Digital Economy Council of Australia

# Digital Economy Council of Australia

## Submission to OAIC

**Date 22 June 2026**

## Consultation on Guidance for Transparency in Automated Decision Making

Digital Economy Council of Australia

## About DECA

As the peak industry body for Australia's blockchain, digital asset, AI, and Web3 sectors, the Digital Economy Council of Australia (DECA) champions responsible innovation. We collaborate closely with government bodies and regulators to establish frameworks that ensure Australia remains a globally competitive leader in the digital economy. DECA gratefully acknowledges the valuable insights provided by our working groups in shaping this response. This submission has been prepared with input from DECA's Artificial Intelligence Working Group.

For further inquiries please contact:

- [redacted]
- [redacted]

# Endorsement of the AUSCL submission

DECA endorses the submission to this consultation led by the Australasian Society for Computers and Law (AUSCL) with the Australasian Institute of Digital Health (AIDH) and Atmos. DECA adopts the detailed analysis, factor rankings and recommendations in that submission. This independent DECA submission restates DECA's own positions and adds the perspective of the digital-economy and digital-asset sector and DECA's AI Working Group. Where this submission and the AUSCL submission cover the same ground, they should be read as consistent and mutually reinforcing.

# Executive summary

DECA welcomes the opportunity to comment on the OAIC's development of guidance for the new ADM transparency obligation in APP 1. DECA supports the obligation and its objective of improving integrity, accountability and trust as adoption of AI and ADM accelerates across the Australian economy. Our key positions are:

- **Broad, technology-neutral, risk-sensitive interpretation:** APP 1.7 to 1.9 should be read to capture automation that materially affects a decision-making process, including rules-based systems, statistical models, machine learning, generative AI and decision-support tools. We support a practical "material influence" test.
- **Govern the system, not just the model:** Risk and accountability rarely arise from an AI model in isolation. They arise from the full system: data sources, orchestration logic, decision thresholds, human oversight arrangements and execution pathways. Guidance should focus on the system as deployed.
- **Human oversight is a factor, not an exclusion:** DECA defines human-in-the-loop as a design pattern in which a clearly accountable human retains decision authority over material outcomes, through review, approval, escalation or override calibrated to the risk profile of the use case. Nominal or rubber-stamped oversight does not take a system out of scope.
- **AI is probabilistic and non-deterministic:** Modern AI systems require continuous monitoring, validation and review rather than one-off certification. Assessments of reliance and any disclosures should reflect that system behaviour can drift over time.
- **Evidence-based auditability over theoretical transparency:** The most useful question is whether an entity can demonstrate what happened, why it happened and who approved it. Consistent with DECA's position that "Blockchain + AI" is stronger than AI alone, distributed ledger technology can provide tamper-evident audit trails of decision lineage and human-in-the-loop validation. We encourage the OAIC to recognise such mechanisms as evidence of good governance.

- **Layered, accessible disclosure:** We support a concise flag in the privacy policy, linked to an ADM notice or register and a pathway to further information, so that privacy policies do not become impenetrable as ADM use grows.
- **Pro-innovation, vertical-specific regulation:** Guidance should protect consumers without imposing blanket high-risk categorisations that stifle Australian startups. We support alignment with the Voluntary AI Safety Standard and AI Ethics Principles, AS ISO/IEC 42001, and the National AI Policy.
- **Foundational privacy and data sovereignty:** Individuals have a right to privacy and agency over their personal data. Consent for the use of personal data in AI training or monetisation should be explicit, informed and revocable.
- **Practical guidance:** Guidance should be clear and usable by businesses without the need for legal advice in most cases, with worked examples and decisive calls on whether particular activities are in scope.

# Question 1: Substantially and directly related to making a decision

**OAIC Question 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.

**DECA Response:**

*Factor ranking: DECA reads the 1 to 5 scale as the relative weight or relevance of each factor, where 5 indicates a strong or core indicator.*

- **Degree of reliance on the ADM output (Ranking: 5):** Core indicator, best assessed in practice rather than by policy wording. Where decision-makers routinely accept, copy or follow the output, the system is substantially related.
- **Ability and likelihood of genuine human override (Ranking: 5):** The focus should be on override that is genuinely available and actually exercised, not

theoretical authority. Automation bias, rubber-stamping and workflow pressure favour inclusion.

- **Nature of the output - advisory or determinative (Ranking: 5):** Determinative outputs are clearly in scope. Advisory outputs are in scope where they score, rank, recommend, prioritise, summarise or narrow options in a way that materially shapes the outcome.
- **Integration into the decision-making workflow (Ranking: 5):** Highly relevant. Systems embedded in intake, eligibility, risk scoring, triage, pricing, recruitment, claims handling, fraud detection or compliance workflows are more likely to be directly connected.
- **Effect on evidence, facts or reasons (Ranking: 5):** Where a program selects facts, summarises records, drafts reasons, identifies issues, infers risk or characterises a person, it is substantially related.
- **Transparency and explainability of outputs (Ranking: 4):** Low explainability does not narrow the obligation. It increases the need for disclosure and supporting governance.
- **Practical optionality (Ranking: 4):** Where a staff member cannot readily make the decision without the output, or must justify any departure from it, the system is materially connected.
- **Scale and repeatability (Ranking: 4):** High-volume, repeated use increases the risk that a design error is replicated and favours inclusion.
- **Auditability of the decision lineage - DECA additional factor (Ranking: 4):** Whether the system records what it produced, on what inputs and who approved the outcome. Strong auditability supports a finding that automation materially shaped a real decision pathway and is also the practical evidence on which the material-influence test turns.

**Commentary:**

DECA supports a practical material influence test. A computer program is appropriately 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 should examine actual operational practice rather than policy labels, including training, interface design, system defaults, performance targets, audit logs and the frequency of genuine human override. Two points are particularly important from a digital-economy perspective. First, the assessment should be directed at the full system as deployed, not the underlying model alone, because reliance and influence are properties of how a model is embedded in data pipelines, thresholds and human workflows. Second, because AI systems are probabilistic and non-deterministic, reliance is not fixed at procurement and should be monitored over time, since behaviour and staff dependence can drift.

In our sector, common systems that would warrant assessment under this test include automated transaction monitoring and suspicious-matter decisions for anti-money-laundering and counter-terrorism-financing purposes, fraud detection, automated credit and eligibility decisions for financial and digital-asset products, robo-advice and recommendation engines, algorithmic and dynamic pricing, and identity verification or know-your-customer screening. Tamper-evident audit trails, including those built on distributed ledger technology, are a practical means by which an entity can evidence the degree of reliance and the genuineness of override, and should be encouraged.

## Question 2: Generative AI with human oversight

> **OAIC Question 2: Fictional Edge Case: Generative AI with human oversight** The National Aged-Care Insurance Agency (NACIA) makes decisions about eligibility for elderly people trying to access life-changing aged-care support. To make eligibility assessments quicker, NACIA staff use a generative AI chatbot, GPTea, to summarise candidate profiles and receive recommendations about eligibility. NACIA's human staff always have oversight and make the final decision about eligibility based on the recommendation provided by the chatbot.
>
> - Would you consider NACIA's described uses of GPTea to be substantially and directly related to making decisions? (Please provide yes/no)
> - Can you provide your reasons for your response?

**DECA Response: Yes.**

**Reasons:**

NACIA's use of GPTea is substantially and directly related to the eligibility decision. The tool both summarises candidate profiles and recommends eligibility outcomes, and each function materially shapes the facts, framing and recommendation on which the human decision rests.

- Human oversight does not remove the system from scope where the AI output materially shapes the facts, recommendation, reasons or decision pathway. Generative AI can influence decision-makers through framing effects, omission of relevant facts, hallucinated content, misplaced confidence, automation bias and time pressure. On DECA's definition, oversight only operates as a genuine control where an accountable human retains real decision authority and the practical ability to interrogate and override the output. Nominal review does not displace the obligation.

- The decision concerns access to life-changing aged-care support, is likely to involve sensitive information, and affects people who may be experiencing vulnerability. These features weigh strongly in favour of disclosure.
- Because AI systems are probabilistic, a single point-in-time approval of GPTea is insufficient. NACIA should monitor the tool's behaviour on an ongoing basis and be able to demonstrate, after the fact, what the tool recommended, on what inputs, and that a human genuinely reviewed and decided. This is the evidence-based auditability DECA advocates, and distributed ledger technology is one mechanism capable of providing a tamper-evident record of the human-in-the-loop validation.
- Guidance should confirm 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, the existence and nature of human review, and how an affected person can request further information, correction or review where available.

## Question 3: Meaning of significantly affect rights or interests

**OAIC Question 3:**

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 the examples using the above mentioned (1-5) ranking system and include any additional examples.

**DECA Response:**

- **Sensitive information (Ranking: 5):** Strong indicator, particularly health, disability, biometric, genetic, racial or ethnic origin, political, religious, union, criminal record or children's information.
- **Vulnerable persons (Ranking: 5):** Strong indicator, because the same decision can have a greater practical effect on a person who is a child, older, has a disability, is in crisis, is a migrant, is in financial hardship or has limited digital access.
- **Intrusive practices (Ranking: 5):** Includes profiling, behavioural prediction, surveillance, inference of sensitive attributes, monitoring, geolocation, emotion inference and intrusive targeting.

- **Financial outcomes (Ranking: 5):** Includes eligibility, debt, pricing, credit, insurance, taxation, fines, benefits, hardship, refunds and access to essential services. Highly relevant to the digital-asset and financial-services sector.
- **Access to public or essential services (Ranking: 5):** Strongly relevant to healthcare, aged care, disability, housing, education, social security, migration, justice, utilities, telecommunications and financial services.
- **Legal status, rights, liabilities or obligations (Ranking: 5):** Includes granting, refusing, suspending, cancelling or varying a right, licence, permission, benefit, entitlement, contractual right or liability.
- **Opportunity denial (Ranking: 5):** Includes employment, education, housing, insurance, finance or public-program opportunities, including the non-display of opportunities.
- **Duration, reversibility and contestability (Ranking: 4):** Long-lasting, hard-to-detect, hard-to-correct or non-contestable impacts favour inclusion.
- **Group or systemic impact (Ranking: 4):** A decision pathway can significantly affect rights or interests where it disadvantages a protected or marginalised cohort, even if each individual impact appears small.
- **Identity integrity - DECA additional factor (Ranking: 4):** Where ADM infers, verifies, replicates or relies on identity, the risk of harm rises, including from synthetic identity, deepfakes and impersonation in fraud and verification contexts.

**Commentary:**

Guidance should 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, education, health, safety, autonomy, privacy, dignity, equal treatment and democratic participation. DECA's data-sovereignty position is relevant here: the use of personal data in ways the individual did not understand or authorise is itself an interest worthy of protection.

We also draw attention to effects arising from the actions of others. Where an automated system infers an individual's circumstances from cohort behaviour, for example by adjusting a credit limit or a risk score based on an analysis of other people in the same area or with similar transaction patterns, the individual's interests can be significantly affected by data that is not their own. This is a live issue for automated risk scoring in financial and digital-asset contexts and supports a contextual assessment grounded in legal, human-rights, privacy and anti-discrimination standards across the system lifecycle.

## Question 4: Vulnerable Persons

**OAIC Question 4:** 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? Can you provide your reasons for your response?

**DECA Response:**

DECA recommends that the OAIC avoid a closed list. Vulnerability is contextual and dynamic, and the same decision can affect different people very differently. Relevant classes include:

- Children and young people, who are still developing, may not understand profiling or ADM, and may face 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, financial or AI literacy, limited English proficiency, low literacy, limited internet access or a limited ability to contest automated outcomes.

From a digital-economy perspective, DECA highlights several cohorts that the rapid adoption of AI and automated financial products brings into focus. These include people with low financial or digital literacy who are navigating complex, automated financial and digital-asset products; people targeted by AI-enabled scams, deepfakes and synthetic-identity fraud, which engages DECA's identity-integrity principle; retail participants in volatile, algorithmically mediated markets; and people subject to automated account decisions such as debanking or account closure, where the practical effect on access to financial services can be severe.

A vulnerability lens helps entities assess the expected effect of a decision. It should not be used to justify more intrusive collection or profiling, which would conflict with the data-sovereignty principle. Entities should be encouraged to consult affected communities where ADM is likely to affect at-risk, vulnerable or marginalised cohorts.

## Question 5: Significant service or support

**OAIC Question 5:**

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 the services/support using the above mentioned (1-5) ranking system and include any additional examples.

**DECA Response:**

- **Physical assistance or support (Ranking: 5):** Includes disability, aged care, family violence, child protection, emergency assistance and personal care.
- **Financial assistance (Ranking: 5):** Includes social security, grants, hardship support, refunds, debt relief, insurance payouts and compensation.
- **Access to educational services (Ranking: 5):** Includes admission, exclusion, learning support, assessment, scholarships and disciplinary decisions.
- **In-home services (Ranking: 5):** Includes aged care, disability, health, safety, housing and family support services.
- **Essential banking and credit services (Ranking: 5):** Includes account access, credit, hardship, fraud flags, insurance and payment services. Of particular relevance to DECA, this extends to access to financial services and payment rails, and to automated account access and debanking decisions.
- **Telecommunications (Ranking: 5):** Essential for access to work, education, government services, safety and social participation.
- **Essential utilities (Ranking: 5):** Includes electricity, water, gas and energy hardship decisions.
- **Healthcare and medicines (Ranking: 5):** Includes diagnosis support, triage, admission, treatment access, insurance, aged care and disability support.
- **Housing and accommodation (Ranking: 5):** Includes public housing, rental screening, homelessness support and tenancy services.
- **Employment and livelihood (Ranking: 5):** Includes recruitment, promotion, performance, rostering, workplace surveillance and access to gig work.

- **Migration, citizenship and policing or justice services (Ranking: 5):** Decisions in these domains can affect liberty, family unity, legal status and safety.
- **Access to financial infrastructure and payment systems - DECA additional (Ranking: 5):** Access to accounts, payment rails and core financial infrastructure is quasi-essential to participation in the modern economy and should be treated as significant.

**Commentary:**

A service or support may be 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. Significance is best assessed by context, including the person's circumstances, the availability of alternatives, urgency, reversibility and whether the service is essential or quasi-essential. DECA emphasises that loss of access to banking, payment and core financial services can rapidly cascade into loss of access to many other services and should be treated accordingly.

# Question 6: Other legal frameworks and policies

> **OAIC Question 6:** Are there any other legal frameworks or policies that the OAIC should have regard to in considering the meaning of 'rights' and 'interest'?

**DECA Response:**

DECA endorses the comprehensive list of frameworks, Australian Standards, prudential standards and industry codes set out in the AUSCL submission. These instruments do not expand APP 1.7 beyond its text, but they provide sector-tested indicators of when ADM is likely to affect an individual in a legally or practically significant way, and entities should not treat them as a substitute for APP compliance. In addition, DECA draws particular attention to the following instruments of direct relevance to the digital economy:

- **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and AUSTRAC guidance**, where automated transaction monitoring, alerting and suspicious-matter decisions materially shape outcomes for individuals, including account restrictions.
- **ASIC regulatory framework relevant to financial and digital-asset products**, including Regulatory Guide 271 on internal dispute resolution and AFCA approaches to fairness, reasons and vulnerability, where ADM affects access to credit, payments, complaints, hardship or financial services.

- **Consumer Data Right rules, standards and privacy safeguards**, where ADM relies on consumer-authorised data sharing, data quality, consent flows, accredited data recipients or action initiation.
- **Australian Government Voluntary AI Safety Standard and AI Ethics Principles**, especially the guardrails on accountability, risk management, data governance, testing, human oversight, transparency, contestability and stakeholder engagement. DECA encourages all digital businesses to benchmark their operations against these guardrails and supports alignment of OAIC guidance with them.
- **AS ISO/IEC 42001:2023 and related AI management and governance standards** (including AS ISO/IEC 23894, 38507, 22989 and 23053), which support leadership accountability, risk treatment, impact assessment, human oversight, monitoring and documentation. Building local certification and assurance capability against these standards is consistent with strengthening Australian sovereign capability.
- **The National AI Policy**, particularly its objectives of capturing the opportunity and keeping Australians safe, with which DECA aligns its industry guidance.

Consistent with our evidence-based-auditability position, DECA recommends that OAIC guidance recognise tamper-evident audit mechanisms, including distributed ledger technology, as practical evidence of reasonable governance, assurance, procurement, monitoring and disclosure. The most useful instruments support an entity's ability to demonstrate what happened, why it happened and who approved it, rather than transparency in principle alone. Where appropriate, it would assist businesses for the OAIC to indicate which standards it regards as addressing the core elements of compliance with the ADM requirements.

# Question 7: Differential pricing

> **OAIC Question 7: Fictional Edge Case: Differential pricing** E-commerce company, Daintree, allows subscribers to order books to their home. To make an account, Marco was required to disclose his address, being the luxurious Capital Crescent in Sydney CBD. Marco is surprised that his desired book, The Art of Inheritance, was priced at $100 when his book-club buddy, Charles, from a country town, paid only $35. Marco is shocked to read an article reporting that Daintree uses differential pricing to inflate prices for individuals from wealthy postcodes. Marco is a freelance artist, so he does not have enough disposable income to purchase the book.
>
> - Restricting access to financial products or healthcare would clearly be a decision which significantly affects the interests of an individual. In the above Edge Case, would you consider the

inflation of prices for a consumer product to have significantly affected the interests of Marco?

- If yes, at what amount would differential pricing be considered to have significantly affected the interests of an individual? 5% price difference, 20% price difference, or other (please specify amount)
- In judging whether differential pricing significantly affects rights or interests, how important would you consider the following factors on a scale from 1 to 5 (with 1 being not important and 5 being very important): The dollar amount of differential pricing, The significance of the product or service being purchased

**DECA Response: Yes. On the stated facts, Marco's interests are significantly affected.**

- The price is approximately 186% higher than the comparator ($100 against $35) and materially impairs Marco's access to the product, given that he does not have enough disposable income to purchase it.
- Using address as a proxy for wealth is crude, potentially misleading and capable of producing unfair outcomes. It infers financial circumstances from location without adequate transparency, which engages both fairness and data-sovereignty concerns.
- Differential pricing should not be assessed by percentage alone. The proper test considers the percentage difference, the dollar amount, the significance of the good or service, vulnerability, the availability of alternatives, cumulative impact, and whether sensitive or proxy-sensitive data is used.

**Threshold:**

For ordinary consumer goods, DECA suggests that a differential price may significantly affect interests where the difference is substantial in context, for example around 20% or more, with 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 or proxy-sensitive data. For essential or significant services, even a 5 to 10% difference may be significant where it materially affects access or imposes hardship.

DECA notes that algorithmic, dynamic and personalised pricing is pervasive across digital markets, platforms and exchanges, and that inference from proxy-sensitive data such as postcode is a live risk in automated pricing systems. This reinforces the case for a contextual test rather than a single percentage trigger.

*Importance of factors, scored 1 (not important) to 5 (very important):*

- **The dollar amount of differential pricing (Score: 4):** Important, but not determinative. A smaller dollar amount may still be significant for a vulnerable person or across repeated transactions.
- **The significance of the product or service being purchased (Score: 5):** Very important. Differential pricing affecting essentials, education, health, utilities, finance, insurance, employment or access to information should be treated as more likely to be significant.

## Question 8: Discriminatory targeted job ad

> **OAIC Question 8: Fictional Edge Case: Discriminatory targeted job ad** Engineering firm, Manscon, is hiring for graduate engineers. To try to target the best candidates, Manscon advertises open roles on job site, Opaque Window. Opaque Window algorithmically promotes this job posting to candidates it thinks are best suited. One metric it uses is gender of account holders. Since most engineers at Manscon are male, Opaque Window prioritises promoting the job to male engineering graduates. Rafqa is a female engineering graduate searching for a job on Opaque Window. She does not receive the Manscon job ad, which limits her employment options.
>
> - Should it be considered a 'decision' that Rafqa did not receive the Manscon job ad? Please provide a Yes/No response.
> - Can you provide your reasons for your response?

**DECA Response: Yes.**

- The non-display of the job advertisement is a practical exclusion from an employment opportunity. APP 1.9 expressly provides that doing a thing includes refusing or failing to do a thing, so a failure to serve or promote an opportunity can be a relevant decision or decision-like act.
- The outcome materially affects Rafqa's interests by limiting her employment options at the point of opportunity, and it raises anti-discrimination concerns because gender is used to prioritise male candidates based on historical workforce composition.
- 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 the loss of a fair opportunity to know about and compete for it.

## Question 9: Meaning of "arranged for"

**OAIC Question 9:** Are there any scenarios relevant to the meaning of 'arranged for' that you consider require guidance? If so, why? Can you provide your reasons for your response?

**DECA Response: Yes, guidance would assist.**

DECA endorses the scenarios identified in the AUSCL submission, including third-party platforms and marketplaces, embedded vendor tools, generative AI used by staff, outsourced decision processes, joint arrangements and data sharing, open-ended APIs and configurable systems, and shadow ADM. DECA adds the following scenarios that are specific to the digital economy and emerging agentic systems:

- **Agentic AI and autonomous agents:** Where an AI agent acts on behalf of an entity or a user, including agents that hold machine wallets or conduct agent-to-agent transactions, the concept of "arranged for" should capture the entity that deploys, configures or materially relies on the agent in its decision pathway, even though the agent operates with a degree of autonomy.
- **Configurable and decentralised systems, including smart contracts:** Where decision logic is embedded in on-chain code or in configurable protocols, the entity that sets the thresholds, parameters, prompts, business rules or risk appetite has arranged for the ADM, even if it does not own or operate the underlying model or protocol.
- **Shadow AI:** Where staff use individual generative-AI accounts within recurring decision workflows with management knowledge, acquiescence or inadequate controls, the entity has arranged for the ADM in substance and should not avoid the obligation through the informality of the arrangement.
- **Third-party model supply chains:** Where an entity relies on an externally provided model or service, the obligation should be supported by supplier due diligence, contractual transparency, audit rights and clear allocation of responsibility, consistent with strengthening Australian sovereign assurance capability.

The key question should 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, by using standard software-as-a-service products, or by labelling the supplier as the operator. Guidance should call for supplier due diligence, contractual transparency, audit rights, documentation of ADM uses, testing obligations, incident reporting and clear responsibility for privacy-policy disclosures. Tamper-evident audit trails, including those built on distributed ledger technology, can help evidence who arranged, configured and relied upon an ADM system.

# Question 10: Extent of disclosure

**OAIC Question 10:**

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?

**DECA Response:**

DECA supports meaningful, accessible and layered disclosure. Privacy policies should not become technical manuals, but they must give a reasonable person enough information to understand when ADM is used, what personal information is used, what kinds of decisions are affected and where to go for more information. As ADM use grows, full disclosure of every system within a single privacy policy risks becoming unwieldy and counterproductive. We therefore support flagging ADM use in the privacy policy with a link to further prescribed detail published separately or in an annexure, drawing on the standard disclosure architecture proposed in the AUSCL submission (a plain-language summary, decision categories, personal-information categories, the role of the system, the nature of human involvement, likely consequences, a further-information pathway, a governance statement, an update history, accessible formats and, for high-impact entities, public register linking).

Having regard to the OAIC's stated considerations, DECA recommends that entities additionally:

- **Preserve evidence-based auditability:** Even where commercial-in-confidence considerations limit public detail, entities should preserve auditable technical documentation and decision lineage for

regulators and oversight bodies, capable of demonstrating what happened, why it happened and who approved it. Distributed ledger technology can provide a tamper-evident record for this purpose.

- **Label AI interactions:** Where a person is interacting with, or being materially affected by, an AI system, that fact should be made clear, for example by indicating that a response was generated by AI.
- **Provide a contestability pathway:** Disclosures should make clear how a person can challenge or seek review of an automated outcome, framed so that the information and the decision can be contested.
- **Acknowledge ongoing monitoring:** Because AI systems are probabilistic and can drift, disclosures should reflect that systems are monitored, tested and reviewed on an ongoing basis rather than approved once.
- **Apply a practical accountability test:** A useful internal benchmark is whether the entity would be comfortable explaining the AI system, and the way it reached its outcome, to a regulator, a customer or a court.

DECA recommends that the OAIC provide model wording, examples and a disclosure template that distinguishes between low-risk administrative automation and high-impact ADM, and that makes clear that commercial confidentiality does not justify withholding the existence, purpose, decision categories, personal-information categories or accountability pathway for ADM. DECA would welcome the opportunity to help workshop model wording and templates, particularly for the digital-asset and AI sectors.

## Concluding recommendations

- **Adopt a practical, technology-neutral approach** that balances meaningful transparency for Australian consumers with the necessity of fostering domestic innovation in the digital economy and AI sectors.