Submission to the Office of the Australian Information Commissioner

Response to Automated Decision Making Obligation (APP 1) Issues Paper

June 2026












IGEA

interactive games & entertainment association

1. Overview

The Interactive Games & Entertainment Association (IGEA) welcomes the opportunity to provide a submission to the consultation on the Issues Paper that will inform the Guidance for Transparency in Automated Decision Making (ADM), led by the Office of the Australian Information Commissioner (OAIC).

IGEA is the industry association representing and advocating for the video games industry in Australia, including developers, publishers and distributors, and the makers of the most popular game platforms, consoles and devices.

We recognise that an ADM obligation has been introduced following the passage of the *Privacy and Other Legislation Amendment Act 2024* (Cth). Taking effect from 10 December 2026, Australian Privacy Principle (APP) entities that use personal information in ADM will be required to provide information in their privacy policies about the kinds of personal information used and the kinds of decisions made using ADM.

Overall, we support the objective of enhancing transparency and enabling individuals to understand how their personal information is handled. However, the implementation of the ADM obligation must remain proportionate and reflect the comparatively low-risk profile of online games, particularly having regard to the criteria:[1]

(a) the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making, a decision; and
(b) the decision could reasonably be expected to significantly affect the rights or interests of an individual; and
(c) personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision.

In practice, automated systems used in online games are unlikely to meet all of these elements. Therefore, game companies should not be subject to the ADM obligation.

In this context, it is important to distinguish between automated systems that are determinative of outcomes affecting an individual, and systems that are experiential or incidental to the delivery of interactive entertainment. ADM in games is generally limited to real-time or session-based gameplay functions, such as matchmaking or difficulty balancing. This differs from profiling practices used in services where personal data is aggregated over time to infer preferences or influence behaviour across contexts.

It is therefore important that the Guidance explicitly recognises the low-risk and contextual nature of ADM in games. While we support the principle of providing meaningful information to individuals, entities should not be required to disclose proprietary algorithms, trade secrets or game mechanics that are essential to service integrity, competitive fairness or anti-cheat protections. Requiring detailed disclosure of ADM logic risks enabling circumvention by bad actors and undermining core gameplay systems, including safeguards designed to protect users.

[1] *Privacy and Other Legislation Amendment Act 2024* (Cth), Item 88.

The Guidance should adopt a proportionate, risk-based approach that allows entities to provide clear explanations of the purpose, context and consequences of ADM, without requiring disclosure of sensitive technical detail. This approach ensures that transparency obligations remain workable for game developers of all sizes and do not impose a "one-size-fits-all model" across sectors with very different risk profiles.

For the purposes of this submission, we will focus on the Issues Paper questions most relevant to the video games industry. For ease of reference, we summarise our key recommendations made in this submission below.

Topic	**IGEA's recommendation**
"Significantly affects rights or interests" should generally exclude ADM in video games	The OAIC should narrow the meaning of "significantly affects rights or interests" to decisions with consequential outcomes for individuals. The Australian Government has endorsed this approach in its response to the Privacy Act Review, noting that relevant decisions may include denial of consequential services or support, such as financial and lending services, housing, insurance, education enrolment, criminal justice, employment opportunities, healthcare services, or access to basic necessities such as food and water.[2] This approach is also consistent with comparable overseas privacy frameworks, such as the EU General Data Protection Regulation (as interpreted by the European Data Protection Board),[3] and US laws (e.g. the Colorado Privacy Act,[4] and the Virginia Consumer Data Protection Act[5]). Guidance on this basis would confirm that low-risk, session-based ADM functions in online games (e.g. matchmaking, moderation and anti-cheat systems) are typically contextual and protective in nature, rather than determinative of outcomes affecting individuals' rights or access to consequential services.
Rights, interests and vulnerability	The OAIC should clarify that protective, safety-by-design interventions (e.g. moderation) do not generally constitute decisions that significantly affect an individual's rights or interests. Guidance should emphasise vulnerability, particularly in relation to children, as a key contextual factor in assessing whether a threshold is met. Consideration should also be given as to how this might inform the OAIC's concurrent development of the Children's Online Privacy Code.
Significant service or support	The OAIC should recognise that online games are interactive entertainment services where data collection is incidental to gameplay, and distinguish them from services whose core model

[2] Australian Government response to Privacy Act Review Report (September 2023), p. 11, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF
[3] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en
[4] *Colorado Privacy Act*, 6 Colo Rev Stat § 6-1-1303(10) (2021)
[5] *Consumer Data Protection Act*, 59.1 Va Code Ann § 59.1-575 (2021)

Topic	IGEA's recommendation
	relies on aggregating and using personal data to make consequential decisions. Such interactive entertainment services should not be treated as "significant services or supports" under the ADM framework.
Other legal frameworks	Guidance should explicitly recognise the relevance of existing frameworks (including the *Online Safety Act 2021* (Cth), National Classification Scheme, Australian Consumer Law, UN Convention on the Rights of the Child, and relevant international data protection and privacy frameworks) in informing the meaning of "rights" and "interests". Alignment with these frameworks is necessary to avoid duplication, inconsistency or unintended conflicts across Australia's broader online regulatory landscape.
Meaning of "arranged for"	The OAIC should provide specific guidance on how "arranged for" applies to online services that depend on third-party services. In particular, it should be clear that "arranged for" is confined to controllers of personal information, who are responsible for making decisions on the purposes and means of how personal information is processed within an ADM. By contrast, processors of personal information generally have no control over this decision and should not be within scope. For example, game developers are often contractually and technically removed from the design and implementation of ADM systems, and in those cases should not be taken to have "arranged for" such systems.
Meaningful disclosure	Guidance should clarify that meaningful ADM disclosures focus on user-understandable explanations of the purpose, context and outcomes, rather than detailed technical or algorithmic information. Entities should not be required to disclose proprietary systems or sensitive logic where doing so could compromise service integrity, competitive fairness or safety mechanisms.

2. Best practice regulation and good public policy design

In developing this submission and the recommendations, we consider that the development of the ADM guidance should be informed by established principles of best practice regulation and good public policy design.

- Principles-based and risk-based regulation: Guidance should focus on automated systems that are substantially and directly related to decisions that significantly affect individuals, ensuring regulatory effort is directed to areas of meaningful impact.
- Proportionality: Requirements should scale according to the level of risk and the nature of the service, recognising that many automated systems in online games are low-risk, session-based and not determinative of outcomes affecting rights or interests.

- Regulatory coherence: Guidance should align with existing Australian frameworks (e.g. *Online Safety Act 2021* (Cth), National Classification Scheme, Australian Consumer Law), as well as relevant international approaches (e.g. UN Convention on the Rights of the Child and comparable data protection and privacy frameworks), to avoid duplication and overreach. The OAIC's concurrent development of the Children's Online Privacy Code, including its consideration of ADM requirements, will also need to be aligned.
- Sector-specific considerations: The application of ADM obligations should recognise that online games differ materially from higher-risk sectors, including that automated systems are often real-time, session-based and incidental to gameplay, rather than determinative of outcomes affecting rights or interests.
- Safety-by-design, privacy-by-design and harm prevention: Automated systems used to protect users and maintain safe environments should be recognised as essential and distinguished from systems that determine access, rights or opportunities.

3. Responses to specific questions raised in the issues paper

3.1. Relevant factors for ADM obligation

1. In your view, what are the relevant factors to enable an entity to assess whether a computer program substantially facilitates and is directly connected to a human decision-maker's decision? For example: Degree of reliance on the ADM system output; Ability and likelihood of human override over an ADM decision; Nature of the output (advisory vs determinative); Transparency and explainability of outputs; Integration of ADM into decision-making workflow; Other. Please rank the factors using the above mentioned (1-5) ranking system and include any additional factors.

ADM in games is generally limited to real-time or session-based gameplay functions. These include:

- matchmaking and session management, which require identifiers, device information and connection data;
- moderation and safety systems, including reporting tools, automated detection of harmful behaviour and enforcement mechanisms; and
- anti-cheat and integrity systems, which protect children from unfair or harmful gameplay environments.

Such systems may fall within the broad definition of a "computer program" and, in some cases, may be characterised as substantially and directly related to making a decision. However, these systems are deployed for protective purposes, including preventing harmful behaviour and maintaining safe environments, and do not generally produce outcomes that significantly affect individuals' rights or interests.

They are integral to the core service and cannot be disabled by default without undermining the gameplay experience or compromising safety. Their outputs are primarily contextual and operational in nature, shaping the user experience and enforcing community standards in real time, rather than creating determinative outcomes that affect an individual's rights or access to services.

These data uses are typically bounded to the gameplay context and do not involve broad secondary use or long-term repurposing. As a result, they have a lower privacy risk profile and do not give rise to decisions that significantly affect an individual's rights or interests.

This differs from profiling practices in other sectors, where personal data is aggregated over time to infer preferences or influence behaviour across contexts. Outputs from such practices may influence decisions that could have significant consequences e.g. on employment, financial, health and other essential services.

Accordingly, in assessing whether a computer program is substantially and directly related to a decision, we consider that the factors that should weigh most heavily are: (1) the nature of the output; and (2) consequences of the output.

Recommendation:

- The OAIC should narrow the meaning of "significantly affects rights or interests" to decisions with consequential outcomes for individuals. The Australian Government has endorsed this approach in its response to the Privacy Act Review, noting that relevant decisions may include denial of consequential services or support, such as financial and lending services, housing, insurance, education enrolment, criminal justice, employment opportunities, healthcare services, or access to basic necessities such as food and water.[6] This approach is also consistent with comparable overseas privacy frameworks, such as the EU General Data Protection Regulation (as interpreted by the European Data Protection Board),[7] and US laws (e.g. the Colorado Privacy Act,[8] and the Virginia Consumer Data Protection Act[9]). Guidance on this basis would confirm that low-risk, session-based ADM functions in online games (e.g. matchmaking, moderation and anti-cheat systems) are typically contextual and protective in nature, rather than determinative of outcomes affecting individuals' rights or access to consequential services.

3.2. Rights, interests and vulnerability

4. What factors do you consider increase the likelihood that a decision could affect an individual's rights or interests? For example: sensitive information; vulnerable persons; intrusive practices; financial outcomes; other. Please rank using the above mentioned ranking system and list any additional factors.

5. What classes of person do you consider to be vulnerable for the purposes of considering a decision's expected effect on a person's rights or interests, and why?

[6] Australian Government response to Privacy Act Review Report (September 2023), p. 11, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

[7] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en

[8] *Colorado Privacy Act*, 6 Colo Rev Stat § 6-1-1303(10) (2021)

[9] *Consumer Data Protection Act*, 59.1 Va Code Ann § 59.1-575 (2021)

In assessing whether a decision could reasonably be expected to significantly affect an individual's rights or interests, it is important to first distinguish between decisions that impose or determine outcomes affecting an individual's rights or interests, and those that are protective in nature.

For example, in the online games context, automated actions (e.g. muting or banning) are designed to protect users and maintain safe environments. Such actions are proportionate and targeted responses to harmful behaviour that do not significantly affect the rights or interests contemplated by the ADM obligation. Instead, they form a core feature of safety-by-design practices that benefit users.

A key consideration in this assessment is the vulnerability of the individual. This reflects the approach being developed in the Children's Online Privacy Code, where the "best interests of the child" requires a holistic and context-specific assessment.

Children are a key class of vulnerable persons in this context, as recognised in Article 3 of the UN Convention on the Rights of the Child (UNCRC). The UNCRC makes clear that a child's best interests encompass not only protection from harm, but also their positive rights, including:

- recognition of children's evolving capacities (Article 5);
- the right to freedom of association (Article 15);
- the right to access age-appropriate information (Article 17);
- the right to participate in social, artistic and cultural life (Articles 30 and 31); and
- the right to play and leisure (Article 31).

Online games play an increasingly vital role in children's play, creativity, socialisation and digital literacy. Overly restrictive regulation may unintentionally limit these opportunities. The "best interests" test must therefore be applied in a balanced and evidence-based manner, recognising that children benefit from safe and age-appropriate opportunities to engage in interactive entertainment. ADM guidance should therefore recognise both the need to protect children from harm, and the importance of preserving safe and developmentally appropriate opportunities for participation.

Recommendation:

- The OAIC should clarify that protective, safety-by-design interventions (e.g. moderation) do not generally constitute decisions that significantly affect an individual's rights or interests. Guidance should emphasise vulnerability, particularly in relation to children, as a key contextual factor in assessing whether a threshold is met. Consideration should also be given as to how this might inform the OAIC's concurrent development of the Children's Online Privacy Code.

3.3. Significant service or support

6. What do you consider to be a significant service or support, for the purposes of considering whether a decision affects access to a significant service or support? For example: physical assistance/support; financial assistance; access to educational services; 'in home services'; access

to essential banking and credit services; access to telecommunications; access to essential utilities; other. Please rank using the above mentioned ranking system and add any additional factors.

We consider that "significant services or supports" should be understood as essential services (e.g. healthcare, financial services, education, telecommunications, and other essential utilities).

Online games are more appropriately characterised as interactive entertainment services, where data collection is incidental to the delivery of the user experience i.e. gameplay. They differ from services that are centred around the collection, aggregation and reuse of personal data as a core part of their service model, where such data may influence decisions that could have significant consequences, including access to essential services or supports.

Therefore, services where automated systems are used to facilitate entertainment should not generally be treated as "significant services or supports" for the purposes of the ADM obligation.

Recommendation:

- The OAIC should recognise that online games are interactive entertainment services where data collection is incidental to gameplay, and distinguish them from services whose core model relies on aggregating and using personal data to make consequential decisions. Such interactive entertainment services should not be treated as "significant services or supports" under the ADM framework.

3.4. Other legal frameworks

7. Are there any other legal frameworks or policies that the OAIC should have regard to in considering the meaning of 'rights' and 'interest'?

There are several existing legal and policy frameworks that the OAIC should have regard to in considering the meaning of "rights" and "interest" in the context of the ADM obligation:

- Online safety: The video games industry implements safety-by-design measures as a part of global best practice. These measures also reflect legal and regulatory expectations under Australia's online safety framework (*Online Safety Act 2021* (Cth) (OSA)), including obligations relating to the prevention of child sexual exploitation, grooming, extortion, bullying and other seriously harmful conduct. This framework is directly relevant to the use of automated systems for moderation and harm prevention, and highlights the importance of ensuring that privacy obligations operate coherently with existing safety requirements.
- National Classification Scheme (NCS): Video games are regulated under the scheme, with classifications providing clear guidelines on age-appropriateness and content, supporting informed decision-making by consumers and parents.

- Australian Consumer Law (ACL): The ACL includes various consumer protections (e.g. misleading or deceptive conduct, unconscionable conduct, unfair contract terms, and consumer guarantees). As consumers' rights and interests are reflected in these protections, there should be alignment between privacy obligations and the ACL.
- UNCRC: As discussed in response to questions 4 and 5, this recognises both the need to protect children from harm, and the importance of preserving safe and developmentally appropriate opportunities for participation.
- International data protection and privacy frameworks: We strongly support international regulatory coherence, including alignment with well-established overseas regimes where appropriate. Comparable regimes (e.g. EU and UK General Data Protection Regulation (GDPR)) provide guidance on concepts such as individual rights and interests. Having regard to these will enable consistency with global practices and reduce regulatory fragmentation.

Recommendation:

- Guidance should explicitly recognise the relevance of existing frameworks (including the OSA, NCS, ACL, UNCRC, and relevant international data protection and privacy frameworks) in informing the meaning of "rights" and "interests". Alignment with these frameworks is necessary to avoid duplication, inconsistency or unintended conflicts across Australia's broader online regulatory landscape.

3.5. Meaning of "arranged for"

11. Are there any scenarios relevant to the meaning of 'arranged for' that you consider require guidance? If so, why?

Online games rely on global infrastructure and third-party services as an inherent part of routine service delivery. These services often incorporate automated systems (e.g. identity management, moderation, fraud detection and other operational functions).

In practice, studios (particularly smaller ones) may have limited or no visibility or control over such services that are delivered through third parties such as global platforms. For example, a small studio publishing through a major platform may have no access to that platform's matchmaking or moderation system. In such cases, developers may be contractually and technically removed from the design and implementation of these automated systems.

Guidance should make clear that mere use of a third-party service does not, of itself, constitute "arranged for" the use of a computer program under the ADM obligation. That responsibility should rest with entities that have meaningful control over the design or implementation of the relevant automated system.

Recommendation:

- The OAIC should provide specific guidance on how "arranged for" applies to online services that depend on third-party services. In particular, it should be clear that

"arranged for" is confined to controllers of personal information, who are responsible for making decisions on the purposes and means of how personal information is processed within an ADM. By contrast, processors of personal information generally have no control over this decision and should not be within scope. For example, game developers are often contractually and technically removed from the design and implementation of ADM systems, and in those cases should not be taken to have "arranged for" such systems.

3.6. Meaningful disclosure

12. When making disclosures about ADM, the OAIC's view is that entities must ensure that meaningful and accessible information is provided to consumers. In doing so, the OAIC considers that entities should strike an appropriate balance to ensure that disclosures are: clearly articulated in plain language and easy to understand; structured to enable consumers to request further information, where required; appropriately tailored – sufficiently specific to be meaningful, while avoiding overwhelming levels of detail; organised so that similar information is grouped in a logical manner; and framed in a way that allows the information and the decision to be challenged or contested. Having regard to the above considerations, is there anything additional that entities should disclose to provide effective and meaningful disclosures about ADM?

We support the objective of enhancing transparency for individuals to understand how personal information is handled. However, the ADM disclosure requirements must remain proportionate and reflect the comparatively low-risk profile of online games.

While we support the principle of providing meaningful disclosure, entities should not be required to disclose proprietary algorithms, trade secrets or game mechanics that are essential to service integrity, competitive fairness or anti-cheat protections. Regulatory measures should avoid overly prescriptive rules that could inhibit innovation and should not adopt a "one-size-fits-all model". Requiring detailed disclosure of ADM logic risks undermining core gameplay systems and enabling circumvention by malicious actors, without delivering meaningful privacy benefits.

A proportionate, risk-based approach should allow entities to provide clear, age-appropriate explanations of the purpose, context and consequences of ADM, without requiring disclosure of sensitive technical detail. This approach ensures that entities are not expected to provide full technical specifications, while at the same time, transparency obligations remain workable for game developers of all sizes.

Recommendation:

- Guidance should clarify that meaningful ADM disclosures focus on user-understandable explanations of the purpose, context and outcomes, rather than detailed technical or algorithmic information. Entities should not be required to disclose proprietary systems or sensitive logic where doing so could compromise service integrity, competitive fairness or safety mechanisms.

IGEA supports clear and proportionate transparency obligations in relation to ADM and considers the industry is well-placed to comply where requirements are practical and appropriately targeted. We welcome ongoing engagement with the OAIC as it develops final guidance in this area.

For further questions or information about our submission, please contact us at policy@igea.net.

About IGEA

IGEA is the industry association representing and advocating for the video games industry in Australia and New Zealand. Our industry includes the developers, publishers, and distributors of video games, as well as the makers of the most popular video 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.

Among our various activities, IGEA also organises the annual Games Connect Asia Pacific (GCAP) conference for Australian game developers and the Australian Game Developer Awards (AGDAs), which celebrate the best Australian-made games each year.

Find out more: www.igea.net

Acknowledgement of Country

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.

IGEA

interactive games & entertainment association