KPMG

Safe and responsible AI in Australia

KPMG submission

KPMG Australia, July 2023

KPMG.com.au

Contents

Executive summary

As a leading professional services firm, KPMG Australia (KPMG) is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also employees, governments, regulators – and the wider community. We strive to contribute in a positive way to the debate that is shaping the Australian economy and we welcome the opportunity to provide a submission to the Department of Industry, Science and Resources *Safe and responsible AI in Australia* discussion paper (the discussion paper).

This submission builds on KPMG's previous engagement in the safe and responsible development of AI in Australia and globally. KPMG has provided a number of submissions to various forums on this topic, including on Automated Decision Making and AI regulation in July 2022, An AI Action Plan for all Australians in December 2020, the Australian Data Strategy in July 2022, and Human Rights and Technology in 2020 and Beyond in March 2020. KPMG published a report with the AIIA in March 2023, Navigating AI: analysis and guidance on use and adoption, which examines the global and domestic regulatory landscape in the Artificial Intelligence space.

We have also done extensive work with the University of Queensland on the topic of *Trust in Artificial Intelligence*. The most recent paper, Trust in Artificial Intelligence: Global Insights 2023, was published in February 2023 and surveyed over 17,000 people from 17 countries on the public's trust and attitudes towards AI. Previous work in this series includes Achieving Trustworthy AI: A Model for Trustworthy Artificial Intelligence, Trust in Artificial Intelligence: A five country study, and Trust in Artificial Intelligence: Australian Insights 2020.

KPMG is an early and active user of AI, having recently expanded our partnership with Microsoft to streamline the deployment of AI in our back-office functions and consider its use across tax, audit and advisory work.[1] KPMG is also developing a people-centred approach to AI that will apply to the design and deployment of AI within the firm.

The successful adoption of responsible AI needs to be assisted by addressing the public's current lack of trust in AI by ensuring the right mix of policy settings, regulations and laws to ensure AI use is safe. KPMG and the University of Queensland's research has found that only two in five people believe current regulations, laws and safeguards are sufficient to make AI use safe. Without appropriate legal and regulatory frameworks, a lack of trust in AI will persist, meaning that it is likely that its full potential will not be realised.

In this submission, KPMG recommends a people-centred approach to AI that prioritises regulatory action on the human rights impact and potential harms of specific types of data used in AI solutions, data protection and integrity and ensuring the definition of personal information can meet the diverse types of data underpinning AI solutions. While in this submission we have focused on a people-centred approach to AI, we acknowledge there are various other impacts, such as environmental considerations, that will also need to be addressed. KPMG supports harmonising overlapping regulatory frameworks across Australia and ensuring greater consistency with international regulatory frameworks to reduce administrative burden and assist technology exporters.

The submission outlines 16 recommendations at section one and directly addresses the consultation questions at section two. If you would like to discuss the contents of this submission further please do not hesitate to reach out. KPMG looks forward to continuing engagement with the Australian Government as it develops a safe and responsible framework for AI in Australia.

Yours sincerely,

James Mabbott	**Richard Boele**	**Danielle Malone**	**Veronica Scott**
Partner in Charge, KPMG Futures	Chief Purpose Officer	Partner in Charge, Data & Cloud	Cyber, Privacy & Data Lead, KPMG Law
KPMG Australia	KPMG Australia	KPMG Australia	KPMG Australia

[1] KPMG and Microsoft agreement to put AI at the forefront of professional services – Media release 12 July 2023

Background

About KPMG

KPMG is a global organisation of independent professional firms, providing a full range of services to organisations across a wide range of industries, governments and not-for-profit sectors. We operate in 146 countries and territories and have more than 227,000 people working in member firms around the world. In Australia, KPMG has a long tradition of professionalism and integrity combined with our dynamic approach to advising clients in a digital-driven world.

Section 1:
KPMG recommendations

RECOMMENDATION 1:

KPMG suggests that the following areas could be considered for regulatory action, subject to further consultation:

- The human rights impacts and harms of using specific types of data (e.g., sensitive information) to develop AI solutions.
- Data related concepts such as data integrity and quality, data ownership, data collection, anonymisation, de-identification, encryption and their role in the context of AI and protection of human rights.
- The definition of "personal information" given the increasingly diverse types of data that could trigger harms and human rights violations.
- The consideration of an advisory board to provide ongoing support in relation to AI regulations, ethics and data sharing, including examining international trends and ensuring Australia's regulations are aligned to reduce administrative burden.

RECOMMENDATION 2:

KPMG considers that there is a range of non-regulatory initiatives the government could consider in supporting responsible AI in Australia, including:

- Investment in public education campaigns to increase the Australian public's awareness, trust and understanding of AI. This should include education on what regulatory safeguards already exist under existing regulations.
- Reviewing the roles and responsibilities of existing regulators with responsibility for data, consumer rights, and online harm protection to address gaps, ensure clarity and reduce overlap.
- Consideration of a federal Commissioner to support regulators, policy makers, governments and businesses to develop and apply laws and other standards in this area.

RECOMMENDATION 3:

The government consider initiatives that help organisations embed assessments and frameworks that are fit for purpose for designing, implementing, procuring, and using different types of AI, and making decisions based on the AI and the data that is used.

RECOMMENDATION 4:

KPMG recommends that any regulatory settings for AI and automated decision making (ADM) should build on existing frameworks such as privacy, discrimination and consumer laws, with a focus on ensuring they are adequate to address potential harms caused by AI and ADM.

RECOMMENDATION 5:

KPMG supports addressing duplication within the broader landscape of data-related regulatory requirements at the state and federal level. We encourage collaboration between Commonwealth agencies to ensure harmonisation between overlapping regulatory frameworks.

RECOMMENDATION 6:

KPMG is supportive of the Commonwealth public sector data sharing scheme given the significant benefits from the ability for government departments and agencies to share and access each other's data.

RECOMMENDATION 7:

Greater consistency with international regulatory frameworks would significantly reduce administrative burden, help with exporting technology out of Australia and set clearer expectations for the importation of technology.

RECOMMENDATION 8:

Given the mature stage of development of the EU's AI Act, Australia could consider the risk-based approach with stricter regulation of AI and ADM applications in high-risk areas, to inform its regulation.

RECOMMENDATION 9:

KPMG considers that both the public and private sector's use of AI technologies must be held to the same minimum standards, including in relation to privacy protection, transparency and explainability, contestability, and discrimination.

RECOMMENDATION 10:

To further support responsible AI practices in Australian Government agencies, KPMG recommends consideration of defining principles and boundaries for ethical data sharing practices and an assessment of the impact on human rights.

RECOMMENDATION 11:

KPMG suggests it would be useful to consider the introduction of transparent disclosure obligations that require organisations to disclose why an AI use case was deemed to have complied with the particular ethics framework.

RECOMMENDATION 12:

KPMG suggests the regulatory framework should be founded on a core set of principles, ideally based on current established principles (such as: safety, security, robustness, fairness, transparency and accountability). These principles should be able to be translated into effective assessment and assurance framework tools that organisations can embed.

RECOMMENDATION 13:

KPMG recommends a range of initiatives that may increase public trust in AI deployment, including the development of a certification regime for responsible AI, embedding data quality requirements, public education campaigns, and other measures such as licencing, auditing, impact assessment and regulatory oversight.

RECOMMENDATION 14:

KPMG considers that the implementation of assurance mechanisms would facilitate greater trust in AI systems. The proposed EU AI Act requires high-risk applications of AI and ADM to be approved through a conformity assessment, and it would be worth considering whether aligning to this approach would be suitable for Australia.

RECOMMENDATION 15:

KPMG considers that the government could usefully explore with industry the development of an initial human rights risk assessment to determine an AI project's level of risk to people upfront and ensure the appropriate level of governance oversight and remediation is applied.

RECOMMENDATION 16:

KPMG considers that self-regulation may ultimately not be sufficient, and agreement on regulatory goals is necessary before effective self-regulation can occur.

Section 2:
KPMG insights

KPMG insights

Definitions

1. Do you agree with the definitions in this discussion paper? If not, what definitions do you prefer and why?

The discussion paper defines AI as an engineered system that generates predictive output without explicit programming and lists machine learning, generative AI models (including large language models, multimodal foundation models) and automated decision making (ADM) as examples.

This definition is consistent with the definitions previously used by KPMG, however given the rapidly advancing nature of this technology, it may be useful to consider a broader definition.

The government could consider the following examples when finalising its definition, which also capture autonomy versus automation:

- *Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.*[2]
- *Artificial intelligence system' (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.*[3]

KPMG also notes that two common types of AI systems are generative AI and predictive AI. Both use neural network machine learning but are not the only systems that use machine learning. Therefore, it may be necessary to identify the underlying technology of neural network machine learning, or the system-level capability of generative/predictive AI that then underpins the application and subsequently use case of that application. However, the government should consider the impact of the proposed definition on the systems that would be in scope for regulation on a risk based approach.

2. What potential risks from AI are not covered by Australia's existing regulatory approaches? Do you have suggestions for possible regulatory action to mitigate these risks?

Appropriate legal and regulatory frameworks are critical to providing individuals, businesses and governments with increased certainty about the risks and benefits of adopting AI and ADM technologies, which in turn will encourage increased uptake and investment.

KPMG supports a regulatory approach that is simple and clear in order to achieve the right balance between appropriate safeguards and enabling innovation. Whilst regulation will help enable trust, doing so without being sensitive to what already exists risks limiting the uptake of the technology and driving out innovation due to a regulatory landscape that could be too complex to manage or navigate.

One of the key challenges for private and public organisations in the deployment and use of responsible AI arises from the multiplicity of guidelines, frameworks, good practices and toolkits developed by the Australian Government as well as national and international policy makers. The development and adoption of a simplified and interoperable regulatory framework for AI should be accompanied by the identification of a leading regulatory body responsible for developing and enforcing AI legislation.

Gaps in regulatory guidance on how existing laws apply to AI

Existing legislative frameworks that aim to address consumer and other individual harms should be considered as a starting point, noting that the current frameworks are generally not yet adequately adapted to the use of AI and ADM technologies and their potential adverse

[2] Key AI terminology – United States IT Modernization Centres of Excellence

[3] European Union – Artificial Intelligence Act

impacts. Further guidance is required on how these existing frameworks and laws apply to AI technologies and effectively prevent the harms that can arise from their use. This should reflect the policy settings and principles framework for AI and would provide guidance and certainty for entities developing or using the technologies and afford individuals or groups of individuals with appropriate rights in relation to the data uses, inputs and outcomes from the use of AI and ADM as well as assurance, monitoring and oversight. There should be a focus on ensuring legislative frameworks are adequate to address outcomes and decisions made as a result of using AI and ADM, including potential harms.

Information privacy

The Privacy Act is intended to be technology neutral and therefore is a foundational regulatory framework that focuses on personal information, which is one of the larger data sets commonly used in AI and ADM. In its current state, the Privacy Act has some legislative gaps related to employee records and small business exemptions, however we note that these areas are subject to reform as a result of the Review of the Privacy Act,[4] including proposals to impose additional obligations in relation to the use of personal information for automated decision making. Areas that are particularly relevant to the application of AI include protections for de-identified information (including consideration of how AI may be used to re-identify information through the use of multiple data sources); high risk privacy processes; the misuse of data which results in detrimental outcomes for consumers, as well as employees; and where technological breakthroughs and innovations are often driven by smaller firms. The impact of the use of different types and combinations of data by AI, in particular sensitive information, must be adequately addressed. Further, the reliance on notice and consent needs revisiting to ensure transparency and choice is embedded.

How to practically and effectively achieve consent needs to be reconsidered in light of the functionalities and capabilities of technology in specific contexts of use, which are not static. For example, in relation to facial recognition technologies where biometric data may be captured without any consent process, such as when this technology is used for theft detection and prevention.

Intellectual property (IP)

Clarity on the IP status of publicly available data being used for development and training of AI models as well as AI outputs, including considering legislating for a database right, should be addressed. This should include regulation of IP ownership of AI systems in relation to opensource algorithms and ownership of the data being used for their development.

Accountability

In investigating an appropriate regulatory framework, KPMG considers that the government could usefully explore with industry:

- the development and adoption of a code of conduct or charter that supports self-regulation and embeds shared values and principles to support ethical and trustworthy data use and AI;
- how responsibility and accountability can be clearly defined, allocated, understood and executed across key stages of the AI lifecycle;
- the development of governance, monitoring and reporting structures that provide appropriate oversight of how AI systems and technologies are brought into an organisation's operations, products and/or services; and
- transparently documenting who can, is and should be making key decisions throughout the AI system lifecycle including based on the outputs.

Governance, monitoring and reporting structures should also include assurance mechanisms that provide assurance for organisations, individuals, and the community more broadly.

Consent

The Privacy Act in its current form does not explicitly set out the requirements for lawful consent or what types of consent must be obtained according to personal information types or processing purposes. The Privacy Act Review proposes that lawful consent and its elements are defined in the Act to cover both implied and express consent which would reflect current guidance. Further consideration should be given to the impact of the use of personal information as inputs and outputs of AI systems and technologies on the proposed consent model. This should include how to strike the right balance consistent with core AI principles, where there may be higher expectations from individuals, and could recognise both the important role of government and the power

[4] Privacy Act Review Report – Attorney-General's Department

imbalances that may exist between individuals and government agencies.

Algorithmic bias

As they currently exist, predictions or outputs from some AI systems exhibit a high rate of error that disproportionately affect already vulnerable or marginalised populations, such as on the basis of skin colour, gender and disability. Existing laws are inadequate to address the potential harm to people caused by the use of these technologies. Consequently, this is an area requiring the development of specific legislation.

RECOMMENDATION 1:

KPMG suggests that the following areas could be considered for regulatory action, subject to further consultation:

- The human rights impacts and harms of using specific types of data (e.g., sensitive information) to develop AI solutions.
- Data related concepts such as data integrity and quality, data ownership, data collection, anonymisation, de-identification, encryption and their role in the context of AI and protection of human rights.
- The definition of "personal information" given the increasingly diverse types of data that could trigger harms and human rights violations.
- The consideration of an advisory board to provide ongoing support in relation to AI regulations, ethics and data sharing, including examining international trends and ensuring Australia's regulations are aligned to reduce administrative burden.

3. Are there any further non-regulatory initiatives the Australian Government could implement to support responsible AI practices in Australia? Please describe these and their benefits or impacts.

Education

KPMG considers that education is a key non-regulatory initiative that the government could implement to support responsible AI practices in Australia.

KPMG and the University of Queensland's recent report *Trust in Artificial Intelligence: Global Insights 2023* found that while 82 percent of people are aware of AI, one in two people report feeling they do not understand AI or when and how it is used.[5] People who better understand AI are more likely to trust and accept it and perceive greater benefits of AI use. Further, the analysis finds that 82 percent of people want to know more about AI. Considered together, these findings suggest a strong need and appetite for public education on AI.

The report finds that Asian countries and Finland have the highest levels of AI awareness. High rates in Finland compared to other western nations may partially reflect investment in public AI education, for example, the *Elements of AI* course is a free online course created by the University of Helsinki and MinnaLearn and has been completed by over 850,000 people.[6]

KPMG recommends the Australian government consider investment in public AI education campaigns in order to drive cultural change and increase awareness, trust and responsible use of AI. This should include education on what regulatory safeguards already exist under existing regulations.

Federal AI Commissioner

KPMG supports the recommendation made by the Australian Human Rights Commissioner in 2021 for the creation of a federal AI Commissioner.[7] The role of the Commissioner would be to "support regulators, policy makers, government and business develop and apply law and other standards in this area." In our view, this function could deliver significant value in filling the gap of uncertainty about how to design and deploy AI in a way that is both lawful and people centred.

AI and mis-, dis- and mal-information (MDM)

The speed and opacity of AI algorithms can be used to facilitate mis-, dis- and mal-information (MDM). This includes attempts, amongst other things, to undermine trust in the fabric of democratic society and mobilise extremist views, including but not limited to, information warfare, as outlined in the recent Defence Strategic Review 2023.[8]

We also note examples where AI has created non-existent references, articles and citations to support a desired output, where there is no ill-intent at play. It is important to consider both the deliberate use of AI systems to create distrust, but also the potential to create false facts due to

[5] Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. (2023). Trust in Artificial Intelligence: A Global Study. The University of Queensland and KPMG Australia.
[6] Elements of AI free online course
[7] AI Safety Commissioner – Australian Human Rights Commission
[8] National Defence: Defence Strategic Review 2023 - Commonwealth of Australia 2023

the way some systems (generative models in particular) operate.

Australia could draw upon lessons learned from Norway[9] and Germany[10] in strengthening Australia's information resilience. As society has become more dependent on information, the ability to think critically about the information citizens receive becomes critical. Greater education and awareness are required at every level of society to build democratic resilience.

Centralisation versus decentralisation of AI

The centralisation of AI may give rise to the notion of encouraging through regulation the decentralisation of AI capability as a means to democratise and curtail the worst effects of AI. Yet, a recent study at Harvard University found AI decentralisation produced similar harmful effects when ethical and regulatory frameworks are absent.[11] As the authors of the study argue:

These technologies enable radical innovations in social, economic, and political institutions and practices, with the potential to support transformative approaches to political economy. They demand governance innovation. There is the potential to overcome persistent injustices power concentrations, and perversions of capitalism and democracy. In fact, recent advances in artificial intelligence (AI) may make these tools critical to preserving human dignity, agency, and even existence. Yet there are also risks of catastrophe and oppression that eclipse those seen in the twentieth century. Calibre of governance will determine which path we find ourselves upon.

RECOMMENDATION 2:

KPMG considers that there is a range of non-regulatory initiatives the government could consider in supporting responsible AI in Australia, including:

- Investment in public education campaigns to increase the Australian public's awareness, trust and understanding of AI. This should include education on what regulatory safeguards already exist under existing regulations.
- Reviewing the roles and responsibilities of existing regulators with responsibility for data, consumer rights, and online harm protection to ensure clarity and reduce overlap.
- Consideration of a federal Commissioner to support regulators, policy makers, governments and businesses to develop and apply laws and other standards in this area.

RECOMMENDATION 3:

The government consider initiatives that help organisations embed assessments and frameworks that are fit for purpose for designing, implementing, procuring, and using different types of AI, and making decisions based on the AI and the data that is used.

4. Do you have suggestions on coordination of AI governance across government? Please outline the goals that any coordination mechanisms could achieve and how they could influence the development and uptake of AI in Australia.

KPMG and the University of Queensland's research finds that 71 percent of people believe AI regulation is required.[12] Further, people are broadly supportive of multiple forms of regulation, including regulation by government and existing regulators, a dedicated independent AI regulator, and co-regulation and industry regulation, with general agreement of the need for some form of external, independent oversight.

Strengthening existing laws and guidance in the context of AI

KPMG recommends that any regulatory settings for AI and ADM should build on existing frameworks such as privacy, discrimination and consumer laws, with a focus on ensuring they are adequate to address potential harms caused by AI and ADM. To ensure a fit for purpose framework, any new regulations to address gaps or inadequacies should be developed through a full industry consultation process, reviewed regularly, and be as technology neutral as possible.

It would be worthwhile to identify areas that are already subject to regulatory oversight and ensure that the rights, duties, and powers created by these regimes are appropriately

[9] The Defence of Norway: Capability and Readiness - Long Term Defence Plan 2020 – Norwegian Ministry of Defence; Setting the Course for Norwegian Foreign and Security Policy - Norwegian Ministry of Foreign Affairs

[10] On German Security Policy and the Future of the Bundeswehr - German Federal Ministry of Defence

[11] Ethics of Decentralised Social Technologies: Lessons from Web3, the Fediverse, and Beyond – March 2023

[12] Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. (2023). Trust in Artificial Intelligence: A Global Study. The University of Queensland and KPMG Australia.

adapted or modified to account for the problems unique to AI/ADM. In particular, this would require consideration about what powers and resources would need to be given to the relevant regulators (i.e., ASIC, TGA, ACCC and OAIC) to enable them to regulate activities to prevent and respond to harmful uses of AI/ADM.

This activity should also aim to address duplication within the broader landscape of data-related regulatory requirements at the state and federal level. We encourage collaboration between Commonwealth agencies to ensure harmonisation between overlapping regulatory frameworks.

Data sharing

An important element of coordination of AI governance across government will be data sharing, privacy, and consent mechanisms between departments and also with citizens. KPMG supports data sharing frameworks such as the Data Availability and Transparency Act 2022 (Cth) and the Data Sharing (Government Sector) Act 2015 (NSW) given the significant benefits that can be drawn from greater levels of safe sharing of quality data across entities such federal and state government agencies, as well as the research community.

KPMG is supportive of public sector data sharing schemes given the significant benefits from the ability of critical government departments and agencies such as Services Australia, the Australian Tax Office, the Department of Home Affairs, the Australian Bureau of Statistics and bodies such as the Australian Institute of Health and Welfare, to share and access each other's data to support the delivery of day to day services, policy development, and critical program provision during national disasters.

KPMG considers that in implementing the Data Availability and Transparency Scheme, there is an opportunity to develop a robust, consistent and clear national framework that addresses overlapping Commonwealth, State, and Territory privacy and data protection frameworks and learnings from other data schemes.

RECOMMENDATION 4:

KPMG recommends that any regulatory settings for AI and ADM should build on existing frameworks such as privacy, discrimination and consumer laws, with a focus on ensuring they are adequate to address potential harms caused by AI and ADM.

RECOMMENDATION 5:

KPMG supports addressing duplication within the broader landscape of data-related regulatory requirements at the state and federal level. We encourage collaboration between Commonwealth agencies to ensure harmonisation between overlapping regulatory frameworks.

RECOMMENDATION 6:

KPMG is supportive of the Commonwealth public sector data sharing scheme given the significant benefits from the ability for government departments and agencies to share and access each other's data.

Responses suitable for Australia

5. Are there any governance measures being taken or considered by other countries (including any not discussed in this paper) that are relevant, adaptable and desirable for Australia?

AI regulation has achieved low levels of maturity mainly due to its reliance on voluntary compliance with AI Ethical Principles. Many jurisdictions are following the examples set by the European Union and the OECD in implementing frameworks to develop 'human-centric' AI through self-regulation. However, there are some examples of international regulation that should be noted, including:

1. **European Union:** the EU's proposed AI Act, if legislated, could mark a paradigm shift away from laws that address different aspects of AI (e.g., data privacy law) towards comprehensive AI regulations. This should be closely monitored.
2. **United States:** has established a National AI Initiative Act which aims to ensure that American values are integrated into the commercial use of AI. The White House also released an executive order on 9 March 2022 that stipulates a policy for the Responsible Development of Digital Assets.
3. **Canada:** the Government has proposed Digital Charter Implementation (Bill C-27) to create rules for the responsible development and deployment of AI. In addition, federal Canadian agencies are subject to the Directive on Automated Decision-Making which, among other things, mandates the conduct of an algorithmic impact

assessment to determine the impact level of an automated decision-making system.

4. **Nordic states:** Denmark, Finland, Norway and Sweden have developed frameworks to guide the development of ethical and trustworthy AI. Denmark has mandatory company legislation for AI and data ethics.
5. **Singapore:** the Model AI Governance Framework aims to support the development of ethical AI solutions to promote public understanding and trust in technology. The Implementation and Self Assessment Guide for Organisations helps organisations to self-regulate alignment to the Model Framework.

Separately, AI standards are also being developed by international bodies such as the International Organisation for Standardisation (ISO) and the Institute of Electrical and Electronics Engineers (IEEE). The UK Government has also released a White Paper on AI regulation which considers current regulatory coverage, starting with a non-statutory approach to support regulator's gaps and acknowledges the risks of regulatory incoherence.[13]

When looking at international examples and developing Australia's regulatory framework, it is important to note that consistency with international frameworks is critical in reducing administrative burden and providing increased certainty for businesses and individuals in adopting these technologies. The developments in AI legislation in Europe, namely the development of the EU AI Act as well as the approach being discussed in the UK, could be considered as a starting point in Australia, particularly the EU's adoption of a risk-based approach to AI regulation and the UK's proposed principles-based approach and regulation of the uses, rather than the technology.

RECOMMENDATION 7:

Greater consistency with international regulatory frameworks would significantly reduce administrative burden, help with exporting technology out of Australia and set clearer expectations for the importation of technology.

RECOMMENDATION 8:

Given the mature stage of development of the EU's AI Act, Australia could consider the risk-based approach with stricter regulation of AI and ADM applications in high-risk areas, to inform its regulation.

Target areas

6. Should different approaches apply to public and private sector use of AI technologies? If so, how should the approaches differ?

In KPMG's view, both the public and private sector's use of AI technologies must be held to the same minimum standards, including in relation to privacy protection, transparency and explainability, contestability, and discrimination. Regulation must consider both inputs and outputs, i.e., what is going into the model, rather than just the output.

Above and beyond those minimum standards, the public sector may be subject to additional requirements, for example, based on the types of data being used and the more limited choices the public have in relation to the collection and use of their data. Given this, it is critical that there are adequate privacy protections, transparency around how decisions are made, and sufficient access to information for data subjects. This can also be supported by freedom of information laws that provide individuals with a right of access to their information.

From a privacy perspective, KPMG supports requirements that privacy policies include whether personal information will be used in automated decision making and for what types of decisions (as proposed by the Privacy Act review). Transparency about the use of personal information in this way is important. Furthermore, where personal information will be used in automated decision making, KPMG considers that there should be an option for individuals to opt out from data being used in this way with reasonable alternative options to avoid a total denial of services, or the right to request human intervention.

RECOMMENDATION 9:

KPMG considers that both the public and private sector's use of AI technologies must be held to the same minimum standards, including in relation to privacy protection, transparency and explainability, contestability, and discrimination.

[13] A pro-innovation approach to AI regulation – policy paper – UK Department for Science, Innovation & Technology

7. How can the Australian Government further support responsible AI practices in its own agencies?

We note the steps outlined in the discussion paper that the Australian Government is already taking to support responsible AI practices, including guidance from the Digital Transformation Agency on public sector adoption of AI as part of its Australian Government Architecture, and the Office of the Commonwealth Ombudsman's *Automated decision-making better practice guide* for agencies implementing AI and ADM systems.

To further support responsible AI practices in Australian Government agencies, KPMG recommends consideration of defining principles and boundaries for ethical data sharing practices and an assessment of the impact on human rights.

Ethical use of data

Consideration should be given to refining the definition of public sector data to require additional details regarding the scope, nature (e.g., raw, processed) and origin (e.g., generated by algorithmic models) of the related data. Additionally, consideration should be given to providing additional guidelines on the types of data included in the "personal information" definition to ensure that new types of identifiable data that have not historically been covered by the current data privacy legislative framework are subject to adequate protection.

Further guidance on the use of data to protect children and vulnerable people should also be considered. This should provide guidelines on responsible practices including, as a minimum, a definition of what constitutes vulnerability and ethical practices and guardrails to be consistently adopted and evidenced by the accredited entities.

Finally, it is critical to define principles and boundaries for the ethical sharing of data between government agencies.

Impact on human rights

Consideration should be given to implementing a human rights impact assessment on any proposed deployment of AI informed decision making. This could be leveraged to identify any mitigation measures that might be required to protect vulnerable people or provide alternative pathways for the AI-informed decision-making system. KPMG notes that special consideration may need to be granted for activities that fall under national security legislation.

RECOMMENDATION 10:

To further support responsible AI practices in Australian Government agencies, KPMG recommends consideration of defining principles and boundaries for ethical data sharing practices and an assessment of the impact on human rights.

8. In what circumstances are generic solutions to the risks of AI most valuable? And in what circumstances are technology-specific solutions better? Please provide some examples.

KPMG notes another challenge is that not all AI is the same, carries the same risk or has the same implementations, making regulation difficult.

KPMG considers that the legislative and regulatory framework should be technology neutral, and that there should be a clear definition of and parameters for AI. This enables principles and guidelines to be tied to how these technologies are being used in various contexts, rather than the technology itself. This approach addresses the challenges associated with the different impacts (i.e., positive versus negative versus unintended consequences) that the same technology can have depending on how it is used. It also results in a higher resiliency of the framework to technological advancements and breakthroughs.

9. Given the importance of transparency across the AI lifecycle, please share your thoughts on:

a. where and when transparency will be most critical and valuable to mitigate potential AI risks and to improve public trust and confidence in AI?
b. mandating transparency requirements across the private and public sectors, including how these requirements could be implemented.

Transparency and explainability are some of the key principles of trustworthy AI and are critical in ensuring safe and responsible AI use in Australia. They are also necessary prerequisites for the ability of individuals or groups to contest the outcomes or impacts of AI systems and seek redress in instances where harm is caused.

KPMG supports the conclusions and recommendations made by the Australian

Human Rights Commission in its 2021 *Human Rights and Technology Final Report* that there should be transparency about when and how government uses AI to make decisions, that individuals should be notified when government uses AI in administrative decision-making, and there should be clarity about when and how government bodies provide reasons for AI-informed administrative decisions.[14] The report also recommends an independent audit of all current or proposed use of AI-informed decision making by the Government, to ensure the quality and safety of such systems.

The circumstances in which the private sector is subject to the same expectations should be considered, including the requirements placed on developers of AI systems to be transparent about the data used to train an AI system and, for example, any methods used to test or screen for biases.

When errors happen, it is crucial for organisations to disclose what went wrong - without transparency, people are unlikely to have confidence in the use of AI technologies. If something goes wrong, transparent disclosures on why the particular use case was deemed to have complied with AI ethics principles (or other decision-making framework used) would assist in maintaining consumer confidence in the technology.

Internationally, the concept of 'human-in-the-loop' is also gaining momentum. The concept empowers people to use AI to do their jobs better and ensures a computer-human interface. KPMG considers that having a human-in-the-loop will also promote understanding and acceptance of AI.

RECOMMENDATION 11:

KPMG suggests it would be useful to consider the introduction of transparent disclosure obligations that require organisations to disclose why an AI use case was deemed to have complied with the particular ethics framework.

RECOMMENDATION 12:

KPMG suggests the regulatory framework should be founded on a core set of principles, ideally based on current established principles (such as: safety, security, robustness, fairness, transparency and accountability). These principles should be able to be translated into effective assessment and assurance framework tools that organisations can embed.

10. Do you have suggestions for:

a. Whether any high-risk AI applications or technologies should be banned completely?
b. Criteria or requirements to identify AI applications or technologies that should be banned, and in which contexts?

KPMG considers that there are certain AI applications or ADM tools that may not be appropriate, that may be damaging and may undermine fundamental values of our society, including democracy and human rights, and should be banned.

While KPMG recommends against a technology-based regulatory approach in most cases, the EU AI Act is helpful in identifying what might be the criteria and implications of certain applications being considered high risk. Specifically, the EU AI Act in its current draft form prohibits certain AI systems because they present an unacceptable risk to human rights, public interests and human safety and dignity. Prohibited systems use subliminal or manipulative techniques to distort behaviour and cause harm, involve public social credit systems, or biometric identification for law enforcement, except in limited circumstances in which such identification is permitted.

KPMG also supports the proposal in the Privacy Act Review to regulate activities with high privacy risks which would capture some AI systems and technologies.

Compatibility with liberal democratic principles

KPMG considers that there is merit in considering if there are uses of AI and ADM that are inherently inconsistent with Australia's position as a liberal democracy because of the risk such uses pose to the rights and fundamental freedoms of individuals as well as potentially to their safety.

Facial recognition technology

KPMG welcomes further consultation on the topic of facial recognition technology and suggests considering the introduction of a process (in lieu of a legal moratorium) which requires organisations to discuss the use case for applying facial recognition with a designated AI regulator/AI Commissioner to seek approval or licensing for the use case.

[14] Human Rights and Technology Final Report – Australian Human Rights Commission, 2021

11. What initiatives or government action can increase public trust in AI deployment to encourage more people to use AI?

The successful adoption of AI can be assisted by addressing the public's current lack of trust in AI by ensuring regulations and laws are sufficient to ensure AI use is safe.

KPMG and the University of Queensland's research found that only two in five people believe current regulations, laws and safeguards are sufficient to make AI use safe.[15] This aligns with previous surveys by KPMG and the University of Queensland showing public dissatisfaction with the regulation of AI, and is problematic given the strong relationship between current safeguards and trust in AI demonstrated by our modelling. This highlights the importance of strengthening and communicating the regulatory legal framework governing AI and data privacy.

To enhance trust in AI, the government should create awareness about the benefits of AI and its potential impact on society by showcasing examples of AI positively impacting key areas such as health, education and the environment - as well as lessons learnt when things go wrong.

The government should also recognise the generational differences that impact appetite and sensitivities to new technology. Government can work towards balancing competing priorities as custodians of people's data and the need to deliver more personalised services. This work includes implementing data protection measures, adopting ethical principles, using data analytics responsibly, and involving citizens in decision-making processes.

KPMG and the University of Queensland's 2020 report, *Trust in Artificial Intelligence: Australian Insights* identifies the following design and governance principles and practices that will help organisations drive greater trust, transparency and accountability in AI.[16]

1. **Technical robustness and safety:** performance and accuracy of AI system output is tested in a range of situations.
2. **Data privacy, security and governance:** safety and privacy measures are designed into the AI system.
3. **Human agency and oversight:** appropriate control of AI systems and their impact on stakeholders.
4. **Transparency and explainability:** the purpose of the AI system, how it functions and arrives at its solutions, and how data is used and managed is transparently explained and reasonably understandable.
5. **Fairness and non-discrimination:** system outcomes are tested regularly to ensure they are fair, free of unfair bias, and designed to be inclusive
6. **Accountability and contestability:** clear accountability and responsibility if something goes wrong with an Ais system. Impacted stakeholders are able to challenge system outcomes.
7. **AI literacy:** people are supported in understanding AI systems.
8. **Risk and impact mitigation:** the risks, unintended consequences and potential for harm from an I system are fully assessed and mitigated prior to and during its deployment.

Initiatives for increasing trust

KPMG puts forward the following initiatives for consideration:

- The development of a certification regime for responsible AI. A nationally and/or internationally endorsed accreditation system developed by a recognised national and/or international standards body will help with building greater transparency and, therefore, trust.
- Embedding data quality requirements in the accreditation framework to make sure users of the data have the right capability to understand the quality implications and use it in the right context based on the provided metadata.
- Conducting a public education campaign to allow people to better understand AI, and therefore trust and accept it.
- Where AI systems are operating in critical functions with high risks to people, potentially impacted communities should be engaged, with a focus on the most vulnerable and marginalised stakeholder groups.
- Other trust-building measures for consideration include licencing, auditing, impact assessment and regulatory oversight

[15] Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. (2023). Trust in Artificial Intelligence: A Global Study. The University of Queensland and KPMG Australia.

[16] Lockey, S., Gillespie, N., & Curtis, C. (2020). Trust in Artificial Intelligence: Australian Insights. The University of Queensland and KPMG Australia.

that can prevent the potential harms poorly deployed AI and ADM create.

RECOMMENDATION 13:

KPMG recommends a range of initiatives that may increase public trust in AI deployment, including the development of a certification regime for responsible AI, embedding data quality requirements, public education campaigns, and other measures such as licencing, auditing, impact assessment and regulatory oversight.

Implications and infrastructure

12. How would banning high-risk activities (like social scoring or facial recognition technology in certain circumstances) impact Australia's tech sector and our trade and exports with other countries?

Australia will likely be a net importer of AI and emerging technologies, given that international technology firms already own and power most commercial AI systems locally. In order to stay competitive, businesses will continue to source and access cutting-edge and lower cost technologies internationally. This may result in ethical trade-offs where other countries may not have equivalent human rights protections in place.

Australian organisations deploying AI and emerging technology solutions will face significant challenges applying a 'human rights by design' approach to technologies developed in jurisdictions with diverging and potentially conflicting human rights values and standards.

To address this, KPMG recommends that policy makers introduce a system to test and govern AI and emerging technologies that we import against our human rights, data protection and related laws and ethical standards. This could be based on an internationally endorsed accreditation system developed by a recognised international standards body, where practical.

13. What changes (if any) to Australian conformity infrastructure might be required to support assurance processes to mitigate against potential AI risks?

Assurance mechanisms are shown to create trust in AI systems. Three out of four people (75 percent) report they would be more willing to trust an AI system when assurance mechanisms are in place that support ethical and responsible use.[17] These mechanisms include monitoring system accuracy and reliability, using an AI code of conduct, oversight by an independent AI ethical review board, adhering to standards for explainable and transparent AI, and an AI ethics certification.

Looking at international examples, the proposed EU AI Act requires AI and ADM applications in high-risk areas to be actively approved in a conformity assessment before they can be implemented. It may be worth considering whether aligning to this approach would be a suitable pathway for Australia to follow, while also considering any local nuances, for example in the specific approach to the conformity assessment, which could leverage the existing AI Ethics Framework.

RECOMMENDATION 14:

KPMG considers that the implementation of assurance mechanisms would facilitate greater trust in AI systems. The proposed EU AI Act requires high-risk applications of AI and ADM to be approved through a conformity assessment, and it would be worth considering whether aligning to this approach would be suitable for Australia.

[17] Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. (2023). Trust in Artificial Intelligence: A Global Study. The University of Queensland and KPMG Australia.

Risk-based approaches

14. Do you support a risk-based approach for addressing potential AI risks? If not, is there a better approach?
15. What do you see as the main benefits or limitations of a risk-based approach? How can any limitations be overcome?
16. Is a risk-based approach better suited to some sectors, AI applications or organisations than others based on organisation size, AI maturity and resources?
17. What elements should be in a risk-based approach for addressing potential AI risks? Do you support the elements presented in Attachment C?

KPMG supports a risk-based approach for addressing AI risks. Consistent with KPMG Australia's *Human Rights Policy*[18] and the KPMG International *Business and Human Rights Statement*,[19] KPMG recommends that any risk-based approach focus on the potential harms to people in the first instance. This approach demands that any entity designing or deploying AI or ADM tools do so with systems and controls in place to avoid causing or contributing to negative human rights impacts, that they address any impacts that do occur, and provide an effective remedy if harm is caused. The benefit of a risk-based approach is that it leads to the systematic identification of potential risks and a proactive approach to avoid those risks.

KPMG considers that the government could usefully explore with industry the development of an initial human rights risk assessment to determine an AI project's potential risks to people upfront and ensure the appropriate level of governance oversight and remediation is applied. In certain contexts, where the risks to people may be high (e.g., in the contexts of employment, education, healthcare, banking or insurance) the government may also consider requiring that before they are deployed, AI systems are subject to an independent audit for consistency with core principles. This approach is being taken in jurisdictions in the United States in the context of employment specifically.

The scheme should encourage specific risk management frameworks that clearly articulate what is required from the internal environments of all parties (including Data Custodians, accredited data service providers (ADSPs) and so on). The Australian risk management model adopted by the Australian National Audit Office (ANAO) could be referenced as an example for a data management framework. This model by the ANAO maps out all risks, controls, shared risks, consequences, and roles.

Additionally, an ongoing human rights due diligence approach would enable a fair apportioning of accountabilities throughout the supply chain and allow organisations to confidently innovate while effectively protecting human rights.

Finally, for a risk-based approach to be most effective, it requires a strong organisational culture, strategic capabilities to establish the governance and systems and controls necessary, and a commitment to ongoing monitoring and continued improvement.

RECOMMENDATION 15:

KPMG considers that the government could usefully explore with industry the development of an initial human rights risk assessment to determine an AI project's level of risk to people upfront and ensure the appropriate level of governance oversight and remediation is applied.

18. How can an AI risk-based approach be incorporated into existing assessment frameworks (like privacy) or risk management processes to streamline and reduce potential duplication?

The risks that may arise through the design, deployment and use of AI and ADM systems will, in many instances, concern risks for which assessment and risk management frameworks already exist, for example, with regard to privacy, cyber security, and worker health and safety. In these instances, new assessment frameworks are not necessary but may need to be revised to take into account unique features of AI and ADM. For example, the United States National Institute of Standards and Technology (NIST) have an AI Risk Management Framework that aligns with other NIST risk management frameworks.[20]

In those instances where existing assessment frameworks are not in place (e.g., if human rights impact assessments are not a part of business as usual) then they will need to be introduced. In addition, having an overarching AI policy and guidance to articulate the policy

[18] KPMG Australia Human Rights Policy
[19] KPMG International Business and Human Rights Statement

[20] AI Risk Management Framework – US National Institute of Standards and Technology

commitment, speak to the purpose of assessment in the context of AI and ADM, and recognise the unique risks they pose would be helpful to ensure a comprehensive and complementary approach across assessment frameworks.

Promote transparency

Entities should include information in their external facing privacy policies and collection notices that advises individuals/consumers that their personal information will be used for artificial intelligence decision making and what types of decisions. This should also include transparency and explainability in AI systems to help individuals understand how data is being used and for what purposes that will impact them.

Consent

The Privacy Act reform proposals are focused on increasing individual/consumer control over their personal information. This consent regime should be reviewed to ensure it is fit for purpose in relation to use of personal information for automated decision making and higher risk privacy activities.

Strengthened individual rights

The current and proposed rights for individuals in the Privacy Act 1988 should reflect the use of personal information in AI and provide the right to request human intervention in decisions. For example:

- Individuals who have received a decision/outcome as a result of AI decision making processing should be offered the right to have their outcome reviewed with human intervention to avoid any unwanted biases and discriminations.
- Individuals should be afforded the right to opt out of automated decision making as well as have their personal information quarantined or erased after being fully informed of the consequences and alternatives.
- Responses to information access and correction requests in relation to these decisions be required to include meaningful information about the logic involved in such decision-making processes.

Privacy by design

In order to build community trust in the use of AI, the role of Privacy Impact Assessments (PIAs) will be important to help identify the privacy impacts and risks of AI projects early on and take into consideration ethical and community expectations, as well as document appropriate recommendations for managing, minimising and eliminating the impact. As previously noted, the Privacy Act Review proposes increased obligations to conduct PIAs for high risk privacy activities as well as requirements to submit these to the regulator, which would cover the use of AI in some cases.

The related role of Algorithmic Impact Assessments as well as human rights impact assessments would also support the analysis of privacy impacts from the use of algorithms.

Sensitive personal information

Additional restrictions should apply when sensitive personal information is used in AI. These additional requirements should be prescriptive in nature and supported by legislative intervention. Further, guidance should be developed to advise entities of the types of statutory conditions that must be satisfied when using sensitive personal information for AI.

Data quality

Data quality is crucial in AI because it directly impacts the performance, accuracy, and reliability of artificial intelligence models. The Privacy Act currently imposes obligations in relation to data quality, and the Privacy Act Review acknowledges that these obligations together with the proposed rights in relation to information about ADM would help to safeguard the integrity of automated decisions through obligations relating to personal information used in ADM systems. It will be important that specific guidance is developed to ensure entities understand the standard of controls they are required to have in place to ensure the ongoing quality of the personal information they use to train AI and make decisions.

Defined privacy and data protection frameworks

AI systems often rely on vast amounts of data including personal information. Current privacy law frameworks such as the Privacy Act (and OAIC guidance), State based information privacy laws and guidance, as well as the GDPR should be taken into consideration as part of the development of the regulatory framework establishing rules for the collection, use and processing of personal information. We have outlined the current proposals in the Privacy Act Review relevant to ADM, rights, transparency and the quality of personal information as aspects of privacy rights and rules that are relevant to AI. These should be further considered to ensure clear and robust legislative requirements and supporting guidance to ensure entities understand their obligations and the steps they need to take to manage AI related risks including leveraging existing defined frameworks.

Strengthening and clarity of security measures

There should be appropriate incentives and legislative obligations with supporting guidance to ensure the right level of security controls and safeguards are in place and documented, supported by regular testing (e.g., penetration testing, vulnerability scans, security assessments) to provide the required assurances in relation to responsible and secure AI. Entities should be able to leverage and uplift existing security measures and mechanisms that for example ensure personal information used in AI is sufficiently protected from unauthorised, use, disclosure and modification. The addition of further policies and frameworks to be administered through different regulators will risk confusion (as currently exists in relation to cyber security and data protection obligations). We refer to our recommendations in relation to the advisory and oversight roles that could be established and the need to ensure consistency and clarity in the regulatory framework that will apply.

19. How might a risk-based approach apply to general purpose AI systems, such as large language models (LLMs) or multimodal foundation models (MFMs)?

KPMG refers to our response in relation to risk-based approaches to questions 14-17.

In addition, given the reach of general purpose AI systems, it is important to ensure that unintended consequences and potential for harm are fully assessed and mitigated prior to, and during, the deployment of any general purpose AI system. Particular care should also be given to human rights and vulnerable cohorts (i.e., how they may use and/or be impacted by the outputs of these systems).

20. Should a risk-based approach for responsible AI be a voluntary or self-regulation tool or be mandated through regulation? And should it apply to:

a. public or private organisations or both?
b. developers or deployers or both?

KPMG and the University of Queensland's research shows that Australians prefer AI to be regulated by government and existing regulators, or by an independent AI body, rather than by industry.[21] 66 percent of Australians think the government should regulate AI, while co-regulation between industry and government, and regulation by existing regulatory bodies are also popular options. In comparison, 42 percent of Australians think industry self-regulation is desirable compared to other forms of external or co-regulation.

KPMG's recent report with the Australian Information Industry Association (AIIA) *Navigating AI* finds that self-regulation may not be sufficient as it may not address all necessary measures. Despite the potential for self-regulation, history has shown that industries driven by profit motives are not successful in regulating themselves. Agreement on regulatory goals is necessary before effective self-regulation can occur – and the EU is leading the way in developing more concrete frameworks to regulate AI. Similar to regulations protecting people from human biases, laws can also protect people from AI biases.

Government and industry have an ongoing responsibility to ensure that AI is designed, developed and implemented to ensure it meets societal expectations and regulatory requirements. This is particularly important as our understanding of AI opportunities, risks and applications in new fields continues to evolve and grow.

KPMG also considers that the impact of regulatory tools will also be limited unless there is an enforcement mechanism to support them. The empowering of regulators who are responsible for enforcing laws that will intersect with AI will need to be considered.

RECOMMENDATION 16:

KPMG considers that self-regulation may ultimately not be sufficient, and agreement on regulatory goals is necessary before effective self-regulation can occur.

[21] Gillespie, N., Lockey, S., Curtis, C., Pool, J., & Akbari, A. (2023). Trust in Artificial Intelligence: A Global Study. The University of Queensland and KPMG Australia.

Key authors and contacts

James Mabbott
Partner in Charge, KPMG Futures

Richard Boele
Chief Purpose Officer; Partner, KPMG Banarra, Human Rights & Social Impact Services

Danielle Malone
Partner in Charge, Data & Cloud

Veronica Scott
Partner, Cyber, Privacy & Data Lead, KPMG Law

Kelly Henney
Partner, Privacy & Data Protection Lead

Dean Grandy
Lead Partner, Technology – Infrastructure, Government & Healthcare

Lhamo Tenzin
Partner, Consulting

Dhawal Jaggi
Partner, Data & Cloud

Shubham Singhal
Director, Privacy and Data Protection

Susan Staples
Director, Governance, Risk & Controls Advisory

Samantha Kwong
Director, Consulting

Francine Hoo
Director, Audit & Assurance

Jessica Wyndham
Associate Director, KPMG Banarra

Rebecca Kitt
Associate Director, Privacy & Data Protection

Dr. Christina Kleinau
Associate Director, Data & Cloud

Dr. Melinda Rankin
Associate Director, Risk Advisory

Craig Campbell
Associate Director, Consulting

Rita Fentener van Vlissingen
Associate Director, ESG & Impact

Jason Kaye
Manager, KPMG Law

Ben Sasse
Manager, KPMG Law

Elly Krambias
Senior Consultant, KPMG Law

Niran Garcha
Senior Consultant, Privacy & Data Protection

Jessica Herbert
Consultant, KPMG Banarra

Sophie Finemore
Director, Corporate Affairs

Olivia Spurio
Manager, Corporate Affairs

Lachlan Hill
Senior Consultant, Corporate Affairs

KPMG.com.au