

13 January 2025

Australian Government
Attorney-General's Department

By email: ADM@ag.gov.au

Submission on Consultation Paper regarding the use of automated decision-making by government

The Queensland Office of the Information Commissioner (**OIC**) welcomes the release of the Consultation Paper regarding the use of automated decision-making by government (November 2024) by the Attorney-General's Department (**Department**). OIC appreciates the opportunity to respond to the Consultation Paper.

OIC is an independent statutory body that reports to the Queensland Parliament. The Information Commissioner is an officer of parliament charged with functions under the *Right to Information Act 2009* (Qld) (**RTI Act**) and the *Information Privacy Act 2009* (Qld) (**IP Act**) to, respectively, facilitate greater and easier access to government held information and oversee safeguarding of personal information held by public sector agencies.

OIC's statutory functions include mediating privacy complaints made against Queensland public sector agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting regulatory audits and reviews to monitor agency performance and compliance with the RTI Act and the IP Act. Our office also reviews agency decisions about access to, and amendment of, information.

Our submission

OIC has previously made several submissions to the Australian and Queensland Governments and the Senate in relation to automated decision-making (**ADM**) and artificial intelligence (**AI**).¹ Consistent with its previous submissions, OIC welcomes the proposal to develop an enforceable legislative framework to govern the safe and responsible use of technology (including AI) to automate government decisions and administrative action. Given ADM can have significant and widespread impacts on individuals' privacy and right to access government information it is crucial that the ADM legislative framework adopt a lifecycle approach for its safety measures.

We note the Consultation Paper addressed only Recommendation 17.1 of the Robodebt Royal Commission, and that Recommendation 17.2 (establishing a body to monitor and audit ADM) will be considered once the ADM legislative framework is developed.

¹ (i) [Submission dated 31 May 2019 to the Department of Industry, Innovation and Science on the 'Artificial Intelligence: Australian's Ethics Framework – A Discussion Paper'](#); (ii) [Submission dated 27 November 2020 to the Attorney-General's Department on the 'Privacy Act Review, Issues Paper'](#); (iii) [Submission dated 10 January 2022 to the Attorney-General's Department on the 'Privacy Act Review, Discussion Paper'](#); (iv) [Submission dated 25 July 2023 to the Department of Industry, Science and Resources on the 'Safe and responsible AI in Australia, Discussion paper'](#); (v) [Submission dated 5 August 2022 to the Department of Justice and Attorney-General on the 'Consultation Paper – Proposed changes to Queensland's Information Privacy and Right to Information Framework'](#); (vi) [Submission dated 10 October 2024 to the Senate Legal and Constitutional Affairs Legislation Committee on the inquiry into the Privacy and Other Legislation Amendment Bill 2024.](#)

Our submission, by way of responses to the Consultation Paper's nine questions, is set out below.

1. How should the need for transparency about the use of ADM be balanced with the need to protect sensitive information about business processes and systems?

OIC agrees that transparency measures in an ADM legislative framework require careful consideration to balance the benefits of providing information about business rules or algorithms with potential risks of cyber security or fraud. However, the default position must be transparency and explainability of the ADM system. Transparency is essential for public trust and accountability in the government's use of ADM technology and the legislative framework.

Several surveys have reflected the community's expectation and need for transparency, such as:

- The Office of the Australian Information Commissioner's Australian Community Attitudes to Privacy Survey 2023, which notes that 89% of Australians surveyed believe they should have extra rights under the *Privacy Act 1988* (Cth) (**Privacy Act**) to know their personal information is used in automated decisions if it could affect them.²
- The Deloitte Australia Privacy Index 2024, which similarly reveals that 71% of consumers want to know what personal information is involved in ADM, 63% want details on how the decision is made, and 56% value knowing how to challenge AI decisions.³
- The 2024 Edelman Trust Barometer, shows that 64% of Australians consider the government lacks adequate understanding to regulate emerging innovations effectively.⁴ The concern that innovation is mismanaged is shared across income, gender and age.⁵ The report notes that Australians are more likely to embrace innovation if they are confident it will lead to a better future.⁶

We suggest the ADM legislative framework should require agencies to conduct a risk assessment and a Privacy Impact Assessment (**PIA**) when it first considers the adoption of ADM technology, and again at the procurement stage, to determine how risks on business processes and system information may be managed to ensure transparency. We note the Office of the Australian Information Commissioner's [guidance on privacy and developing and training generative AI models](#) would be a useful resource for agencies when considering the use of ADM technology, in addition to the [National Framework for the Assurance of AI in government](#).

Another useful resource may be the Canadian [Directive on Automated Decision-Making](#), which requires an [Algorithmic Impact Assessment \(AIA\)](#) to be completed and the results published before the production of any automated decision system.⁷ The AIA is designed to assist departments and agencies to better understand and manage the risks associated with

² Australian Government, Office of the Australian Information Commissioner, [Australian Community Attitudes to Privacy Survey August 2023](#), pages 9 and 37.

³ [A Transparent Tomorrow Deloitte Australia Privacy Index 2024, 10th edition](#), page 14.

⁴ Edelman Trust Institute, [2024 Edelman Trust Barometer Global Report](#), page 16.

⁵ Edelman Trust Institute, [2024 Edelman Trust Barometer Global Report](#), page 20.

⁶ Edelman Trust Institute, [2024 Edelman Trust Barometer Global Report](#), page 36.

⁷ Section 6. The Directive defines an 'automated decision system' as: 'Any technology that either assists or replaces the judgment of human decision-makers. These systems draw from fields like statistics, linguistics and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets.'

automated decision systems. To assess and mitigate risks, the AIA requires consultation with privacy and legal advisors, policy teams and subject matter experts, as well as measures to safeguard procedural fairness and personal information used or generated by the system.

2. What transparency rules would be appropriate to build into the framework?

OIC agrees with the options set out in the Consultation Paper⁸ that the ADM legislative framework should include express obligations for agencies to:

- Publish information on the agency's website about its use of an ADM process and how that process works. It is suggested that the information should include:
 - the type of personal information that may be used
 - the type of decisions that may be subject to ADM
 - the ability and circumstances in which decisions made by ADM may be substituted by a decision-maker; and
 - rights of review.

The information should be easy to find and available in multiple languages.

- Report on the use of ADM processes as part of the agency's annual reports. This would also allow additional parliamentary scrutiny of the agency's use of ADM. This need not be the only means of reporting, and as suggested in the Consultation Paper, reporting may also occur via a central registry. We note the Consultation Paper does not specify which entity would be responsible for maintaining such a central registry. This may be a function of the body that is tasked with monitoring and auditing ADM.
- Publish business rules and algorithms, consistent with the [Commonwealth Ombudsman's Automated Decision-making Better Practice Guide](#). As noted in our response to Question 1, risks in relation to publishing business rules can be considered as part of the risk assessment. The risk assessment should also consider any potential limitations on an agency's ability to disclose the algorithm and the ability to explain how the algorithm arrives at its outputs. In this context, we note the Senate Select Committee on Adopting Artificial Intelligence states in its final report that providing meaningful transparency based on generative AI may raise particular challenges in the context of ADM.⁹

In addition, the ADM legislative framework should require agencies to publish their risk assessment report, PIA and other relevant assessments, such as human rights, before deploying ADM technology to enable the public to better understand how risks will be managed.

3. What pre-implementation safeguards should apply where ADM is intended to be used?

As noted in our response to Question 1, the ADM legislative framework should require agencies to conduct a risk assessment. That risk assessment may consider, for example:

- the type of automation to be adopted (full or partial)
- the suitability of the technology to achieve the agency's needs

⁸ Pages 18-20.

⁹ The [Senate Select Committee on Adopting Artificial Intelligence \(AI\) November 2024](#), pages 43 and 138.

- the ability for the technology to be customer-centric and to comply with legislative requirements, such as privacy, public records and confidentiality/secrecy provisions, and administrative law requirements for procedural fairness and natural justice; and
- the impact that ADM will have on affected persons (particularly vulnerable groups) such as impacts on privacy and personal autonomy, and economic interests.

As noted in Question 1, the Canadian AIA may be another useful tool to consider in this context.

We agree with the Consultation Paper¹⁰ that human rights, and data security assessment are also necessary to ensure compliance with relevant legislation, policies and guidelines.

Conducting a PIA in addition to those assessments, and a risk assessment, would allow agencies to identify and mitigate any risks in relation to personal information to ensure the technology being considered for adoption complies with the Privacy Act and other policies and guidelines that govern consent, collection, storage, use and disclosure, and retention of personal information.¹¹

Any technology that is used in ADM, including AI, must be designed to minimise the collection and use of personal or sensitive information, and to protect personal information. The ADM technology must also be capable of deleting personal or sensitive information once it is no longer needed or required for record keeping. The technology should be able to track and record data and information that is used and generated to enable appropriate access in the future.

It is also important that the ADM technology be able to explain how it arrives at an output to assist in preparing statement of reasons, and in responding to access to information requests under the *Freedom of Information Act 1982* (Cth) (**FOI Act**). The ability to trace and record outputs will further assist in record keeping obligations, and monitoring and auditing of the ADM process and technology.

4. What system-level safeguards should be required to ensure that ADM operates appropriately?

The Consultation Paper¹² suggests system-level safeguards may include requirements for agencies to:

- undertake regular internal and external audits of the ADM system
- maintain good record keeping
- follow general administrative principles and take reasonable steps to ensure automated decisions are consistent with the objects of the Act and administrative law standards; and
- update the ADM system throughout its lifecycle to ensure administrative actions taken continue to be legally valid.

OIC agrees that all of these measures would assist in ensuring best practice when using ADM, assuming the system has been designed to be customer-centric, free from bias and developed or trained using the correct understanding of the law. It is suggested these system-level safeguards would also need to include clear governance arrangements, and sample tests of decision outcomes as part of the audit process.

¹⁰ Page 21.

¹¹ This would also be consistent with existing guidelines such as, the [National Framework for the Assurance of artificial Intelligence in Government](#) (pages 18-19).

¹² Pages 21–23.

We also welcome the suggestion in the Consultation Paper for the ADM legislative framework, to be accompanied by guidance material to clarify administrative law standards and to potentially clarify and consolidate into a single source existing guidance material and recommendations.¹³

5. What decision-level safeguards should there be for persons affected by decisions made using ADM (for example, review rights)?

The Consultation Paper suggests the following decision-level safeguards¹⁴:

- **Human referral.** OIC supports the ADM legislative framework expressly requiring human intervention (by an appropriate officer) in the decision-making process, particularly for decisions that can have a significant impact on the rights of individuals.
- **Substitution of decisions.** OIC supports the ADM legislative framework expressly authorising the substitution of both incorrect and undesirable automated decisions with a correct decision by decision-makers, in addition to merits review. OIC also supports an obligation on decision-makers to consider whether to substitute an automated decision to correct an administrative error.
- **Protection for actions taken in reliance of an incorrect decision.** OIC agrees with the Consultation Paper that the power to substitute a decision may need to consider protecting actions taken in reliance of an incorrect automated decision where that decision is due to an administrative error.
- **Notification about the use of ADM.** OIC supports the ADM legislative framework expressly requiring agencies to notify affected individuals about how ADM technology is used to make decisions and how decisions may be challenged. The notice should not be complex, lengthy, legalistic or vague, and should be given *before* a decision is made.
- **Providing statements of reasons.** OIC supports the ADM legislative framework requiring agencies to provide affected individuals with a meaningful explanation of how and why the decision was made.¹⁵ Affected persons must be able to understand the reasoning the ADM technology used to arrive at the decision as well as the legal requirements for the decision.

In addition to the above safeguards, OIC suggests that consideration be given to whether the ADM legislative framework expressly prohibit ADM in certain high risk settings or the use of ADM by certain agencies (see also our response to Questions 8 and 9).

Consistently with previous submissions, we also recommend the ADM legislative framework provides individuals with a right to not be subject to a decision that is based solely on ADM that produces legal effects, similar to the European Union General Data Protection Regulation (**GDPR**).¹⁶ We note the GDPR provides additional safeguards for data subjects, including the right for the data subject to obtain human intervention, express their point of view and contest the decision.¹⁷ The new Australian Privacy Principles (**APP**) 1.7, 1.8 and 1.9 introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth) do not go as far as the GDPR and only confer a discretion on an APP entity to assess whether the use of

¹³ Pages 23 and 24.

¹⁴ Pages 24–29.

¹⁵ The [Senate Select Committee on Adopting Artificial Intelligence \(AI\) November 2024](#) has also recommended (Recommendation 11) that the Australian Government implement the recommendations pertaining to automated decision-making in the review of the *Privacy Act 1988* (Cth), including Proposal 19.3 to introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similar significant effect affect them, pages xvi and 140–141.

¹⁶ Regulation (EU) 2016/679, Recital 71 and Article 22(1).

¹⁷ Regulation (EU) 2016/679, Recital 71 and Article 22(3).

ADM 'could reasonably be expected to significantly affect the rights or interests of an individual' (APP 1.7(b)).

6. What post-decision safeguards should there be to allow a decision to be challenged after it has been made?

The Consultation Paper¹⁸ suggest merits review may be provided as either:

- internal and external review by right for all automated decisions
- external review only by right for all automated decisions; or
- external review only if it would ordinarily apply to a decision made by a human.

To afford affected persons procedural fairness and natural justice, OIC would prefer the adoption of both internal and external review rights for all automated decisions.

7. Should individuals be notified of the use of ADM? If so, should notification be required at a specific point in the decision-making process, or should flexibility be provided to agencies about the appropriate time to make a notification?

OIC recommends individual be notified of the use of ADM. The notice should be required before a decision is made. As noted in our response to Question 5, the ADM legislative framework should provide individuals with a right to not be subject to a decision that is based solely on ADM that produces legal effects, similar to the GDPR.

8. Should there be any exemptions to ADM safeguards? If so, what exemptions should be included and why?

OIC suggests there should not be a need for any exemptions for ADM safeguards. However, as noted in response to Question 9, the ADM legislative scheme may need to expressly prohibit ADM in certain high risk settings or the use of ADM by certain agencies.

9. Should safeguards be different depending on the risks associated with the use of ADM for a particular decision or administrative action?

OIC suggests that consideration be given to whether the ADM legislative scheme should expressly prohibit ADM in certain high risk settings or by certain agencies. In addition, consideration should be given to:

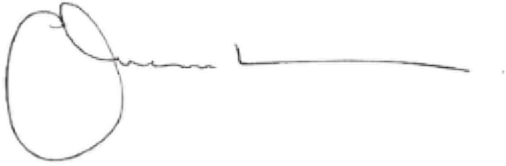
- Whether the ADM legislative framework specifies circumstances for an agency to override, suspend or decommission the use of the ADM technology.
- Consequences for agencies for not complying with the obligations under the ADM legislative framework, or accountability for outcomes when ADM causes harm. This may be a matter that is considered as part of the implementation of Recommendation 17.2 of the Robodebt Royal Commission.
- Whether the ADM legislative framework expressly requires regular training of staff using the ADM technology.

We hope the above assists the Department in considering options for the ADM framework.

¹⁸ Pages 29–31.

Should you require further information regarding the above matters, please contact us at administration@oic.qld.gov.au or on 07 3234 7373.

Yours sincerely

A handwritten signature in black ink, consisting of a large, stylized capital 'J' followed by a series of loops and a long horizontal stroke.

Joanne Kummrow
Information Commissioner