interactive games & entertainment association

Submission to Senate Legal and Constitutional Affairs Legislation Committee

Response to Inquiry into the Privacy and Other Legislation Amendment Bill 2024 [Provisions]

October 2024

IGEA acknowledges and pays respect to the past and present Traditional Custodians and Elders of this land and the continuation of cultural, spiritual and educational practices of Aboriginal and Torres Strait Islander peoples. We would like to extend our acknowledgments to the indigenous people from countries overseas and recognise their strength, wisdom and creativity.

1. Introduction

The Interactive Games & Entertainment Association (IGEA) welcomes the opportunity to provide a submission to the inquiry into the Privacy and Other Legislation Amendment Bill 2024 [Provisions] (Privacy Amendment Bill), led by the Senate Legal and Constitutional Affairs Legislation Committee.

1.1 About IGEA

IGEA is the industry association representing and advocating for the video game industry in Australia, including the developers, publishers and distributors of video games, as well as the makers of the most popular game platforms, consoles and devices. IGEA has over a hundred members, from emerging independent studios to some of the largest technology companies in the world. Amongst our various activities, IGEA also organises the annual Games Connect Asia Pacific conference for Australian game developers and the Australian Game Developer Awards that celebrate the best Australian-made games each year.

Video games are a beloved Australian activity and significantly benefit Australian game players, the wider community, and the economy. Video game developers and publishers are the innovators, creators and business leaders reimagining entertainment and transforming how we learn and play. Over 80% of Australians play games, with most Australian households having a device for playing video games, mainly for enjoyment and relaxation, and games are increasingly being used for serious and educational purposes, including by governments.[1] Video games provide a digital outlet for Australian art, culture, stories and voices, and Australian-made video games are among Australia's most successful and valuable cultural exports. Our medium also brings kids into Science, Technology, Engineering, the Arts and Mathematics (STEAM) and helps them build technology skills that will feed Australia's workforce needs.

In supporting local content, the video game industry is a major contributor to the Australian digital economy. According to our data, video games are worth around $4.4 billion annually in Australia,[2] while Australian-made games brought in $345.5 million in largely export revenue last year.[3] Moreover, because the video game industry uniquely sits at the intersection of entertainment, the arts and technology, video game companies hire a wide range of artistic, technical and professional roles and are thus a wellspring of high-quality sustainable careers, and are an engine for growth in the Australian national economy. Indeed, Australian game developers are internationally renowned, and ours has the potential to be one of Australia's most important future growth industries and an integral component of the government's vision for Australia to be a top 10 digital economy and society by 2030.

---

[1] IGEA, 'Australia Plays' (August 2023), https://igea.net/2023/08/australia-plays-2023/.

[2] IGEA, '2023 Australian video game consumer sales continue stable growth' (Media Release, June 2024), https://igea.net/2024/06/2023-avgcs/.

[3] IGEA, 'Aussie game developers pull in $345.5 million for local economy' (Media Release, December 2023), https://igea.net/2023/12/2023-agds/.

1.2 Overview

Overall, we support privacy laws that are modern, practical, sensible, evidence-based and compatible with the digital economy, including for the video game industry ecosystem.

Video games could not exist without data. Not only is data largely used by game developers to make their games better for players, but the use of personal data for this goal is a core expectation of players. The video game industry treats its responsibility to protect the data of its players as among its highest priorities, including leading the digital industry in the pseudonymisation of their players through 'gamer tags'.

We believe that privacy and data stewardship reforms should take a clear but flexible principles-based approach that encourages good privacy practices, while avoiding overly prescriptive rules, stymie innovation, impose unreasonable red tape, or even have unintended negative impacts on privacy.

Over the last several years, IGEA has been a highly engaged and long-standing stakeholder in the Australian Government's ongoing review of the *Privacy Act 1988* (Cth) (Privacy Act), led by the Attorney-General's Department. Among IGEA's various contributions, comprehensive submissions were lodged in response to the Department's Issues Paper,[4] Discussion Paper,[5] and Privacy Act Review Report.[6]

At this current stage of privacy reform, we understand that the Privacy Amendment Bill implements the Government's first tranche of recommendations arising from the Privacy Act Review,[7] progressing 23 legislative proposals (out of a significant 116 proposals) from the Government's response to the Privacy Act Review Report.[8] We welcome further consultation by the Government for any future proposed privacy reforms.

Previously, we observed that the high volume of proposals and limited time for consultation meant that we had to focus our attention on issues of most significance and anticipated impact on our members, our consumers, and our industry. For similar reasons, this latest submission will only address previous issues that have carried over into this Bill, namely with respect to a proposed Children's Online Privacy (COP) Code and overseas data flows. That being said, where we have not provided a response to a proposal at this inquiry stage, it should not necessarily be taken to represent support for other proposals that have also been put forward in this Bill.

Below is a summary of our recommendations to this consultation.

---

[4] IGEA submission to Attorney-General's Department (November 2020), https://igea.net/2020/12/submission-responding-to-the-australian-attorney-generals-departments-issues-paper-review-of-the-privacy-act-1988/.

[5] IGEA submission to Attorney-General's Department (January 2022), https://igea.net/2022/01/igea-submission-to-the-consultation-on-the-australian-privacy-act-review/.

[6] IGEA submission to Attorney-General's Department (March 2023), https://igea.net/2023/04/igea-submission-to-the-australian-privacy-act-review-report/.

[7] Attorney-General, 'Better protection of Australians' privacy' (Media Release, 12 September 2024), https://ministers.ag.gov.au/media-centre/better-protection-australians-privacy-12-09-2024.

[8] See: https://www.ag.gov.au/rights-and-protections/privacy.

Topic	Recommendations
Children's Online Privacy Code	• As the Australian Government has committed to developing the Children's Online Privacy (COP) Code, the Code should be referring to services that are 'targeted at, or directed to, children', which is less ambiguous than the term 'likely to be accessed by children'. • Should the Office of the Information Commissioner (OAIC) be assigned with the responsibility for developing and consulting on the COP Code, the Bill should explicitly require the OAIC to meaningfully consult with relevant industry stakeholders who are directly impacted by the COP Code. Consultation should at least occur during the development and public consultation stages of the Code. • For the COP Code development process to be effective, it is also important that there be sufficient time allocated to the process, flexibility for consideration of relevant issues, clearly scoped and avoid overlapping requirements between the COP Code and other regulatory instruments (e.g. under the Online Safety Act), and mutual transparency between the regulator and industry stakeholders to ensure a more productive process. • It would be prudent and logical to refer to the outcomes of the Government's age assurance trial before considering age assurance measures in the context of privacy reform. In the meantime, we caution against infringement upon privacy and security, especially pertaining to the data of children, which may arise from implementing age assurance technologies, to give effect to the COP Code. We would be keen to understand whether these concerns are addressed from the Government's separate age assurance trial. • Regardless, the video game industry has long spearheaded parental control capabilities in video game services to address child access to age-inappropriate games, based on global industry best practice. Ensuring children's safety online hinges on parental and caregiver consent. Our industry has led the way in creating effective parental control tools across different devices and platforms. Parents and carers are therefore empowered to use technological and/or non-technological means to help manage their children's viewing and playing experiences, as opposed to deferring to the government. This nuance needs to be better appreciated in how online safety and privacy is approached for video games by government.
Overseas data flows	• While not in the scope of this Bill, the Australian Government should continue to work on a path towards an adequacy

Topic	Recommendations
	decision to facilitate overseas data flows between Australian and the EU. • The EU's General Data Protection Regulation be prioritised at the first opportunity, in accordance with the overseas data flows provision of the Bill. • The Australian Government (via the relevant Minister) should favourably consider 'whitelisting' countries that already have an adequacy decision with the EU, where the Governor-General could then make regulations to prescribe that these countries provide substantially similar protections to the APPs, in accordance with section 100(1A) of the Bill e.g. the United Kingdom and Japan. The Bill should also clarify Australia's position on 'onward transfers', where personal information that was first transferred from Australia to a whitelisted country (Country A), is further transferred from Country A to another country (Country B). • The Government should reconsider whether 'substantially similar' is the best term to use as the certification threshold for establishing overseas data flows between Australia and a given country. We would prefer the term 'adequate' or 'similar'.

2. Children's Online Privacy Code

The Bill introduces a requirement for the OAIC to develop a Children's Online Privacy (COP) Code, along with associated considerations and processes to develop such a Code under section 26GC. The Australian Government has also committed an additional $3 million over three years to the OAIC to develop this Code.[9]

2.1 Consideration of overseas approaches

While we do not necessarily disagree with the idea of a COP Code in principle, we previously recommended that the Australian Government first monitor and assess the implementation of the UK's Age Appropriate Design Code (AADC) (which only came into full operation in 2021), before making a decision on whether to introduce such a Code in Australia.

Although not considered perfect by all stakeholders, the UK's AADC is a useful reference point, because it is generally regarded as balanced and flexible in how it approaches the need for protecting children's data, as well as ensuring that children can continue to participate online. However, it is also important to appreciate its nuances. For instance, the

[9] Attorney-General, 'Better protection of Australians' privacy' (Media Release, 12 September 2024).

AADC is a specific implementation of the General Data Protection Regulation (GDPR) by the UK and is administered by the UK's Information Commissioner's Office (ICO).

Subsequent to the UK AADC, California adopted the California Age-Appropriate Design Code Act (CAADCA).[10] However, that Californian statute has been challenged in US federal court and blocked by the district court on broader constitutional grounds (i.e. violating the First Amendment of the US Constitution).[11] This has been recently partially upheld in a subsequent court of appeal.[12] Notwithstanding the ongoing litigation with the CAADCA, Maryland has now passed its own Age-Appropriate Design Code Act this year, leaving it potentially open to also being subject to similar legal challenges. Adding to this complex landscape of US state-based privacy legislation is the US federal statute, Children's Online Privacy Protection Act (COPPA), which also addresses online privacy.

We note that the Explanatory Memorandum refers to the UK's AADC as the basis for introducing the COP Code, reflecting the Government's intention for international alignment.[13] While we do not object to international coherence, we consider there may be lessons learnt from the UK's implementation (and other countries) that can be improved upon in the Australian context.

2.2 Scope of services captured under the COP Code

If the Government wishes to proceed with the development of the COP Code, we strongly recommend that the provisions of the Bill explicitly state that relevant stakeholders, especially industry, are properly consulted with, and services are clearly scoped.

For example, consider section 26GC(5)(a) of the Bill, where entities that would be bound by the COP Code include a provider of a 'relevant electronic service', 'within the meaning of the *Online Safety Act 2021*' that is 'likely to be accessed by children'.

Firstly, our strong preference would be to use the term 'targeted at, or directed to, children'. Similar terminology (i.e. 'directed to children') has been used overseas in legislation such as the US federal statute, Children's Online Privacy Protection Act, which industry considers to be unambiguous.[14] This approach will make it clearer which services will be subject to the COP Code. In contrast, the term 'likely to be accessed by children' appears to have been adopted from the UK's AADC, which is more ambiguous.

---

[10] See: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

[11] *NetChoice v Bonta* (ND Cal, No 22-cv-08861-BLF, 18 September 2023), https://storage.courtlistener.com/recap/gov.uscourts.cand.406140/gov.uscourts.cand.406140.74.0.pdf.

[12] For instance, the court of appeal found that the CAADCA included a Data Protection Impact Assessment (DPIA) requirement for online service providers will likely violate the First Amendment. The DPIA requires providers to "opine on and mitigate the risk that children are exposed to harmful or potentially harmful materials online" for their online services, which are 'likely to be accessed by children'. The court stated that the DPIA "clearly compels speech by requiring covered businesses to opine on potential harm to children", and "deputizes covered businesses into serving as censors for the State". See: *NetChoice v Bonta* (9th Cir, No 23-2969, 16 August 2024), pp. 2, 26-29, https://cdn.ca9.uscourts.gov/datastore/opinions/2024/08/16/23-2969.pdf.

[13] Australian Government Response to the Privacy Act Review Report (September 2023), p. 13, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF.

[14] See: https://www.law.cornell.edu/uscode/text/15/6501.

Secondly, a 'relevant electronic service' is wide in meaning under the Online Safety Act. For example, a 'relevant electronic service' includes "a service that enables end-users to play online games with other end-users" under the Online Safety Act.[15] Therefore, the COP Code will likely include multiplayer video games, which needs to be properly thought through. We discuss further below regarding the nuances of video games in the context of privacy.

2.3 Proper consultation in developing the COP Code

As a matter of good public policy and best practice regulation, the Government has previously rightly stated that "[t]he code developer should consult broadly with children, parents, child development experts, child welfare advocates and **industry** in developing the code".[16] Following this statement, the Bill has assigned that code development responsibility to the OAIC, with the Explanatory Memorandum providing the following rationale:[17]

> There is a public interest and community expectation in ensuring that a COP Code is developed and registered, and is developed by the Information Commissioner who has particular expertise in privacy. This will avoid any potential industry regulatory biases, and conflicting commercial interests.

We do not necessarily agree with the argument of perceived industry bias as an inhibitor for industry to take the lead in developing codes. For instance, industry (including IGEA as one of the leading industry representatives) has demonstrated that it can effectively develop industry online safety codes, in accordance with the Online Safety Act, which have been accepted and registered by the eSafety Commissioner. Although the industry online safety codes development process is not perfect, there is always room for improvement, which we are seeking to have addressed as part of the Statutory Review of the Online Safety Act.

Setting aside that moot point for the moment, we are not opposed in principle to the OAIC taking the lead in developing the COP Code(s), so long as the regulator genuinely and properly consults with relevant stakeholders in accordance with good public policy and best practice regulation. This includes allocating sufficient time to consult, flexibility to consider relevant issues, acting in good faith, and promoting a genuinely collaborative environment for mutual transparency between the regulator and industry stakeholders to ensure a more productive process.

Unfortunately, the Bill does not explicitly reflect the Government's clear expectation that industry should be consulted in developing the COP Code under section 26GC(8) of the Bill. We support children, relevant organisations or bodies concerned with children's welfare, the eSafety Commissioner, and the National Children's Commissioner being consulted. However, industry has been omitted from those who *may* be automatically consulted with by the OAIC. Instead, they *may* be consulted along with 'any other person' at the OAIC's own discretion under clause 26GC(8)(b). This consultation process is further

---

[15] *Online Safety Act 2021* (Cth), section 13A(1)(f).

[16] Australian Government Response to the Privacy Act Review Report (September 2023), p. 13.

[17] Explanatory Memorandum to the Bill, p. 40.

downgraded when the OAIC proceeds to *invite* public submissions on the Code, where the OAIC will only be required to *consult with* the eSafety Commissioner and the National Children's Commissioner, under clause 26GC(9).

It is critical that industry is properly consulted, especially as the COP Code will directly impact them. Industry is also better placed to understand its capabilities to meet its privacy obligations, in a similar vein to how the OAIC should have the relevant capabilities to enforce privacy regulations.

2.4 Understanding how games manage user data

If video games are to be subject to the COP Code, it is also important to understand the context in which data is managed and protected in video games to avoid inadvertently negatively impacting game players' experiences.

For instance, the data generated by players has many uses, but most importantly to help ensure that games run well and players can have the best gameplay experience. Developers use data to find bugs, identify areas of improvement, monitor in-game behaviour like text chat, detect cheating, and to learn how to make better gameplay experiences. Likewise, video games and game services may use limited personal information such as email addresses to strengthen account security, or ask for age-related data to help parents and carers better monitor what their children play. Some games are also ad-supported, which typically allow players to play them for free.

Best practice means companies should be collecting consumer data responsibly, collect only what is needed, and keep personal information secure. Our industry is committed to upholding all Australian data management laws, providing multiple and clearly worded privacy notices to give transparency to players, adopting best practice account security measures, and, for many platforms, offering privacy settings to give players choice around how their data is used. To better protect the privacy of their players, our industry is renowned for its widespread use of pseudonyms, 'gamer tags', avatars, and device identifiers in lieu of more sensitive personal information such as player names. This is a practice that our sector arguably leads the digital world in.

It is also important to ensure that reference to the video game industry is properly defined to avoid unintentionally conflating issues that may arise more broadly in digital platforms. The primary purpose of video games is in its name – to play video games and entertainment, offering immersive experiences, adventure, activities and storytelling.[18] This is in contrast to socialising in a manner synonymous with other online platforms where they may be primarily intended for user communication. Those other platforms also monetise or commercialise private information as their core business model, as opposed to in video games. To this end, online game features are vastly different from other online services.

[18] For example, see: https://www.comeback.world/2023/05/12/difference-between-social-media-video-games/.

2.5 Age assurance

A relevant consideration when considering online regulation with respect to children is age assurance. This will be important to determine how to address online services accessed by children.

Indeed, the Government suggests this needs to be factored in with respect to addressing children's privacy:[19]

> To meet requirements in relation to children, it is expected that entities will need to take reasonable steps to establish an individual's age with a level of certainty that is appropriate to the risks, for example by implementing age assurance. Age assurance is an umbrella term which includes both age verification and age estimation solutions. Age verification measures determine a person's age to a high level of certainty, while age estimation technologies provide an approximate age or age range.

While age assurance has been recently discussed with respect to various online safety reforms, it is important to be reminded that the Government's age assurance trial is still being conducted by the Department of Infrastructure, Transport, Regional Development, Communications & the Arts. We understand this trial is designed to evaluate the maturity, effectiveness, and readiness for use of available age assurance technologies.[20] It would therefore be prudent and logical to refer to the outcomes of the trial before considering age assurance measures in the context of privacy reform.

In the meantime, public commentary from experts suggests the likelihood of policy failure with such a trial due to the lack of feasibility of these technologies, which can be easily circumvented by users and legitimate public concerns regarding privacy and security.

We caution against infringement upon privacy and security, especially pertaining to the data of children, which may arise from implementing such age assurance technologies. This was previously acknowledged by the Government in response to eSafety's Roadmap for Age Verification. In particular, the Roadmap found that age assurance technologies were immature and presented their own privacy, security, effectiveness and implementation issues; hence the Government was unable to mandate age assurance at the time.[21] We do not consider that technology would have advanced dramatically over a year to address those legitimate concerns. However, we would be interested to see if the Government's age assurance trial suggests otherwise.

To reiterate, the video game industry follows strict age-appropriate standards, and user interactions are often limited and subject to parental controls or age restrictions.

In advocating for responsible gameplay, the video game industry supports the significance of parental and caregiver participation, enabling them to play an active role in setting up

---

[19] Australian Government Response to the Privacy Act Review Report (September 2023), p. 14.

[20] Information about the age assurance trial can be found here: https://www.tenders.gov.au/Atm/Show/adb00180-20b7-4396-af3d-acb3f87b5d58.

[21] Australian Government response to the Roadmap for Age Verification, (August 2023), p. 2, https://www.infrastructure.gov.au/sites/default/files/documents/government-response-to-the-roadmap-for-age-verification-august2023.pdf.

parental controls. With settings prioritising safety and privacy, parents and carers can make informed choices regarding content access and online interactions, tailored to their child's age and maturity level. This approach facilitates meaningful communication and oversight between parents or carers and their children in online activities.

Ensuring children's safety online hinges on parental and caregiver consent, and our industry has led the way in creating effective parental control tools across different devices and platforms. These tools enable parents and caregivers to customise content access, oversee in-game spending, and supervise online communication based on their preferences and their child's requirements.

Our industry endeavours to offer transparent and dependable guidance to users and their parents or carers through age-specific account types and thorough pre-contractual information. The industry's commitment to responsible gameplay practices, demonstrated by its adherence to age rating systems globally, including in Australia, implements objective content assessment, responsible advertising, consumer grievance mechanisms, and rigorous privacy standards.

Preserving robust privacy policies and nurturing a secure online game atmosphere are fundamental principles of our industry, empowering users to retain control over their personal information and to resolve any privacy issues that may arise.

Recommendations:

- **As the Government has committed to developing the COP Code, the Code should be referring to services that are 'targeted at, or directed to, children', which is less ambiguous than the term 'likely to be accessed by children'.**
- **Should the OAIC be assigned with the responsibility for developing and consulting on the COP Code, the Bill should explicitly require the OAIC to meaningfully consult with relevant industry stakeholders who are directly impacted by the COP Code. Consultation should at least occur during the development and public consultation stages of the Code.**
- **For the COP Code development process to be effective, it is also important that there be sufficient time allocated to the process, flexibility for consideration of relevant issues, clearly scoped and avoid overlapping requirements between the COP Code and other regulatory instruments (e.g. under the Online Safety Act), and mutual transparency between the regulator and industry stakeholders to ensure a more productive process.**
- **It would be prudent and logical to refer to the outcomes of the Government's age assurance trial before considering age assurance measures in the context of privacy reform. In the meantime, we caution against infringement upon privacy and security, especially pertaining to the data of children, which may arise from implementing age assurance technologies, to give effect to the COP Code. We would be keen to understand whether these concerns are addressed from the Government's separate age assurance trial.**

- **Regardless, the video game industry has long spearheaded parental control capabilities in video game services to address child access to age-inappropriate games, based on global industry best practice. Ensuring children's safety online hinges on parental and caregiver consent. Our industry has led the way in creating effective parental control tools across different devices and platforms. Parents and carers are therefore empowered to use technological and/or non-technological means to help manage their children's viewing and playing experiences, as opposed to deferring to the government. This nuance needs to be better appreciated in how online safety and privacy is approached for video games by government.**

3. Overseas data flows

The Bill includes a provision for overseas data flows. This reflects the Government's agreement that "[t]he free flow of information [with appropriate protections] across borders is an increasingly important component of international trade and digital service models".[22]

As expressed in IGEA's previous submission, we are supportive of an overseas data flows provision that enables interoperability with overseas data protection frameworks such as the European Union's (EU) General Data Protection Regulation (GDPR). We continue to support an adequacy decision between Australia and the EU that would enable free flow of data between the regions.[23] International regulatory coherence between Australia and data management frameworks of larger markets abroad are crucial to facilitate free flow of information and international digital trade. In the video game context, it will aid in friction-free compliance and enhanced accountability, and to facilitate cross-border expansion for the local Australian game industry.

We therefore support the inclusion of an overseas data flows provision in the Bill as one further step towards enabling international regulatory coherence.

Further, we understand that the Privacy Act's requirements for cross-border disclosure of personal information to overseas recipients under Australian Privacy Principle (APP) 8.1 are less prescriptive than the EU GDPR Articles 44–50 requirements for transfers of personal data to third countries.[24] There would be a practical benefit for the Australian Government (via the relevant Minister) to favourably consider 'whitelisting' countries that already have an adequacy decision with the EU, where the Governor-General could then make regulations to prescribe that these specific countries provide substantially similar protections to the APPs, in accordance with section 100(1A) of the Bill. Such countries include, for example, the United Kingdom and Japan. The Bill should also clarify Australia's

[22] Australian Government Response to the Privacy Act Review Report (September 2023), p. 16.

[23] See: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[24] See: https://gdpr-info.eu/chapter-5/.

position on 'onward transfers', where personal information that was first transferred from Australia to a whitelisted country (Country A), is further transferred from Country A to another country (Country B).

In terms of the proposed test for 'adequacy' to facilitate secure overseas data flows between Australia and a given country, the Bill uses the term 'substantially similar' as the certification threshold.[25] The Explanatory Memorandum explains that:[26]

> 'Substantially similar' means that the law or binding scheme provides a comparable, or a higher level of privacy protection to that provided by the APPs. When determining this, the overall effect of the law or scheme is considered – each provision of the law or scheme is not required to correspond directly to an equivalent APP.

While we understand the explanation, we question whether it would be better (and more seamless) to adopt similar terms as those already established overseas such as in the EU GDPR e.g. 'adequate'.[27]

Recommendations:

- **While not in the scope of this Bill, the Australian Government should continue to work on a path towards an adequacy decision to facilitate overseas data flows between Australian and the EU.**
- **The EU's GDPR be prioritised at the first opportunity, in accordance with the overseas data flows provision of the Bill.**
- **The Australian Government (via the relevant Minister) should favourably consider 'whitelisting' countries that already have an adequacy decision with the EU, where the Governor-General could then make regulations to prescribe that these countries provide substantially similar protections to the APPs, in accordance with section 100(1A) of the Bill e.g. the United Kingdom and Japan. The Bill should also clarify Australia's position on 'onward transfers', where personal information that was first transferred from Australia to a whitelisted country (Country A), is further transferred from Country A to another country (Country B).**
- **The Government should reconsider whether 'substantially similar' is the best term to use as the certification threshold for establishing overseas data flows between Australia and a given country. We would prefer the term 'adequate' or 'similar'.**

Thank you for allowing IGEA to contribute to this inquiry. For more information on any issues raised in this submission, please contact us at policy@igea.net.

[25] Privacy and Other Legislation Amendment Bill 2024, section 100(1A).

[26] Explanatory Memorandum to the Bill, pp. 44-45.

[27] See: https://gdpr-info.eu/art-45-gdpr/.