Comments on Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems

24 August 2023

Workday appreciates the opportunity to comment on the Personal Data Protection Commission's ("PDPC") "Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems" ("Advisory Guidelines"). 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.

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. We have taken a leading role in AI policy discussions at the federal, state, and local level in the United States. Workday has also partnered with officials in the European Union on the Artificial Intelligence Act, as well as with governments around the world, to provide thoughtful and concrete policy approaches to responsible AI.

At the outset, Workday commends PDPC on its efforts in developing this set of draft Advisory Guidelines. Singapore has been at the forefront of leading various AI Governance initiatives such as the Model AI Governance Framework, the Implementation and Self-Assessment Guide (ISAGO), and the AI Verify Toolkit. Workday believes that when completed, these Advisory Guidelines would help lead to meaningful progress in global discussions on the development and adoption of trustworthy and responsible AI.

Workday supports the development of AI-focused policies, regulations, and practices that are meaningful, technically sound, and advance safe and responsible innovation. Building on our early call for AI regulation, Workday offers the following recommendations to select portions of the Advisory Guidelines that highlight the need to:

- Expressly reflect the distinction between AI developers and AI deployers; and,
- Include impact assessments as an additional accountability tool.

I. Importance of Role-based Obligations in AI Governance

As we have seen in similarly situated regulatory frameworks, Workday believes that in order to be effective and build trust AI governance needs to be 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. The 2019 OECD Recommendation makes clear that 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). Tailoring obligations to an entity’s role as an AI developer or AI deployer not only ensures that specified obligations accurately reflect the entity’s role in the AI ecosystem, but also enables the entity to fulfil the corresponding obligations and better protect consumers.

This “developer – deployer” distinction is conceptually similar to, although distinct from, the “controller - processor” distinction under data protection and privacy laws (e.g., the European Union’s General Data Protection Regulation) and continues to be relevant in the context of these Advisory Guidelines. The Advisory Guidelines are organised according to the stages of AI systems implementation: i) Development, testing and monitoring, ii) Deployment, and iii) Procurement; and Workday notes that PDPC has already implicitly taken into consideration the “developer-deployer” distinction when assigning the relevant PDPA Obligations and clarifying how the various obligations would apply, depending on the implementation stage that an AI system is in.

For instance, during the development stage, developers of AI are better positioned to have access to information about the type of data that is used to train an AI system and its intended use cases. Hence the PDPA Obligations pertaining to training data anonymisation and/or pseudonymisation would best apply during the AI development stage. Conversely, it is the AI deployer – the entity using the AI system – which would have insights into how the AI system is used and therefore best positioned to provide details about new data being fed into AI systems, the outputs from the AI system and other real-world factors affecting the system’s performance. In this regard, we agree that the Notification and Consent Obligations and Accountability Obligation would best apply during the AI deployment stage.

Indeed, the Advisory Guidelines already make many references to concepts related to the developer-deployer distinction but do not directly address or explain the distinction**. We recommend that the Advisory Guidelines clearly articulate and reflect the developer-deployer distinction, for example within Paragraph 3.2, which sets out stages of AI System implementation**. 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 and ultimately support the goal of building trust in AI systems.

Further, while there is much to draw from the “controller-processor” concept when discussing AI governance approaches, we would be mindful of likening business-to-business service providers of bespoke or fully customisable AI systems to “data intermediaries” as mentioned in Paragraph 11.2. The reference to “data intermediaries” is potentially confusing as an enterprise SaaS company that is developing AI systems as part of their products and services would also typically be regarded as a “data intermediary” or “data processor” in the data protection context. If the policy intent is to make clear that

[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.”

certain AI service providers are still subject to the PDPA, we would recommend specifying what these obligations are and remove the reference to “data intermediaries” in 11.2. In fact, the applicable PDPA Obligations should principally be dependent on an organisation’s role within the AI ecosystem, and we would reiterate our call for PDPC to make clear the distinction between developers and deployers of AI systems in the Advisory Guidelines. This would then clearly assign obligations to the entity best positioned to both identify and mitigate the risk of harm.

II. 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 AI systems, in particular high-risk AI uses, 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.

Singapore has worked closely with the industry in the development of AI governance mechanisms and accountability tools since 2019. The Advisory Guidelines highlight several of these initiatives such as the ISAGO and AI Verify toolkit as additional resources that organisations may wish to leverage to support their compliance efforts.

In addition to aforementioned tools, Workday would also encourage PDPC to include impact assessments as an additional resource for organisations to consider. Impact assessments are a proven accountability tool and are already widely used by organisations to identify, document, and mitigate the risks posed by technology, especially in the fields of privacy and data protection. The PDPC has previously published a Guide on Data Protection Impact Assessments (“DPIA”) encouraging organisations to conduct DPIAs. Notably, impact assessments 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. Given so, **Workday recommends for impact assessments to be included as a potential accountability tool under the sub-section, “Additional resources”.**

Workday is committed to supporting efforts to develop meaningful AI safeguards and is heavily engaged in AI-focused conversations around the world in order to ensure a regulatory and policy landscape that builds trust in AI and supports innovation. We appreciate the thoughtful approach PDPC has taken and the leadership role Singapore has played in the region and in the global conversation. We would welcome the chance to continue our engagement on this important topic as the process moves forward. 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.