AUSCL

AIDH
AUSTRALASIAN INSTITUTE OF DIGITAL HEALTH

SOCIAL CYBER INSTITUTE

Digital Economy Council of Australia

Submission to the OAIC Automated Decision-Making (ADM) Transparency Obligation (APP 1) Issues Paper

Australasian Society for Computers and Law (2026).
Office of the Australian Information Commissioner (OAIC).
AUSCL Policy Series PS-2026-02.

15 June 2026

Submission to the OAIC Automated Decision-Making (ADM) Transparency Obligation (APP 1) Issues Paper

Submitted 15 June 2026

AUSCL

The Australasian Society for Computers and Law (**AUSCL**) is a multidisciplinary association bringing together professionals from law, technology, government, academia and industry to advance the responsible development, governance and regulation of digital technologies. AUSCL contributes to public policy, professional education and thought leadership across areas including artificial intelligence, privacy, cyber security, digital identity, computational law, digital government, critical infrastructure and emerging technologies.

Supported by AIDH

The Australasian Institute of Digital Health (**AIDH**) is the peak body for digital health in Australasia, championing a unified voice for the professionals and leaders driving digital transformation across healthcare.

With a membership that spans clinical practice, health informatics, administration, research, and health technology, the Institute brings together the expertise shaping the future of healthcare. Its community includes more than 250 distinguished Fellows, recognised for their leadership, innovation, and contribution to the field. The vision of the Institute is "healthier lives, digitally enabled". http://www.digitalhealth.org.au

Supported by SCI

The Social Cyber Institute (**SCI**) creates new social science insights to complement technology in the fight for a more secure cyberspace. The Institute is a non-profit research centre: htttps://www.socialcyber.co

Endorsed by DECA

The Digital Economy Council of Australia (**DECA**) traces its origins back the Australian Digital Currency Commerce Association (**ADCCA**) established in 2014. ADCCA was formed as the country's leading council and representation of and for digital currency businesses and key industry participants. The organisation was formed with a mandate to act as "the leading community association dedicated to the education, policy development and promotion of Blockchain and Digital Currency in Australia". In 2019, ADCCA and Blockchain Australia merged. Blockchain Australia rebranded as the Digital Economy Council of Australia in 2024: https://deca.org.au

Executive summary

AUSCL welcomes the opportunity to comment on the OAIC's guidance for the new automated decision-making (**ADM**) transparency obligation in APP 1.

- We support a practical, technology-neutral and risk-sensitive interpretation of APP 1.7–1.9 that promotes meaningful transparency without encouraging formulaic privacy policies that obscure rather than explain ADM.
- In addition to our specific comments below, the guidance issued by the OAIC should aim to be very practical, clear and easy to read for businesses (without the need for legal advice in most cases). We suggest the guidance include very clear examples with decisive calls on whether the particular activity is subject to the ADM provisions and what is required for APP entities to do as a result.
- The guidance should apply to automation that materially affects a decision-making process, including rules-based systems, statistical models, machine learning systems, generative AI tools, decision-support tools, triage systems and third-party platforms.
- We support the view that human oversight should not, by itself, take a system outside scope of the relevant provisions. The critical question being whether the automation/program materially influences the decision-making process in practice.
- We support a layered transparency model comprising:
  - concise privacy policy disclosures;
  - a linked ADM notice or register; and
  - a pathway for affected individuals to obtain further information or seek review where available under law.
- We recommend that the guidance promote practical governance measures, including ex ante assessment, procurement transparency, ongoing monitoring, auditability and clear allocation of responsibility for ADM systems.
- We encourage the OAIC to align its guidance with related legal and assurance frameworks, including administrative law, anti-discrimination law, the FOI Act Information Publication Scheme, the DTA Policy for the Responsible Use of AI in Government and emerging AI assurance frameworks.
- To promote regulatory certainty and consistent compliance, we recommend the OAIC publish a practical implementation guide with worked examples, case studies and compliance scenarios that clearly identify:
  - systems likely to be captured by APP 1.7–1.9;
  - systems unlikely to be captured;
  - factors relevant to assessing whether automation materially affects a decision-making process; and
  - transparency, governance and documentation measures likely to assist organisations in demonstrating compliance.

We are grateful to the OAIC for its acknowledgement of and reference to our (AUSCL, The Allens Hub for Technology, Law and Innovation and The Gradient Institute's) earlier submission to the Robodebt Royal Commission, concerning the use of the Trust Framework to show how the harms of Robodebt could have been mitigated. **Our submission** below is structured to align with the form issued by the OAIC.

AUSCL

Question 1 - Substantially and directly related to making a decision

Factor	Ranking	Comment
Degree of reliance on the ADM system output	5	Core indicator. Reliance is best assessed in practice, not merely by policy wording. If decision-makers routinely accept, copy or follow the output, the system is substantially related.
Ability, competency and likelihood of human override	5	Important, but the focus is best placed on genuine and exercised override, not theoretical authority. Rubber-stamping, automation bias and workflow pressure are relevant factors favouring inclusion. An additional factor should also be the competency and authority of the human reviewer. Logging of human review decisions (or lack of) can help identify whether human review or override is tokenistic or genuine (taking lesson from UK ICO). Noting the EU AI Act, Article 26(2), requires deployers to assign human oversight to persons with "the necessary competence, training and authority". If the reviewer lacks the competency, training or authority to override, then the decision is effectively made by the system/program.
Nature of the output: advisory vs determinative	5	A determinative output is clearly in scope. Advisory outputs are also in scope where they score, rank, recommend, prioritise, summarise evidence or narrow options in a way that materially shapes the outcome.
Integration into decision-making workflow	5	Highly relevant. Systems embedded in case management, intake, risk scoring, eligibility, triage, pricing, recruitment, claims handling or compliance workflows are more likely to be directly connected.
Transparency and explainability of outputs	4	Relevant to compliance and risk. Low explainability does not narrow the obligation; it increases the need for disclosure and supporting governance.
Effect on evidence or reasons	5	Additional factor. If the program selects facts, summarises records, drafts reasons, identifies issues, infers risk or characterises a person, it is substantially related.
Practical optionality	4	Additional factor. If a staff member cannot readily make the decision without the output, or must justify departure from it, the system is materially connected. There must be a clear severing of the causal link between the output from the AI system and the final decision.

Factor	Ranking	Comment
Scale and repeatability	4	Additional factor. High-volume use increases the risk that a design error will be replicated and is a factor favouring inclusion.

Free text comments:

Other additional factors for consideration:

- **the impact and/or irreversibility of the decision:** the more severe and irreversible the decision's potential impact on an individual, the more weight should be given to whether the system's role is 'substantial' in making that decision;
- **where sensitive personal information is involved:** the threshold for what constitutes 'substantially facilitates' must be assessed more conservatively - a lower degree of reliance on the system output may still trigger the threshold because the potential harm to individuals is greater.

We recommend that the OAIC adopt a practical "material influence" test. A computer program may appropriately be treated as substantially and directly related to making a decision where its output is a material input to the decision pathway, including by scoring, ranking, triaging, recommending, summarising, drafting, validating, flagging, escalating or excluding a person from consideration.

The test could examine actual operational practice, including training, interface design, system defaults, performance targets, audit logs and the frequency of human override. This approach is consistent with ADM+S' research which found that ADM governance is most effective when it covers automation broadly, not only AI, and addresses systemic and preventative controls rather than relying only on high-level principles after harm occurs.

Question 2 - Generative AI with human oversight

Response: Yes.

Reasons:

- GPTea system summarises candidate profiles and provides recommendations about eligibility for life-changing aged-care support. Both functions are substantially and directly related to the eligibility decision. The individual reviewer has more to do and must actively reason against the GPTea recommendation to reach a different conclusion.
- The GPT's system output (eligibility recommendation) maps directly onto the decision to be made (eligibility determination). There is no intermediate transformation or independent analytical step that severs the causal chain between GPTea's output and the decision being taken.
- Human oversight does not remove the system from scope where the AI output materially shapes the facts, recommendation, reasons or decision pathway. In practice, generative AI outputs may influence decision-makers through framing effects, omission of relevant facts, hallucinated content, misplaced confidence, automation bias and time pressure.
- GPTea's summary function is not neutral. By selecting which information to include and exclude, and how to frame it, the chatbot defines the informational environment from which the

human decides. The human decision-maker may never see information that GPTea chose not to highlight.

- The decision affects access to significant support and likely involves sensitive information and vulnerable persons. This weighs strongly in favour of disclosure.
- As AI chatbots are inherently opaque, GPTea's reasoning for its eligibility recommendation is not readily explainable, auditable or reproducible.
- The guidance could usefully clarify that entities using generative AI in this way are expected to disclose the categories of personal information used; the kinds of eligibility, triage or support decisions affected; the role of the AI tool; how the eligibility recommendation was reached – in a manner that is auditable and reproducible, the existence of human review; the reversibility of a decision, and how an affected person can request further information, correction or review where available.

Question 3 - Factors increasing likelihood that a decision affects rights or interests

Factor	Ranking	Comment
Sensitive information	5	Strong indicator, particularly health, disability, biometric, genetic, racial or ethnic origin, political, religious, union, criminal record or children's information.
Vulnerable persons	5	Strong indicator because the same decision may have a greater practical effect on a child, older person, person with disability, person in crisis, migrant, financially distressed person or person with limited digital access.
Intrusive practices	5	Includes profiling, behavioural prediction, surveillance, inference of sensitive attributes, monitoring, geolocation, emotion inference or intrusive targeting.
Financial outcomes	5	Includes eligibility, debt, pricing, credit, insurance, taxation, fines, benefits, hardship, refunds and access to essential services.
Access to public or essential services	5	Additional factor. Strongly relevant to healthcare, aged care, disability, housing, education, social security, migration, justice, utilities and telecommunications.
Legal status, rights, liabilities or obligations	5	Additional factor. Includes granting, refusing, suspending, cancelling or varying a right, licence, permission, benefit, entitlement, contract right or liability.
Opportunity denial	5	Additional factor. Includes employment, education, housing, insurance, finance or public program opportunities, including non-display of opportunities.

Factor	Ranking	Comment
Duration, reversibility and contestability	4	Additional factor. Long-lasting, hard-to-detect, hard-to-correct or non-contestable impacts are factors favouring inclusion.
Group or systemic impact	4	Additional factor. A decision pathway may significantly affect rights or interests where it disadvantages a protected or marginalised cohort, even if each individual impact appears small.

Free text comments: Additional factor to consider is **material power imbalance**: Where the entity making the decision holds substantially more power than the individual (no practical alternative), the impact is more readily 'significant.' E.g. Government agencies; employers /employees; essential service providers (utilities, telecommunications); and/or tech platforms with market dominance over gig workers or sellers.

The guidance could avoid an overly narrow or purely economic interpretation of "rights or interests". The phrase can capture legal rights, entitlements, contractual rights, statutory benefits, access to significant services, reputation, livelihood, employment opportunities, education, health, safety, autonomy, privacy, dignity, equal treatment and democratic participation. We support the position that ADM is best assessed by reference to legal, human rights, privacy and anti-discrimination standards, and that vulnerable and marginalised cohorts could be considered before deployment and throughout the system lifecycle.

Question 4 - Vulnerable persons

We recommend that the OAIC avoid a closed list. Vulnerability is best understood as contextual and dynamic (noting that a person or class may be vulnerable in one context, or at one time, but not in another). Relevant classes include:

- children and young people, because they are still developing, may not understand profiling or ADM, and may experience long-term consequences from educational, health, welfare or online targeting decisions;
- older persons, particularly where decisions concern aged care, health, insurance, financial services, digital exclusion or dependency on carers;
- people with disability, chronic illness or mental health conditions, including where ADM uses health information, risk scores, accessibility assumptions or behavioural data;
- Aboriginal and Torres Strait Islander peoples, culturally and linguistically diverse communities and migrants, especially where data quality, historical bias, language barriers or institutional distrust may affect outcomes;
- people experiencing family violence, homelessness, poverty, financial hardship, unemployment, caring responsibilities or legal vulnerability;
- people in custodial, migration, welfare, health, aged-care, education, employment or other dependency relationships with government or service providers;
- people with low digital literacy, limited English proficiency, low literacy, limited internet access or limited ability to contest automated outcomes.

AUSCL

A vulnerability lens would assist entities to assess the expected effect of a decision. It would not be appropriate for this lens to be used to justify more intrusive collection or profiling. Entities could be encouraged to consult affected communities where ADM is likely to affect at-risk, vulnerable or marginalised cohorts.

Question 5 - Significant service or support

Factor	Ranking	Comment
Physical assistance/support	5	Includes disability, aged care, family violence, child protection, emergency assistance and personal care.
Financial assistance	5	Includes social security, grants, hardship support, refunds, debt relief, insurance payouts and compensation.
Access to educational services	5	Includes admission, exclusion, learning support, assessment, scholarships and disciplinary decisions.
In-home services	5	Includes aged care, disability, health, safety, housing and family support services.
Essential banking and credit services	5	Includes account access, credit, hardship, fraud flags, insurance and payment services.
Telecommunications	5	Essential for access to work, education, government services, safety and social participation.
Essential utilities	5	Includes electricity, water, gas and energy hardship decisions.
Healthcare and medicines	5	Additional example. Includes diagnosis support, triage, admission, treatment access, insurance, aged care and disability support.
Housing and accommodation	5	Additional example. Includes public housing, rental screening, homelessness support and tenancy services.
Employment and livelihood	5	Additional example. Includes recruitment, promotion, performance, rostering, workplace surveillance and access to gig work.
Migration, citizenship and policing/justice services	5	Additional example. Decisions in these domains can affect liberty, family unity, legal status and safety.

Free text comments: Additional factor: **Access to transport services / mobility support** (Ranking 5) Example: For individuals in remote areas, persons with disability, or elderly persons, access to transport is essential for participation in society. Decisions here can affect access to work, healthcare and social/wellbeing.

A service or support may be considered significant where refusal, delay, differential treatment, escalation, exclusion or price manipulation could materially affect a person's health, safety, dignity, livelihood, legal position, financial stability, autonomy, access to opportunity or participation in society. Government services more broadly fit into this category. Significance is best assessed by context, including the person's circumstances, availability of alternatives, urgency, reversibility and whether the service is essential or quasi-essential.

Question 6 - Other legal frameworks and policies

We invite the OAIC to have regard to the following legal frameworks, Australian Standards, prudential standards, industry codes and best-practice instruments, as well as international law comparators, when interpreting "rights" and "interests". These examples do not expand APP 1.7 beyond its text, but they provide useful, sector-tested indicators of when ADM is likely to affect an individual in a legally or practically significant way.

Where appropriate, it would be extremely helpful to businesses to understand what Standards the OAIC believes address the core elements of compliance with the ADM requirements and/or to assess the relevance of the ADM requirements on their activities.

Core legal and public-sector frameworks - Australia

- Privacy Act 1988 (Cth), including APPs 1, 3, 5, 6, 10, 11, 12 and 13, and the broader Privacy Act Review reforms agreed or agreed in principle by government.
- Administrative Review Tribunal Act 2024 (Cth), Administrative Decisions (Judicial Review) Act 1977 (Cth), Acts Interpretation Act 1901 (Cth) s 25D and principles of procedural fairness, lawful authority, relevant and irrelevant considerations, reasons, merits review and judicial review.
- Freedom of Information Act 1982 (Cth), especially the Information Publication Scheme and operational information obligations for government decision-making systems.
- Commonwealth Ombudsman Automated Decision-Making Better Practice Guide and relevant Robodebt Royal Commission findings concerning legality, culture, accountability, independent assurance and oversight.
- Australian Human Rights Commission guidance and Commonwealth, state and territory anti-discrimination laws, including frameworks addressing disability, age, race, sex, family responsibilities and indirect discrimination.
- International human rights instruments to which Australia is a party, including instruments concerning privacy, equality, social security, health, education, children's rights and rights of persons with disability (including International Covenant on Civil and Political Rights (**ICCPR**).
- Administrative law – common law duty to accord 'procedural fairness' (as per High Court decision in *Kioa v West (1985) 159 CLR 550* when public officials interpret statutes by reference to rights, interests and/or legitimate expectations. Courts have broadly interpreted

as encompassing legal rights, economic, reputational, relational interests (falling short of legal rights) and legitimate expectations (e.g. as created by past practices, policy or representations). This appears to be directly analogous to APP 1.9 and provides a well-developed body of authority on what constitutes an 'interest' that gains legal protections.
- Digital Transformation Agency Policy for the responsible use of AI in government and AI transparency statement standard.
- NSW AI Assurance Framework, NSW Ombudsman ADM work, NSW Information and Privacy Commission work and WA Privacy and Responsible Information Sharing Act 2024 Principle 10.

International Law comparators

- UK *Data (Use and Access) Act 202* (**UK DUAA**), new UK GDPR Article 22A – 'legal effect' or 'similarly significant effect' and regulation-making power for specifics. Closest comparator and sets a minimum threshold/floor for Australian interpretation.
- Updated ICO guidance on ADM (consultations on which recently closed on 29 May 2026) which highlights detailed examples of 'similarly significant effects' (e.g. financial, access to services, behavioural etc).
- EU GDPR, Article 22 (incl. Recitals and guidance on ADM)
- EU AI Act high-risk system concepts
- Canadian Charter of Rights and Freedoms / Canada's Directive on Automated Decision-Making
- Colorado AI Act (Feb 2026) – and definition of '*consequential decision*'
- California CCPA/CPRA — Final ADMT Regulations (2025) (effective 2027) – re definition of '*significant decisions*' and '*substantially facilitates*' drafting history
- OECD Legal Instruments — OECD Recommendation on Artificial Intelligence (2019, as updated 2024)

Australian Standards and standards adopted for Australian use

- AS ISO/IEC 42001:2023, Artificial intelligence - Management system: directly relevant to AI governance, leadership accountability, risk treatment, impact assessment, human oversight, monitoring, documentation and continual improvement.
- AS ISO/IEC 23894:2023, Information technology - Artificial intelligence - Guidance on risk management: relevant to identifying, analysing, evaluating and treating AI risks, including privacy, bias, transparency, reliability and downstream effects on individuals.
- AS ISO/IEC 38507:2022, Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations: relevant to board and senior executive accountability for AI/ADM use, including strategic direction, evaluation and monitoring.
- AS ISO/IEC 22989:2023, Artificial intelligence concepts and terminology: useful for consistent terminology in OAIC guidance, particularly for distinguishing AI, machine learning, model outputs, automation and human-in-the-loop controls.
- AS ISO/IEC 23053:2023, Framework for Artificial Intelligence systems using machine learning: useful for describing AI system components, data flows and points of human or automated intervention in ADM workflows.

- AS ISO 31000:2018, Risk management - Guidelines: relevant to proportionality, risk ownership, risk criteria, risk treatment and ongoing review of ADM systems that may affect rights or interests.
- AS/NZS ISO/IEC 27001:2023, Information security management systems - Requirements, and related ISO/IEC 27002 controls: relevant where ADM systems use personal information, integrate with third-party systems or create cyber, integrity or availability risks.
- ISO/IEC 27701:2025 privacy information management requirements and ISO/IEC 29100:2024 privacy framework: relevant to privacy-by-design, privacy risk management, role allocation, notice and data handling in technology systems that process personal information.
- AS ISO/IEC 42006:2025, which concerns certification bodies for AI management systems, may also be useful where the OAIC considers how entities evidence conformance, assurance or supplier claims about AI management systems.

Australian government, prudential and sector codes adopted by industry

- Australian Government Voluntary AI Safety Standard and AI Ethics Principles, especially guardrails on accountability, risk management, data governance, testing, human oversight, transparency, contestability and stakeholder engagement.
- APRA Prudential Standards CPS 230 Operational Risk Management and CPS 234 Information Security, particularly for banks, insurers and superannuation entities using ADM in credit, claims, fraud, hardship, member services, outsourcing or critical operations.
- ASIC Regulatory Guide 271 Internal dispute resolution, the ePayments Code, credit reporting codes and AFCA approaches to fairness, reasons and vulnerability: relevant where ADM affects access to credit, payments, complaints, hardship or financial services.
- Australian Banking Association Banking Code of Practice and related vulnerability guidance: relevant to banking decisions affecting credit, hardship, account access, fraud holds, customer vulnerability and guarantor/customer protections.
- General Insurance Code of Practice and Life Insurance Code of Practice: relevant to underwriting, pricing, claims triage, claim denial, fraud detection, catastrophe responses, vulnerability and access to information relied upon in claims handling.
- Telecommunications Consumer Protections Code C628:2019 and related ACMA/TIO guidance: relevant where ADM affects service connection, billing, credit management, debt collection, hardship, disconnection or complaint handling.
- Consumer Data Right rules, standards and privacy safeguards: relevant where ADM relies on consumer-authorised data sharing, data quality, consent flows, accredited data recipients or action initiation.
- Advertising, marketing and online safety codes, including AANA codes and digital platform codes where relevant: useful for targeted advertising, profiling, exclusion from opportunities, age-appropriate design and manipulation risks.

We recommend that OAIC guidance expressly clarify that entities are not expected to treat standards or industry codes as a substitute for APP compliance. Rather, those instruments can be used as practical evidence of reasonable governance, assurance, procurement, monitoring and disclosure practices.

This approach is consistent with submissions already made, for example, by the ADM+S and HTI, which emphasise on broad ADM coverage, procurement transparency, independent oversight, ex ante controls, auditability and meaningful accountability.

Recommendation: Creation of a digital legislative twin

AUSCL strongly recommends that, given the volume and overlap of privacy, administrative law, anti-discrimination, consumer protection, cyber security, AI governance, prudential and industry code requirements, the OAIC consider a non-binding **digital legislative twin** for the ADM transparency obligation.

This could provide:

- **plain-language obligation maps** linking APP 1.7–1.9 to related legal, standards and industry code requirements (we recommend the use of various tools, including Knowledge Maps);
- **decision trees and worked examples** to help entities assess rights, interests, vulnerability, access, contestability and accountability;
- **model disclosure artefacts** for privacy policies and layered notices;
- **machine-readable schema** to support consistent implementation and future regulatory interoperability.

This would improve clarity, reduce duplicated interpretation costs and support consistent, risk-based ADM compliance across sectors. AUSCL's Future Law Working Group would welcome the opportunity to discuss with the OAIC and other regulators how such an approach / solution could be developed and piloted within ADM / AI / Privacy context.

Question 7 - Differential pricing edge case

Response: Yes, on the stated facts Marco's interests are significantly affected.

- The price increase is approximately 186% higher than the comparator price ($100 compared with $35). It materially impairs access to the product for Marco, who does not have enough disposable income to purchase it.
- The use of address as a proxy for wealth is crude, potentially misleading and may produce unfair outcomes. It can also infer financial circumstances from location without adequate transparency.
- Differential pricing should not be assessed by percentage alone. The proper test should consider percentage, dollar amount, significance of the good or service, vulnerability, alternatives, cumulative impact and whether sensitive or proxy-sensitive data is used.

Threshold: For ordinary consumer goods, we suggest guidance that a differential price may significantly affect interests where the difference is substantial in context, for example 20% or more, or a lower threshold where the dollar amount is material, the person is vulnerable, the good or service is important, or the practice is systematic, opaque or based on sensitive/proxy-sensitive data. For essential or significant services, even a 5-10% difference may be significant where it materially affects access or imposes hardship.

AUSCL

Factor	Ranking (1-5)	Comment
Dollar amount of differential pricing	4	Important, but should not be determinative. A smaller dollar amount may be significant for a vulnerable person or for repeated transactions
Significance of the product or service	5	Very important. Differential pricing affecting essentials, education, health, utilities, finance, insurance, employment or access to information should be treated as more likely significant

Question 8 - Discriminatory targeted job ad

Response: Yes.

Reasons:

- The non-display of the job advertisement is a practical exclusion from an employment opportunity. APP 1.9 expressly contemplates that doing a thing includes refusing or failing to do a thing; therefore a failure to serve or promote an opportunity can be a relevant decision or decision-like act.
- The decision materially affects Rafqa's interests because it limits employment options at the point of opportunity. It also raises anti-discrimination concerns because gender is used to prioritise male candidates based on historical workforce composition.
- The guidance should treat algorithmic targeting, ranking, demotion, suppression, non-display and exclusion from consideration as capable of being decisions or things substantially and directly related to making decisions, especially in employment, education, housing, financial services and essential services.
- It should not be necessary for Rafqa to prove that she would have obtained the role. The relevant impact is loss of a fair opportunity to know about and compete for the role.

Question 9 - Meaning of arranged for

Response: Yes.

The OAIC could usefully provide detailed guidance on the following scenarios:

- **Third-party platforms and marketplaces:** where an entity uses a recruitment, advertising, insurance, credit, claims, fraud, identity verification or platform service that algorithmically ranks, excludes, targets, prices or prioritises individuals.
- **Embedded vendor tools:** where ADM functionality is built into CRM, HRIS, case management, contact centre, claims, underwriting, risk, learning management or productivity tools.
- **Generative AI used by staff:** where an employer permits, encourages or directs use of AI tools to summarise evidence, draft reasons, recommend decisions, conduct performance reviews or triage cases.
- **Outsourced decision processes:** where a supplier conducts screening, scoring, identity verification, fraud detection, eligibility assessment or customer segmentation on behalf of the entity.
- **Joint arrangements and data sharing:** where multiple entities contribute data, configure rules or benefit from a shared ADM system.

- **Open-ended APIs and configurable systems:** where the entity does not own the model but configures thresholds, prompts, business rules, risk appetite, target audiences or escalation logic.
- **Shadow ADM:** where an entity has not formally procured ADM but staff use tools in recurring decision workflows with management knowledge, acquiescence or inadequate controls.

The **key question** could usefully be: Whether the entity caused, authorised, procured, configured, embedded, materially relied on or knowingly permitted the ADM use in its decision pathway? Entities should not avoid the obligation by outsourcing, using standard SaaS products or labelling the supplier as the "operator". Guidance should require supplier due diligence, contractual transparency, audit rights, documentation of ADM uses, testing obligations, incident reporting and clear responsibility for privacy policy disclosures.

Question 10 - Extent of disclosure

Response: Yes.

The OAIC's principles provide a strong foundation for *how* disclosures should be communicated. However, drawing on overseas frameworks, there are additional substantive elements that we consider the OAIC should require for entities to consider disclosing to ensure ADM transparency is genuinely *meaningful*.

We support meaningful, accessible and layered disclosure. Privacy policies should not become technical manuals, but they must provide enough information for a reasonable person to understand when ADM is used, what personal information is used, what kinds of decisions are affected and where to go for more information.

We recommend that the OAIC propose a range of methods for organisations to provide this information to individuals. For example, the California CCPA differentiates between:

1. 'just-in-time'/'pre-use' notices (provided before ADM processing begins e.g. what will happen; what data will be used; that ADM is involved; how to opt out (if available);
2. decision-information (the outcome; that ADM was involved; how to challenge and/or complain etc); and
3. post-decision access rights (information available after a decision is made, upon request - e.g. how the system reached its output; what data was weighted; why alternatives were not chosen).

This tri-track approach recognises that information needs differ depending on timing - and prevents the privacy policy from attempting to serve all functions simultaneously - which inevitably results in either over-disclosure (overwhelming) or under-disclosure (meaningless).

AUSCL notes that, as APP entities increasingly adopt automated decision-making (ADM) systems, there is a risk that privacy policies may become excessively lengthy and complex if required to contain detailed disclosures regarding all ADM activities. This may inadvertently reduce accessibility, comprehension and practical transparency for individuals. AUSCL encourages consideration of a layered disclosure approach, whereby privacy policies clearly identify the use of ADM and direct individuals to a dedicated, readily accessible source containing prescribed

information about relevant ADM systems. Such an approach may better balance transparency objectives with readability and usability.

We recommend that the OAIC prepare or recommend a standard disclosure architecture. Our preliminary thoughts are that the following fields be included:

- **Plain-language summary:** what ADM is used for, why it is used, and the kinds of decisions affected.
- **Decision categories:** the categories of decisions made solely by computer programs and those materially assisted by computer programs. This should also clarify *what function* the computer program performs in relation to the decision—whether it makes the decision autonomously, recommends an outcome, filters or prioritises information, generates a risk score, narrows available options etc.
- **Personal information categories:** the kinds of personal information used, including inferred, derived, observed, sensitive and third-party information – and the *source* of that information – particularly where the information is not directly collected from the individual but is sourced from a third party or inferred or derived from behavioural tracking.
- **Role of the system:** whether the system scores, ranks, triages, recommends, drafts, verifies, flags, escalates, predicts, prices, targets or determines an outcome.
- **Third party Involvement:** where the computer program is provided, operated, or hosted by a third party (e.g., a SaaS vendor, a contracted service provider, or a data broker providing input scores), entities should disclose this fact.
- **Logic Involved in decision-making:** This does not mean disclosure of any proprietary technology or commercial in-confidence source code – but it does require disclosing the general reasoning process in how personal information was used in the decision-making process (e.g. *'we assess eligibility by weighting your income, assets, care needs, and living arrangements'*). Known limitations of the system should also be highlighted (e.g. taking lesson from Canada's Algorithmic IA tool).
- **Human involvement:** whether human review occurs, when it occurs, whether it is genuine, and whether staff can override or reverse outputs.
- **Practical Consequences:** the likely practical consequences of the decision for affected persons, including benefits, refusals, delays, exclusions, differential pricing, prioritisation, escalation or altered service levels. This enables the individual to understand what is at stake and whether to challenge the decision.
- **Further information pathway:** a contact point and process (including timeframes) for requesting further information, correction, reasons, internal review, external review or complaint pathways where available. This information should also be available at the point that the decision is taken - not just in the privacy policy.
- **Governance statement:** a concise explanation of safeguards and evaluations completed for factors such as, accuracy, bias, discrimination, including such as testing, monitoring, bias assessment, privacy impact assessment, security controls, procurement controls, audit logs and periodic review.
- **Update history:** date of last update and material changes to ADM uses.
- **Right to opt-out of ADM**: information on whether – and how - an individual can choose to have their matter assessed by a human decision-maker without ADM involvement, or through an

alternative pathway. This could be included in the right to challenge decisions made (after use of ADM) or a right provided at the outset – depending on the circumstances of the matter.

- **Accessible formats:** child-appropriate, disability-accessible, multilingual or community-specific versions where relevant.
- **Public register/linking:** for government agencies and high-impact entities, link privacy policy disclosures to a public ADM/AI transparency statement or register, including relevant IPS material where applicable.

We recommend that the OAIC consider providing model wording, examples and a disclosure template/mechanism. The template could distinguish between low-risk administrative automation and high-impact ADM.

It could also make clear that commercial confidentiality does not justify withholding the existence, purpose, decision categories, personal information categories or accountability pathway for ADM. Where technical details cannot be publicly disclosed, entities could still provide a meaningful explanation and preserve auditable technical documentation for regulators and oversight bodies. AUSCL would welcome the opportunity to workshop model wording or templates with the OAIC.

To support practical transparency, consideration could also be given to interactive digital interfaces that allow users to navigate information at varying levels of detail, according to their individual needs and interests. For example:

- **Expandable sections**: A summary heading (e.g: '*How we use AI in assessing your eligibility'*) that expands to reveal more details when clicked;
- **Hover tooltips**: Technical terms (e.g: '*profiling', 'risk score'*) explained in plain language on hover tools;
- **Decision flowcharts:** A visual representation showing how data flows through the system, where human review occurs, and where the final decision is made;
- **Personalised dashboards**: For entities with customer portals (e.g: banks, insurers, government services), a section where the individual can view which automated decisions have been made about them, what data was used, and how to request review etc.

Further, the **EU GDPR (Article 12(7)) and the EU AI Act** both contemplate the use of standardised icons to convey key information at a glance, which is a very useful and recommended way to standardise and ensure comparability with how information is presented across entities. These do not replace the text required to be presented but work well to support transparency for low-literacy or multi-lingual audiences – or for mobile interfaces where space is limited e.g.

- Human oversight icon (e.g: a person with a checkmark) indicating that a human reviews the output before it is applied;
- 'Solely automated' icon (e.g: a robot) indicating that only ADM is used or that no human is in the loop;
- 'Challenge or Complain available' icon (e.g: a speech bubble with a question mark) linking to the mechanism to challenge or complain re an ADM decision;
- Sensitive information indicator (e.g: a shield icon) indicating that sensitive personal information is used as an input.

In addition, in Europe, color-coded risk rating scales - analogous to energy efficiency labels or food quality ratings (e.g: the French Nutri-Score) - have been proposed for AI ethics and trustworthiness, which can also be added to the above.

Further, the OAIC could consider authorising the use of visually consistent 'ADM Facts' panels to appear alongside or linked from ADM-related interactions, highlighting the minimum information required on transparency, for example:

Field	Example of content
Decision-type	Aged-care eligibility assessment
System Role	Summarises your profile; recommends eligibility
Data Inputs Used	Financial information (including as derived from third party banking information provided); health information; living arrangements
Human Oversight	Yes. Human assessor reviews recommendation at [X] stage and before final decision
Override Rate	[X]% of recommendations changed by human reviewer in past 12 months
Last Evaluated	March 2026
How to Challenge or Complain	Contact [*insert details*] within 28 days

We would welcome the opportunity to workshop additional model wording, templates, icons and standardisation methods with the OAIC, including the identification of opportunities for process automation and safe deployment of AI agents.

Concluding recommendations

We make the following concluding recommendations:

- Adopt a broad, technology-neutral interpretation of computer program and ADM, covering rules-based systems, AI, machine learning, generative AI and decision-support systems.
- Apply a practical material influence test for "substantially and directly related".
- Treat human oversight as a factor, not an exclusion from the obligation.
- Use a contextual approach to "significantly affect rights or interests", including vulnerability, opportunity denial, essential services, cumulative impact and systemic discrimination.
- Provide specific guidance for third-party ADM, procurement, SaaS tools, platform targeting and generative AI use by staff.
- Recommend layered disclosures and model privacy policy wording, supported by public ADM/AI registers and FOI IPS alignment for government agencies.
- Align APP 1 guidance with administrative law, human rights, anti-discrimination, FOI, DTA responsible AI policy, AI assurance frameworks and emerging high-risk AI guardrails.

- Encourage ex ante assessment, ongoing monitoring, auditability, error notification, accessible review pathways and clear allocation of responsibility.

AUSCL and its Contributors would be pleased to engage further with the OAIC regarding this submission.

We would welcome the opportunity to respond to any questions, provide additional information where helpful, and facilitate discussions with multidisciplinary experts across law, privacy, technology, digital health, governance and public policy to support the development of practical and effective guidance.

References

1. Office of the Australian Information Commissioner, *Automated Decision-Making Transparency Obligation (APP 1) Issues Paper*, 18 May 2026.
2. Office of the Australian Information Commissioner, *Automated Decision-Making Transparency Obligation (APP 1) Issues Paper Submission Questions*, May 2026.
3. Bello Villarino, J.M., Carney, T., Weatherall, K., Matulionyte, R., Thomas, J., Henman, P. and Lenard, V., *Submission to the Attorney-General's Department consultation paper on ADM Reform*, ARC Centre of Excellence for Automated Decision-Making and Society, 15 January 2025.
4. Sacher, S. and Santow, E., Human Technology Institute, University of Technology Sydney, *Use of Automated Decision-Making by Government*, submission to the Attorney-General's Department, 28 January 2025.
5. Commonwealth Ombudsman, Office of the Australian Information Commissioner and Attorney-General's Department, *Automated Decision-Making: Better Practice Guide*, March 2025.
6. Digital Transformation Agency, *Policy for the responsible use of AI in government* and *Standard for AI transparency statements*.
7. Royal Commission into the Robodebt Scheme, *Report of the Royal Commission into the Robodebt Scheme*, 7 July 2023.
8. UK Information Commissioner's Office and The Alan Turing Institute, *Explaining decisions made with AI*.
9. EU AI Act and *Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject - General Data Protection Regulation* (GDPR): URL: https://gdpr-info.eu/art-12-gdpr/
10. The Data Use and Access Act 2025 (DUAA) - summary of the changes to data protection law | ICO. URL: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-duaa-summary-of-the-changes/
11. ICO consultation on the draft guidance about automated decision-making, including profiling | ICO [May 2026]. URL: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2026/03/ico-consultation-on-the-draft-guidance-about-automated-decision-making-including-profiling/
12. Canada - Algorithmic Impact Assessment tool - Canada.ca. URL: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html
13. California CCPA – Final Regulations Text. URL: https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf
14. California - Fact Sheet: Draft Automated Decision-making Technology Regulations. URL: https://cppa.ca.gov/meetings/materials/adt_regulations.pdf
15. Standards Australia, *AS ISO/IEC 42001:2023, Information technology – Artificial intelligence – Management system*.
16. Standards Australia, *AS ISO/IEC 23894:2023, Information technology – Artificial intelligence – Guidance on risk management*.
17. Standards Australia, *AS ISO/IEC 38507:2022, Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations*.

18. Standards Australia, *AS ISO/IEC 22989:2023, Information technology – Artificial intelligence – Artificial intelligence concepts and terminology*; and *AS ISO/IEC 23053:2023, Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)*.
19. Standards Australia, *AS ISO 31000:2018, Risk management – Guidelines*; and *AS/NZS ISO/IEC 27001:2023, Information security, cybersecurity and privacy protection – Information security management systems – Requirements*.
20. Australian Government, *Voluntary AI Safety Standard* and *Australia's AI Ethics Principles*.
21. Australian Prudential Regulation Authority, *Prudential Standard CPS 230 Operational Risk Management* and *Prudential Standard CPS 234 Information Security*.
22. Australian Banking Association, *Banking Code of Practice* and *Customer Vulnerability Guideline*.
23. Insurance Council of Australia, *General Insurance Code of Practice*; and Council of Australian Life Insurers, *Life Insurance Code of Practice*.
24. Communications Alliance, *Telecommunications Consumer Protections Code C628:2019 Incorporating Variation No. 1/2022*.

AUSCL

Contributors

AUSCL Data and Privacy Working Group

AUSCL Future Law Working Group

[redacted], Partner, Gadens

Atmos Privacy Risk & Digital Law Team

[redacted] Fellow Social Cyber Institute

[redacted] Social Cyber Institute

[redacted] Director, Social Cyber Group

[redacted], Red Beard Consulting

Contact Details

contact@auscl.org

Attention: AUSCL Lead Policy Analyst

Disclaimer

This submission has been prepared by the above Contributors for the purpose of contributing to public policy, law reform and regulatory discussions.

The views and recommendations expressed in this submission do not necessarily reflect the views of any individual member, contributor, employer, client, government agency, academic institution or other organisation with which a contributor may be associated.

This submission is intended to provide general information and policy analysis only. It does not constitute legal advice, professional advice or any other form of advice and should not be relied upon as such. Readers should obtain independent professional advice appropriate to their circumstances.

This submission has been informed by the expertise of the Contributors' members and working groups across law, technology, government, academia and industry. Participation in the development of this submission does not imply endorsement of every view, recommendation or conclusion contained within it.

While reasonable care has been taken in the preparation of this submission, the Contributors make no representation or warranty as to the completeness, accuracy or currency of the information contained in it and accepts no liability for any loss or damage arising from reliance upon its contents.

Copyright © Australasian Society for Computers and Law (AUSCL). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited.

Suggested citation

Australasian Society for Computers and Law (2026). Office of the Australian Information Commissioner (OAIC). AUSCL Policy Series PS-2026-02.