilities.

- What should be done to ease the reporting burden for preparers?

The reporting process should not require additional reports to be generated but rather leverage existing reports (eg. annual reports) and support processes where the desired data can be extracted. Furthermore, guidance should be provided on the tagging of industry specific non-IFRS information eg. Gross Written Premium data for the insurance sector.

There should be flexibility built into the reporting framework to facilitate the adoption of AI or other digital tools over time.