CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

29 April 2022

Department of the Prime Minister and Cabinet
PO Box 6500
Canberra ACT 2600
Australia

By email: digitaltechnologytaskforceinbox@pmc.gov.au

Dear Sir/Madam,

Positioning Australia as a leader in digital economy regulation – Automated decision making and AI regulation – Issues Paper

CPA Australia represents the diverse interests of more than 170,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

We recognise the need to strike a balance between regulation to protect the community and encouraging innovation to advance the uptake of artificial intelligence (AI) and automatic decision making (ADM). It's crucial to enhance the community's understanding of and trust in AI systems and create a level playing field where small technology providers can compete with larger counterparts. Moreover, small businesses must be supported and incentivised to adopt AI.

Our key recommendations are:

- A single definition of AI be legislated.
- Guidance including case studies and examples of AI systems be developed to enhance the community's understanding of AI systems and the different levels of automation used in decision making.
- Harmonise and simplify data access request criteria/standards across different levels of government.
- Invest in upskilling the public services' knowledge of AI and ADM.
- AI regulation and/or guidance be aligned with legislation and policies which regulate or impact the use of data and take account of international developments.
- Enhance community participation in the design, development, deployment and oversight of how regulators use AI and ADM.
- Increase consumer protection from AI-informed decision making and introduce effective remedies and redress mechanisms.
- Encourage users of AI and ADM to test systems regularly to ensure they operate safely and are fit for purpose.
- Consider establishing a regulatory sandbox to support innovation and uptake of AI and ADM innovation.
- Introduce SME-specific measures to help SMEs understand, implement and use AI and ADM solutions.
- Help SMEs prepare for and address AI-specific cyber-risks.
- Encourage and incentivise the development of sustainable AI.
- Develop guidance on providing assurance over AI systems.
- Consider defining circumstances in which human oversight of and/or intervention in AI systems are required.

Responses to the Issues Paper questions are included in the Attachment.

If you have any questions about this submission, please do not hesitate to contact Dr Jana Schmitz, Digital Economy Policy Lead at jana.schmitz@cpaaustralia.com.au, or Dr Gary Pflugrath, Executive General Manager at gary.pflugrath@cpaaustralia.com.au.

Yours faithfully

Pflugrath

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy

Encl.

Attachment

1. What are the most significant regulatory barriers to achieving the potential offered by AI and Automated Decision Making (ADM)? How can those barriers be overcome?

There's no single legal definition for Artificial Intelligence (AI) and Automated Decision Making (ADM) in Australia. In fact, more than one definition of AI and AI-informed decision making is currently in use in laws and reform discussions on AI.

For example, the Issues Paper uses an amended version of the AI definition developed by the Commonwealth Scientific and Industrial Research Organisation (CSIRO).[1] CSIRO's definition has not been adopted uniformly across federal and state governments. This may cause confusion and uncertainty amongst those impacted by potential AI regulation, which could affect the uptake of AI and ADM and slow down innovation.

We propose that the term AI system should be more clearly defined to ensure legal certainty, given that the determination of what an 'AI system' constitutes is crucial for the allocation of legal responsibilities.

The OECD, for example, defines an AI system as a "machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."[2] This definition captures the characteristics of AI systems and addresses AI systems' decision-making capabilities with varying levels of autonomy (see also our response to **Q9**).

Recommendation 1:

A single definition of AI be legislated.

Once defined, the government should assess the different levels of risk AI systems pose. Regulatory responses should be tailored to the risk profile. As outlined in more detail in our response to **Q10**, the European Commission, for instance, has proposed a risk-based approach to regulate AI systems.

Irrespective of whether the government decides to regulate AI systems, it should develop guidance, including examples or case studies, to enhance user's and the community's understanding of AI systems and the different 'levels' of automation used in decision-making.

Recommendation 2:

Guidance including case studies and examples of AI systems be developed to enhance the community's understanding of AI systems and the different levels of automation used in decision making be developed.

The use of AI and ADM within government usually requires access to and sharing of data between multiple agencies, including between different levels of government. We note that different states and territories have their own sets of data access requirements. For technology software providers that often means being required to obtain approvals from different levels of government to access data.

For example, digital service providers (DSPs) offering AI and ADM software tools that handle taxation, accounting, payroll and superannuation related data require interaction with regulatory bodies such as the Australian Taxation Office (ATO) and the Australian Securities and Investments Commission (ASIC).

[1] For CSIRO's AI definition, see Hajkowicz S.A. et al. (2019) Artificial intelligence: Solving problems, growing the economy and improving our quality of life. CSIRO Data61, Australia. Available at: https://data61.csiro.au/en/Our-Research/Our-Work/AI-Roadmap (accessed on 26 April 2022)

[2] See OECD (2019): Legal Instruments - Recommendation of the Council on Artificial Intelligence, available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed on 27 April 2022).

To access information held by the ATO, DSPs must apply for ATO approval. This can take some time as it requires, amongst others; ISO/IEC 27001 (Information Security Management) compliance and numerous gating processes before the DSP is allowed to access the ATO's platform.

Similar processes requiring the same or different criteria apply to ASIC (see ASIC Digital Services Access Terms and Conditions) and most other federal, state and local government agencies to varying degrees. For example, in NSW, software providers need to comply with the NSW Data Request Checklist criteria when requesting data unavailable on the Open Data Portal.

Whilst it makes sense from a security perspective to jump these 'hurdles' once, it does not make sense to have to jump these hurdles for each government agency.

A standard recognised by all government agencies at all levels of government that facilitates appropriate access to their platforms for software developers would significantly improve and simplify the application process.

Recommendation 3:

Harmonise and simplify data access request criteria/standards across different levels of government.

The level of understanding of AI and ADM within the public service varies greatly.

AI and ADM present significant opportunities for government to improve public services and regulator efficiency. However, as with any organisation, the public service needs the skills to ensure any automated decision making is explainable, defensible and operates with appropriate safeguards.

Relying solely on ADM runs the risk of businesses and individuals being unfairly impacted by decisions that don't take account of their specific circumstances. This in turn can impact community trust in government and the technology it uses.

Community trust in AI and ADM would be enhanced by the promotion of examples of it being used to help the community. While using AI to improve the enforcement of regulations is important, the community should also see AI being used to improve the delivery of public services.

All levels of government need to ensure they have access to the skills required to explain and oversee automated decision making.

Recommendation 4:

The government invests in upskilling the public services' knowledge of AI and ADM.

2. Are there specific examples of regulatory overlap or duplication that create a barrier to the adoption of AI or ADM? If so, how could that overlap or duplication be addressed?

While we haven't identified specific examples of regulatory overlap or duplication that could potentially hinder the adoption of AI and ADM, we highlight the importance of aligning any potential AI regulation or guidance to existing legislation, strategies and policies which regulate data. These include the:

- Privacy Act 1988 (which is currently under review)
- Freedom of Information Act 1982
- Data Availability and Transparency Act 2022
- 2015 Public Data Policy Statement
- Productivity Commission's 2017 Inquiry into Data Availability and Use
- Consumer Data Rights
- Cyber Security Strategy
- Digital Economy Strategy,
- Australian Data Strategy (currently open for comment) and others.

Further, regulators and government should take into consideration AI regulation currently being developed or in existence in other jurisdictions. See our response to **Q10**.

Recommendation 5:

AI regulation and/or guidance be aligned with legislation and policies which regulate or impact the use of data, and take account of international developments.

3. What specific regulatory changes could the Commonwealth implement to promote increased adoption of AI and ADM? What are the costs and benefits (in general terms) of any suggested policy change?

The initial AI action Plan Discussion Paper recognised arguments for and against AI-specific regulation. For example, it noted that "regulatory settings must balance innovation with safeguarding consumers and the broader community". It also referenced concerns raised by business that regulation of AI could lead to uncertainty and become a barrier to the development and adoption of AI.

A regulatory framework could enhance the development and uptake of AI in two ways. One; effective regulation of high-risk AI could increase the community's acceptance of such technology. Two; aligning AI-specific regulation with the laws of other jurisdictions (e.g., the European Union's Artificial Intelligence Act; see our response to **Q10**) would better enable Australian AI providers to export their innovations to other markets. It would also enhance local competition by making it easier for foreign AI providers to distribute their innovations in Australia with minimum change necessary.

However, such regulation will result in increased compliance costs and burden for business. If the government decides to regulate AI in some way, it's critical that it undertakes a cost-benefit analysis before deciding if regulation is necessary and before deciding on the design of such regulation. Small innovators would be particularly deterred from entering the market if compliance costs are high.

Recommendation 6:

If regulation of AI is deemed necessary, any associated compliance costs be kept at a minimum.

4. Are there specific examples where regulations have limited opportunities to innovate through the adoption of AI or ADM?

No comment.

5. Are there opportunities to make regulation more technology neutral, so that it will apply more appropriately to AI, ADM and future changes to technology?

See our response to **Q10**.

6. Are there actions that regulators could be taking to facilitate the adoption of AI and ADM?

There must be broad community participation in the design, development, deployment and oversight of how regulators use AI and ADM. Unequal access to information and participation in AI and ADM can significantly worsen existing biases and inequality. Broad participation must include technologists, policymakers, legal professionals, representatives of business (including small business) and vulnerable groups who are likely to be affected by this technology.

Recommendation 7:

Enhance community participation in the design, development, deployment and oversight of how regulators use AI and ADM.

To increase community confidence in AI and ADM, they must be provided with sufficient protection. Consumers should be granted a strong set of rights, effective remedies and redress mechanisms, including collective redress. We therefore believe that the government should consider introducing the right for individuals to 'not to be subject' to certain forms of AI-informed decision-making and require businesses to implement measures to enable individuals to obtain human review of an AI-informed decision to express their point of view and to contest the decision. This is in line with Article 22 of the General Data Protection Regulation (GDPR). See also our response to **Q9**.

Recommendation 8:

Increase consumer protection from AI-informed decision making by introducing effective remedies and redress mechanisms.

Regulators and businesses should perform regular testing of their AI and ADM systems. Systems that continuously learn from previously collected data must be evaluated over time to ensure they are still fit for purpose.

Testing and assurance should increase community trust in AI and ADM systems. We also believe that it will increase business confidence to invest in AI and ADM systems. See also our response to **Q7**.

Recommendation 9:

Encourage users of AI and ADM to test systems regularly to ensure they operate safely and are fit for purpose.

We encourage the government to consider establishing AI regulatory sandboxes for start-ups and SMEs to test innovative AI and ADM solutions for a limited time within a controlled environment. The AI regulatory sandbox allows developers to test their product with greater legal certainty and at lower cost. For regulators, it allows them to increase their understanding of the opportunities and emerging risks and the impacts of AI and ADM.

Recommendation 10:

Consider establishing a regulatory sandbox to support innovation and uptake of AI and ADM innovation.

Our 13th annual Asia Pacific Small Business Survey shows that Australia's small business sector lags the region in tech adoption. While it's primarily the responsibility of businesses to make decisions on tech adoption, our research shows that many businesses struggle to understand what tech is available, and how best to apply it in their business.

We welcome the government's recent budget announcements and its investment in four Artificial Intelligence and Digital Capability Centres to help SMEs to adopt AI. However, SMEs will require continuous support, information and incentives to overcome barriers to implement such emerging technologies.

The following measures could help government in supporting SMEs in the adoption of AI and ADM:

- connecting SMEs to technology talent
- providing SMEs with access to advice and training to help them better understand what technology options exist and how best to apply them in their business
- supporting SMEs to identify their technology needs and connect them to experts and researchers
- connecting SMEs with each other to share best practice approaches as well as lessons learned from using AI and ADM
- encourage entrepreneurs and founders to establish businesses that are "born digital", i.e., have a digital presence or are using digital technologies as crucial part of their business model

We believe that if the government doesn't allocate significant support to SMEs to take advantage of existing and emerging technologies, including AI and ADM, a large digital underclass is likely to develop in the SME community. This will adversely impact SMEs' revenue-generating ability and business valuations, as well as impact economic growth and jobs creation. The government's digital economy strategy must therefore include a significantly stronger focus on helping to build the digital capability and capacity of Australia's small business sector.

Further, while the federal government is doing a good job in building the digital infrastructure underpinning its digital strategy, such as the Australian Business Registry Services and eInvoicing, it needs to provide more help to all businesses to utilise such important infrastructure.

Recommendation 11:

Introduce SME-specific measures to help SMEs understand, implement and use AI and ADM solutions.

With the adoption of AI and ADM, businesses of all sizes may be exposed to additional cyber risks. The government needs to be prepared to offer additional support to protect businesses from such additional risks.

We appreciate that the Department of Home Affairs is currently consulting on the National Data Security Action Plan which acknowledges that small businesses are particularly vulnerable to data breaches due to a lack of resources, capability and expertise to manage cyber security risk. The use of AI by small businesses will exacerbate their vulnerabilities to cyber risk. The support the government will provide to SMEs to encourage their uptake of AI and ADM must include measures that help them prevent, mitigate and manage cyber-attacks.

Recommendation 12:

Help SMEs prepare for and address AI-specific cyber-risks.

Lastly, the government should encourage and incentivise innovators to contribute to sustainable AI (e.g., developing less data-intensive and energy-consuming AI systems). We encourage the government to invest in environmentally friendly AI through setting up data spaces, covering areas like the environment, energy, and agriculture, to ensure that more data becomes available for use in the economy and society.

Additionally, the government should consider investing in testing and experimentation facilities that have a specific focus on environment/climate (such as circular economy and smart cities) to contribute to environmental/climate transitions.

Recommendation 13:

Encourage and incentivise the development of sustainable AI.

7. Is there a need for new regulation or guidance to minimise existing and emerging risks of adopting AI and ADM?

We encourage the government to develop guidance around AI and ADM assurance to minimise and prevent risks posed by these technologies.[3]

It's also important that the community can quickly discover whether an AI and ADM system is compliant with any proposed regulation or guidance.

With increased volumes of data, process automation and decisions being made by algorithms, AI systems users and the broader community need assurance that such algorithms are working as intended and achieving the desired outcomes. Therefore, AI assurance should involve processes for testing the behaviour of and learning by algorithms.

Assurance over AI and ADM systems allows the community, businesses, governments and regulators to build trust and confidence in the use of these systems.

Recommendation 14

[3] See the UK's Centre for Data Ethics and Innovation's (CDEI) AI Assurance Guide.

Developing guidance on providing assurance over AI systems.

8. Would increased automation of decision making have adverse implications for vulnerable groups? How could any adverse implications be ameliorated?

See also our responses to **Q6** and **Q9**.

9. Are there specific circumstances in which AI or ADM are not appropriate?

It may not always be appropriate that AI and ADM operate fully autonomously, i.e., without human oversight and/or intervention.

For example, the automated debt recovery system, 'Robodebt', illustrated how a calculation that is algorithmically correct can be in error or unfair if it's applied without, for example, due consideration of personal circumstances. Such AI requires appropriate human intervention and consideration.

Recommendation 15:

Consider defining circumstances in which human oversight of and/or intervention in AI systems are required.

10. Are there international policy measures, legal frameworks or proposals on AI or ADM that should be considered for adoption in Australia? Is consistency or interoperability with foreign approaches desirable?

The government should consider the following regulatory developments in other jurisdictions:

European Union (EU): The proposed Artificial Intelligence Act seeks to improve trust in the AI environment. The proposed regulation covers the supply and use of AI. The law will apply to AI used or placed on the EU market, irrespective of whether the providers are based within or outside the EU. Thus, the regulation has a direct effect on Australia-based AI developers/providers looking to service the EU market.

The European Commission proposes a risk-based approach to AI regulation, which implies that AI systems will be subject to different levels of obligations or prohibitions depending on the risks posed to the health, safety and fundamental rights of persons in the EU. However, the regulation's risk framework focuses exclusively on the risks AI poses for the public, not the broader set of AI risks to businesses themselves, e.g., the risk of losses due to misclassified inventory.

Other relevant European regulatory frameworks include the General Data Protection Regulation (GDPR), which is meant to be technology neutral (see GDPR Recital 15) and thus helps promote innovation by not discriminating against particular technologies and helps prevent the law from becoming out of date.

Canada: see Law Commission of Ontario's Executive Summary on Regulating AI: Critical Issues and Choices

United Kingdom: Guidance - National AI Strategy