Comments on "Safe and Responsible AI in Australia" Discussion Paper

24 July 2023

Workday appreciates the opportunity to comment on the Department of Industry, Science and Resources' ("DISR") Discussion Paper regarding Safe and Responsible AI in Australia ("Discussion Paper"). Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics are built with artificial intelligence and machine learning at the core to help organizations around the world embrace the future of work. Workday is used by more than 10,000 organizations around the world and across industries – from medium-sized businesses to more than 50% of the *Fortune* 500. With offices in Brisbane, Melbourne, and North Sydney, two in-country data centres, and a customer support presence, we are proud of our robust offerings in Australia. Workday serves major Australian customers including Atlassian, Canva, the Commonwealth Bank of Australia, Latitude Financial Services, One Rail Australia, QANTAS, Reece Group, Telstra, and St Vincent's Health Australia.

At Workday, we believe that Artificial Intelligence ("AI") is powering the future of work by unlocking human potential, driving business value, and enabling our customers and their employees to focus on more strategic and fulfilling work. Consistent with our commitment to ethical AI, Workday has been helping to lay the groundwork for smart AI safeguards since 2019.

Workday supports the development of safe and responsible AI policies, regulations and practices that are meaningful, technically sound, and advance responsible innovation. Building on our call for AI regulation, Workday offers the following recommendations to select portions of the Discussion Paper. Please do not hesitate to contact Eunice Lim, Director Corporate Affairs - APJ, at eunice.lim@workday.com if you have any questions or would like further information.

I. Enhance Regulatory Coherence

As the Discussion Paper rightfully points out, there are existing legislations in Australia which may already provide the guardrails required to protect against AI harms, such as the Privacy Act, Australian Consumer Law, anti-discrimination laws, and Online Safety Act, among others. These legislations can inform how AI tools used in consequential decisions can be further regulated. For example, the proposed introduction of rights regarding "*automated decision making with legal or similarly significant effects*" under the ongoing Privacy Act review or new powers to combat online misinformation and disinformation generated using AI technologies under the Online Safety Act. As a constructive first step towards supporting the safe and responsible development and adoption of AI, Workday supports further examination of the current domestic governance landscape, with the aim to minimise potential regulatory overlap and enhance regulatory coherence.

II. Risk-Based Approach to AI Governance

The development and use of AI tools is growing rapidly. To navigate these dynamics, policymakers are converging on a risk-based approach to AI governance that maximises the benefits of AI and minimises the risks of potential harm. Many of the countries referenced in the Discussion Paper, including the European Union ("EU"), Canada, the United Kingdom, and Singapore, have adopted a risk-based approach to AI governance, which means applying rules to contexts where AI carries the highest risk of potential harm to individuals. As AI systems are and will be used in a wide variety of scenarios, policies and regulations must be designed to reflect this diversity in risk profiles

To achieve a risk-based approach to AI governance in practice, Workday recommends that policymakers:

a) Focus regulatory efforts based on consequential decisions with high risk of harm.

The AI ecosystem is broad, encompassing a diverse range of technologies and use cases and a wide array of stakeholders. Because the risks of AI are inherently use-case specific, any regulations should focus on specific applications of the technology that pose higher risks to the public but should be flexible enough to account for the unique considerations that may be implicated by specific use cases. It is therefore important to define what such higher risk use-cases are and avoid assigning risks solely based on a sectoral approach. High-risk AI use-cases can include an AI tool that is used for a decision about an individual's access to an essential opportunity where it has the potential to pose harm to that individual. AI regulatory efforts should focus on these kinds of consequential decision tools, which may be used to hire, promote, or terminate an individual's employment, or in other contexts, determine access to credit, healthcare, or housing. For example, the American Data Privacy and Protection Act, among other leading proposals, focuses on AI tools used in ways that pose a "consequential risk" to individuals.

Workday notes that the Discussion Paper already takes a risk-based approach to AI governance, and we are supportive of an approach that is tiered according to different levels of risks. Box 4 illustrates a draft risk management approach setting out three risk levels – low, medium, and high. While the current thresholds for determining the three risk levels lie in whether the impacts on individuals are: i) time-bound (limited, ongoing, systemic) and ii) reversible, Workday recommends including "consequential decisions" as another factor for consideration, especially for use cases under the medium and high-risk categories to further strengthen the risk-based management framework. This would also bring it in line with leading frameworks in the EU and US.

b) Distinguish between automated tools and tools with a human in the loop.

Regulations should also focus on fully automated AI tools that seek to replace human decisions rather than those that augment human decision-making. This is because an automated tool can make consequential decisions at a higher volume and velocity than a human, and without the judgment that a human brings. By contrast, when an informed human is in the loop, they can leverage an AI tool's insights and remain in control of and accountable for the final decision.

Attachment C of the Discussion Paper outlines instances where assessments may be required in circumstances involving human oversight, however the section also acknowledges that such requirements may not be appropriate where there are benefits related to efficiency and automation at scale and potential impact on individuals is minor. Workday is supportive of this nuanced distinction and would encourage DISR to adopt a similar approach when looking at different elements that would support the safe and responsible development and adoption of AI.

III. Importance of Role-based Obligations in AI Governance.

AI governance is a shared responsibility between *developers*, which design, code, and produce an AI tool, and *deployers*, which operate and use the tool and interact with end users. *Developers* typically have insight into how an AI tool is built but may not have access to their customers' data or control over how a customer configures and uses the tool. By contrast, *deployers* determine how an AI tool is implemented and used, but typically do not have control over how the AI tool was designed. As explained in the OECD's Recommendation, effective AI policies must necessarily account for "stakeholders according to their role and the context" in which AI is being deployed.[1] The OECD also recognises this distinction in the risk management context as AI "in the lab" (i.e., developers) versus AI "in the field" (i.e., deployers). Distinguishing between AI developers and AI deployers ensures that specified obligations reflect an entity's role in the AI ecosystem. Tailoring obligations to an entity's role as an AI developer or AI deployer would also enable the company to fulfil the corresponding obligations and better protect consumers.

For instance, AI developers are better positioned to have access to information about the type of data that is used to train an AI system, the system's known limitations and its intended use cases. However, the AI developer would not have insight into how the AI system is used after another company has purchased and deployed the AI system. Instead, the AI deployer – the entity using the AI system – is generally best positioned to provide details on how the system is being used, the outputs from the AI system, the nature of any customer complaints, and other real-world factors affecting the system's performance. AI deployers are also best positioned to understand the risk profile that an AI system may present to individuals. Ensuring AI policies create obligations that reflect these different roles will allow the different entities within the AI ecosystem to better understand how their organisations can identify and address harmful bias in AI systems.

As the Australian Government considers its options regarding AI governance, Workday strongly recommends that DISR incorporate this important role distinction by separately defining "developers" and "deployers" and assigning obligations to both types of entities that reflect their different roles.

IV. AI Risk Management Programs

A risk management program provides the overarching framework necessary to identify, document, and mitigate AI risks. It ensures that appropriate personnel have been designated to oversee accountability measures, that organisational policies are established to guard against risks of algorithmic discrimination, and that processes are in place to implement safeguards that address any issues identified in the impact

[1] OECD Recommendation (2019). Per the Recommendation, the AI stakeholder community "encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly."

assessments and design evaluations. A key purpose of such AI risk management programs would be to help drive accountability and transparency within the organisation. It would also provide a basis for organisations to document their compliance to regulators and to the outside world. In principle, Workday supports the adoption and implementation of internal AI risk management programs by organisations deploying and developing AI and the nature of the obligations proposed in Box 4 of the Discussion Paper.

However, obligations associated with AI should not apply to all entities in the AI ecosystem in the same way. Box 4 outlines some of the risk management requirements/obligations based on the risk levels, however, without a distinction between an AI developer and AI deployer, it does not clarify which entity is better suited to comply with these proposed requirements/obligations.

For any AI risk management programme to be effective, it is important to assign obligations to the entity that is best positioned to identify and mitigate the risk of harm to individuals. Workday would like to reiterate the importance of clearly distinguishing the role of an AI developer from an AI deployer which will minimise uncertainty about which entity will bear responsibility with respect to complying with the requirements and better enable organisations to fulfil responsibilities according to their different roles.

For example, AI deployers would be in a better position to meet the requirements to i) provide notices to individuals, ii) provide explanations regarding the AI output to users; and iii) ensure that there is a meaningful human intervention at various points of AI deployment. In contrast, the requirements to conduct self-assessment and to monitor and document the AI system fall on both the deployer and developers, and the extent of their obligations could differ depending on the information required.

In this regard, Workday recommends that DISR draw on the US' National Institute of Standards and Technology Artificial Intelligence Risk Management Framework which identifies specific practices that AI developers and deployers can implement to ensure that AI is developed and used responsibly.

V. Practicable Governance Mechanisms and Accountability Tools

The field of AI governance is nascent, with best practices, standards, and accountability tools still maturing. When considering guardrails for high-risk AI tools, policymakers should consider which proven, workable approaches are available today and which require additional building blocks to be in place before they can be implemented effectively.

In this regard, Workday commends DISR for proposing impact assessment as one of the requirements under the draft risk management framework to help organisations manage risks associated with AI.

Workday is supportive of impact assessments as they are a proven accountability tool. Impact assessments are widely used by organisations to identify, document, and mitigate the risks posed by technology, especially in the fields of privacy and data protection as they are required under the EU's General Data Protection Regulation. Notably, they are also helpful tools in detecting and mitigating potential bias that could result in unlawful discrimination. There is also a growing consensus among lawmakers, business leaders, and civil society that impact assessments for high-risk AI tools are the most promising AI accountability tool available today.

Impact assessments are also practical because they are a holistic and iterative risk evaluation that can be carried out by a developer and deployer of a high-risk AI tool and do not rely on still-nascent technical standards. In contrast, AI auditing is a field that is still in development, as there are neither consensus

technical standards nor a common set of criteria to audit AI tools against. There is also no professional standards that are binding on third-party AI auditors, which are necessary for ensuring auditing quality and integrity. Without such standards, the scalability of AI auditing is a significant practical challenge. Given so, we would urge policymakers to avoid instituting pre-mature third-party audit requirements as this may unintentionally diminish trust in the AI marketplace by failing to promote consistent accountability.