Insurance Council of Australia

Australian Information Commissioner
GPO Box 5288
Sydney NSW 2001

Via email: copc@oaic.gov.au

Dear Commissioner,

Exposure Draft of the Children's Code

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to provide comment on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (the Code).[1] The Insurance Council is the representative body of Australia's general insurance industry. Our members account for approximately 90 per cent of total premium written by general insurers and reinsurers. As a foundational component of the Australian economy, the general insurance industry writes 90 million policies a year, paying out $58.9 billion in claims in 2025 – an average of $226 million every working day.

The Insurance Council supports the objective of strengthening privacy protections for children in the online environment. We recognise that children increasingly interact with digital services and that robust, fit-for-purpose protections are essential. We also acknowledge the objective of the OAIC to make privacy disclosures more accessible to children, helping them to understand how their information is used. However, the Insurance Council submits that the Code, as currently drafted, goes well beyond the original policy intent. Critically, it does not adequately distinguish between online services that pose heightened or inherent risks to children's privacy, with beneficial, welfare-orientated services such as insurance.

Some of our members estimate that children make up less than 1% of their customer base. Where children are direct customers, the vast majority are over 15 (usually representing those who can obtain a driving licence before turning 18). The most common insurance product held by children is CTP (Compulsory Third Party), which is legally required for all car owners in every state and territory. In this insurance line, children still account for less than 1% of CTP policyholders in some of our largest members.

Insurers have indicated that the costs associated with discovery activities, assessment of compliance obligations, and implementation of the Code will be significant. One insurer has estimated the cost of implementing the Code, based on a worst-case scenario, would be at least $14-$17 million. These costs would deliver no corresponding benefit because the data practices the Code targets, such as commercial exploitation or sale of children's data, simply do not occur in the insurance context.

These implementation costs contribute to the sector's existing inflationary pressures being driven by macro-economic factors outside of insurer's control, including rising interest rates, supply chain disruptions and international conflict. The costs of implementing inefficient and unnecessary regulation directed by Government bodies are ultimately carried by all policy holders, including children.

[1] Office of the Australian Information Commissioner.(2026). *Draft Children's Online Privacy Code (consultation for industry, civil society, academia)*. https://www.oaic.gov.au/engage-with-us/consultations/draft-childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia

We also note that the Government has not yet provided certainty on tranche two reforms to the *Privacy Act 1988*. Some of the measures in the Code overlap with proposals from the Privacy Act Review[2] that have not been enacted yet, such as rights to data erasure. The Office of the Australian Information Commissioner (OAIC) should consider the risk of pursuing these changes in isolation to tranche two, which increases the risk of regulatory overlap. This awkward phasing of reform may also require businesses to make similar changes twice, within a short period of time, at significant cost. This again, places unwarranted pressure on the cost of insurance for all policy holders.

The current regulatory framework

The Explanatory Statement highlights that the Code responds to the 2023 Privacy Act Review, which raised concerns about children being tracked and profiled through online services. These concerns focus on services that collect detailed data about children's activities, interests, location, wellbeing and relationships, often to profile or monetise their behaviour. Key examples included social media platforms, mobile apps and connected devices. These are services where children engage directly and often make privacy decisions without clear understanding or parental oversight. General insurance operates in a very different way to the types of services the Code seeks to regulate.

Firstly, general insurers are already subject to a strong set of laws and regulatory frameworks that protect individuals, including children:

1. ASIC's Design and Distribution Obligations (**DDO**) prescribed by the *Corporations Act 2001*, require insurers to actively consider their target market and produce a Target Market Determination (**TMD**) for each product. TMDs require insurers to assess whether their products are appropriate for the consumers who will acquire them, and distribution to consumers outside the target market trigger reporting obligations.
2. APRA's prudential standards require insurers to have robust governance, data management, and risk frameworks that extend across all customer groups, including children. These include CPS 234, CPS 230 and CPS 220, which collectively cover overarching requirements around risk management. Certain contraventions of these prudential standards are required to be reported to APRA, including material information security control weaknesses under CPS 234.
3. APRA-regulated entities are also subject to the Financial Accountability Regime, which imposes personal accountability on senior executives for consumer outcomes, including outcomes for vulnerable cohorts such as children.
4. Insurers are also bound by the General Insurance Code of Practice (GICOP) and must follow its requirements. GICOP includes specific protections and provisions for insurers to support customers experiencing vulnerability, including with specific reference to age being a potential vulnerability under paragraph 92(a), which would capture children. GICOP is currently under review, in consultation with consumer groups and regulators.
5. Insurers are also regulated under the *Australian Securities and Investment Commission Act 2001* against deceptive and misleading conduct, unconscionable conduct, false and misleading representations and are required under the *Corporations Act 2001* to operate efficiently, honestly and fairly with all customers.

Secondly, children's involvement in insurance is typically limited and structured. In rare cases, minors may be the policy holder (for example, in CTP, motor, or home and contents insurance). More commonly, they are beneficiaries under a policy taken out by a parent, guardian or other party, such as in travel insurance or workers' compensation. In these cases, the personal information collected is handled almost exclusively in their interest to:

[2] Attorney-General's Department.(2023). *Privacy Act Review report*. Australian Government. https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

- Cover asset losses arising from unforeseen events.
- Arrange time critical transportation or towing services.
- Meet statutory requirements in the case of CTP or workers compensation.
- Arrange medical treatment, rehabilitation expenses, weekly or lump sum benefits following injury or illness and coordination with healthcare providers for required services.
- Coordinate evacuation or repatriation during travel.

Children are not actively engaging with insurers to create profiles, share content, or make ongoing privacy choices to their detriment. Instead, any collection and handling of their personal information by insurers occurs for defined, necessary purposes linked to providing cover or managing a claim.

Since the Code takes an economy-wide approach to its application, these distinctions of insurance products and services are not appreciated. Part 2, section 5(a) of the Exposure Draft applies the Code to providers of a 'designated internet service'. This term is taken from the *Online Safety Act 2021* and is defined broadly to include any service that allows users to access material online such as websites or applications. All insurers operate websites and applications, not dissimilar to other corporate entities in Australia, and therefore are likely to be captured by the new requirements of the Code. Consequently, general insurers are facing the same operational standards that other higher risk products and services must meet.

Operational challenges

If insurers are caught by the Code, they would be required to introduce new systems and processes across all digital products to manage new age-based requirements. The Code as it stands would require insurers to:

- Identify minor policyholders at the point of policy inception.
- Apply different and concurrent data handling defaults and consent frameworks depending on the age of each insured person (see requirements under section 12 to 21)
- Maintain and update those distinctions over the life of the policy until they turn 18 — including tracking when an insured child turns 15 (triggering new consent obligations) and when they turn 18 (releasing them from the Code's scope entirely).
- Implement new data destruction and consent processes that can be triggered across the varying age brackets.
- Implement audit trails and annual privacy impact assessments reflecting these age-differentiated data flows.
- Implement an absolute right to erasure for children, regardless of whether information is required to provide an ongoing business product or service (noting that the specific approach to a more general right to erasure under proposed reforms to the Privacy Act has not yet been outlined).

Insurers may determine, through internal cost-benefit assessments, that the compliance burden is disproportionate to the benefits, particularly where children make up less than 1% of the customer base for a relevant service. One way that this might occur is that an insurer may choose to restrict online services to over 18 year olds only as a way to avoid the complications presented by the Code requirements. The Code should avoid unintentionally making it harder for children to access products or support, particularly where the relevant product or service serves a public good and prevents moral hazard (such as how motor insurance policies cover not-at-fault third parties from loss or damage).

There are also several areas requiring clarification (either in the Code or in supporting guidance) that are important for implementation. These issues include: how cookies and metadata should be treated; how a commercial entity would be able to determine the best interests of a child; and how data erasure requests would interact with existing data retention laws. It's also unclear how general insurers would be expected to comply with the Code while implementing state-based statutory insurance regimes, such as CTP and workers compensation. In these insurance lines, insurers not only do not always control the communications to insureds and claimants, but the specific wording of privacy consents and data-handling practices are regulated by state-based compensation legislation and outside of insurers' control. In this regard we strongly recommend that personal information obtained and managed under state-based legislation (such as for CTP or Workers Compensation schemes) be expressly excluded from the scope of the Code.

Slowing down time-critical service

A one-size-fits-all application of the Code across the economy risks overregulating lower-risk activities in insurance, frustrating processes for consumers and impacting their access to timely insurance services.

The Code's consent framework that requires voluntary, specific, current, and unambiguous consent (see Sections 13 to 19) is designed for online services where consent can be managed iteratively through user interfaces. These requirements are ill-suited to insurance services that frequently operate in time-critical and emergency contexts, such as following a disaster or where evacuation or repatriation is required including where deferral would create uninsured periods or legal non-compliance; and integral to statutory or contractual frameworks such as in compulsory third party (CTP) insurance or worker's compensation schemes. Mechanisms such as consent expiry (Section 16 limits consent currency to 12 months), repeated consent validation requirements, and overly rigid consent scoping are likely to introduce operational friction at precisely the point where speed, clarity, and authority are essential. For example, division 2 section 20 would introduce the need for an insurer to seek separate consent from a child under 15 years listed as a beneficiary of a travel insurance policy because the child would be a *direct end user* of the insurer's service in the case of a claim. This adds unnecessary friction to the onboarding and claims process and would also require specially tailored collateral to ensure the child under the age of 15 could understand their legal obligations under the policy.

Interpreting the term *likely to be accessed*

The OAIC has made several references in the Explanatory Statement indicating an intent to align the Code with the UK Information Commissioner's Age Appropriate Design Code. The Insurance Council recommends the OAIC adopt a similar threshold for *likely to be accessed* which would ultimately apply the Code to:

a) services that are intended for use by children; or
b) services not specifically aimed or targeted at children, but where it is still more probable than not to be accessed by children as a distinct cohort.

This approach should:

- Exclude utility or basic services which do not target children as a distinct cohort but are utilised by the general population;
- Exclude services that occur where consent has been given by a parent or guardian; and
- Ensure consistency with data retention policies under existing legislation; and
- Exclude general insurance lines that are regulated and controlled by state-based entities (such as CTP and workers compensation regimes).

Members of the Insurance Council do not support minimum numerical thresholds being set via the Code to determine what is in scope of *likely to be accessed.* This would freeze the Code at a point in time and require ongoing compliance monitoring, again adding additional cost for minimal benefit.

Options to improve the effectiveness of the Code

Best-practice privacy regulation is risk-based, targeted to where harm is most likely, and proportionate to the activity regulated. Section 8(2) of the Code itself acknowledges this principle by requiring that steps taken to ascertain an end-user's age be reasonable 'having regard to the risk of harm that may arise from any collection, use or disclosure of the end-user's personal information.'

The Exposure Draft also recognises that some types of services with a social benefit should be treated differently. For example, it provides exemptions for certain services that deliver important public or social benefits, such as health and telecommunications services (see Part 2, section 5(c) and section 6). Insurance serves a similar function. It provides critical support in times of need and operates within a highly regulated environment. On this basis, the Insurance Council proposes that the Code be amended to exclude APP entities providing general insurance products where the insurance service is provided pursuant to an insurance contract, and is consistent with the Design and Distribution Obligations required under the *Corporations Act 2001*.

Having a clear exemption in the Code would provide insurers with operational certainty and avoid unnecessary costs in determining if, when and how the Code might apply. It would also avoid regulatory friction between the Code and state-based regulatory regimes, such as CTP and workers compensation where insurers do not control the privacy policies of statutory bodies.

The ICA and its members would like to see the Code achieve its intended goals, whereby it effectively targets risk-based activities that are likely to be accessed by children and track, and monetise children's data. The general insurance sector does not present these risks and should not be subjected to the same level of additional compliance currently being presented by the Code.

If the Code does not take a risk-based approach and provides no exemption, the Insurance Council could advise the OAIC on a partial exemption or phased implementation with a view to managing the significant impact on insurers and their customers.

If you would like to discuss the issues outlined in this submission, please contact Brooke Noorbergen, Senior Adviser Strategic Policy at bnoorbergen@insurancecouncil.com.au.

Yours sincerely

Andrew Hall
Executive Director & CEO