Workday contribution to the consultation on the European Commission’s proposal for a Regulation Laying Down Harmonised Rules On Artificial Intelligence (AI Act)

August 2021

Executive Summary

Workday’s response to the European Commission’s proposal for regulation on artificial intelligence (the AI Act) draws on our contributions to the Commission’s preparatory consultations as well as earlier work developing Ethics Guidelines for Trustworthy AI. We highlight important areas of alignment between the Act and Workday’s January 2021 white paper including a horizontal approach to regulation, self-assessment, life-cycle analysis, transparency and provision of necessary information to deployers and end-users, as well as consideration of the ethical implications and impact of the technology on users.

Notwithstanding significant areas of alignment, we take issue with certain aspects of the Act and make recommendations for improvement. For example, we call into question the product-safety framing of the Act, noting that AI is not a product, it is a tool or method that can manifest in products, software, or services. We suggest that the Commission should consider adopting a framework more closely tied to ethical and trustworthy AI rather than product safety, at least for standalone software systems. We argue that certain aspects of the product safety framing do not make sense in this context, including post-market monitoring requirements and ordering products off market when they are deemed ‘unsafe.’

We further call into question the allocation of responsibilities in the Act, noting that as currently drafted the AI Act places disproportionate obligations on AI developers. For example, in the context of software as a service, AI systems are routinely trained and tested on data provided by the deployer of the system. In this instance, obligations such as ensuring that data sets are appropriately accurate and unbiased, retaining data documentation, and updating conformity assessments should rest with the deployer as well as, if not in place of, the developer.

We make several recommendations regarding tightening definitions and specifications, such as limiting the definition of AI to align with existing international standards and limiting the scope of high-risk employment systems to those that are intended to be used for hiring, promotion, or termination decisions. We note that the Act imposes significant requirements that apply three months after adoption, and companies will need greater specificity in guidance with regard to these definitions as well as accuracy, transparency, and other requirements in order to comply. We also explain that certain standards listed in the Act are impossible to meet and as such should be struck, such as the requirement that the training data be error-free and complete.

We strongly advise against requirements to provide Market Surveillance Authorities with source code and APIs to training and testing data as access to this type of information introduces significant data protection and trade secrets risks and should not be necessary to evaluate how a system works. Instead, required transparency to deployers and users, along with technical documentation of such, should more than suffice in the context of an ethical/trustworthy AI regulation. We argue that these types of requirements, along with specific guidelines regarding measures and metrics, will positively impact the AI market and will be welcomed by companies wishing to provide trustworthy, ethical, and quality products and services to customers and to the public.

Introduction

Workday welcomes the European Commission's proposal for regulation setting forth harmonized rules on artificial Intelligence (*i.e.,* the AI Act). 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 have been adopted by thousands of organisations around the world and across industries—from medium-sized businesses to more than 45 percent of the Fortune 500. Headquartered in Pleasanton, California, Workday has more than 13,000 employees worldwide and over 2,750 employees in our 21 offices across Europe. Workday has more than 650 customers headquartered in Europe, including Airbus, BlablaCar, ING, Siemens, Sanofi, Santander, and ThyssenKrupp.

Artificial intelligence is becoming an ever-increasing and transformative presence in our lives. The technology holds great promise if it is developed in an ethical and trustworthy manner but could harm individuals if misapplied or misused. We see manifestations of AI, primarily through machine learning (ML) applications, in every sector from transportation to robotics to analytics to workforce management to government. Like any technology, society (via laws and regulation) determines how it should be used; technology is not an inexorable force acting on society.

Given its transformative nature, it is important that AI be subject to proportionate regulation that protects fundamental rights and ensures that appropriate safeguards are in place where it is deployed in high-risk scenarios. Workday has been among the leaders in calling for AI regulation and participated in the European Commission's preparatory consultations leading up to the publication of the AI Act, as well as in the earlier work developing Ethics Guidelines for Trustworthy AI conducted by the High Level Expert Group on AI. Earlier this year we released a white paper which laid out a proposal for a 'Trustworthy by Design' regulatory framework for AI and ML. Drawing from risk-based models in the fields of cybersecurity and privacy, the framework is designed to promote trust, accountability, and transparency while also giving organizations broad flexibility to innovate. In many respects, our approach is aligned with the Commission's proposal: it calls for a life-cycle approach to evaluating AI systems, it embraces transparency and provision of necessary information to deployers and end-users, and it requires consideration of the ethical implications and impact of the technology on users. Further, in the U.S., we have worked with bipartisan stakeholders to pass legislation directing the National Institute of Standards and Technology to develop a trustworthy AI framework as the basis for future regulation. And we've been vocal in calling for the need for a harmonised transatlantic approach to AI policy, including participating in a hearing before the European Parliament's Special Committee on Artificial Intelligence in a Digital Age. Accordingly, we welcome the proposed AI Act and this opportunity to provide input.

General comments

Importantly, the Commission has taken a horizontal approach to regulating AI, rather than a sector-specific approach. While different sectors apply AI in different ways, and may have different existing legal and regulatory obligations, a sector-specific approach risks having both gaps, where technology falls in between the sector definitions, and overlaps, where it is used in multiple sectors subject to different rules. In addition, sector-specific rules create a non-uniform standard, confusing developers, deployers, and users about their obligations, responsibilities, and rights, ultimately blunting the overall effectiveness of the regulatory scheme. The Commission's approach of using standards to define sector-specific requirements and best practices, where needed, under a generally applicable approach is to be commended.

Also to be commended is the self-assessment approach to conformity assessment for AI on the European market. Simply put, a third-party assessment requirement for individual products/services will not work for AI technologies. Third-party assessment would extend time to market as it means companies would be dependent on a third party for release times, negatively impacting innovation. For software as a service, where improvements are released frequently, this could slow down innovation and product releases. Moreover, the range of AI applications would challenge any single assessment body, meaning that a third-party assessment regime would become fragmented at best and have gaps at worst.

Product safety framework

The model for the AI Act is product safety regulation (the New Legislative Framework approach). In some respects, this is a natural model for the Commission to have adopted; after all much AI is embodied in products, whether Internet of Things devices, cars, robotics, or other machinery. However, it is important to clarify that AI in itself is not a product but a method. For example, at Workday we create software services enhanced by machine learning. These services can be used to help accounting teams detect financial anomalies, help workers identify additional skills and opportunities, and suggest training content to learners based on their role and interests. While some such applications of machine learning will fall in the high-risk categories listed in Annex III, because they implicate important considerations such as those related to employment, they do not pose the same fundamental safety issues as a malfunctioning product.

Using existing product safety regulation for physical AI-powered products is sensible. However, for standalone software and services embedding AI, a regulatory framework should include a set of rules and requirements that guide developers, deployers, and users toward ethical and trustworthy technologies protecting the fundamental rights of citizens. Using a twentieth-century product safety approach to regulate AI does not translate well to the twenty-first century virtual world.

From this perspective, we highlight the following specific concerns:

- While we appreciate and support the self-assessment approach to conformity assessment, the required cadence for self-assessment must be clarified. At Workday, we have two major releases a year and smaller weekly updates in-between. Because it isn't clear what constitutes a significant update, we suggest that the self-assessment be required on specific time periods, such as annually. This corresponds to common audit periods for compliance with other regulatory regimes, such as privacy laws.

- Similarly, the AI Act requires post-market monitoring of AI systems. The challenge here is that unlike a stand-alone product that is put on the market by a manufacturer, AI systems are often deployed by entities other than the developer, and often with significant changes to their operations. The data used to train and test the specific system may belong to the deployer, rather than the developer. That is certainly true of Workday's ML functionality, where the services may be configured by our customers and operate on their data (whether their employee data or financial data). As such, post-market monitoring in the AI context is different than in a strict product context, where for example the requirement might be to ensure that a car operates properly and doesn't have a defect requiring a recall. Indeed, often, the developer of the AI system will not have access to data about how the product operates, because the deployer will not want to share that information with the developer, and indeed may prohibit such access contractually. Indeed, in some cases, laws such as GDPR may restrict or prohibit a developer's ability to access the deployer's data or monitor its usage of a data-powered system. Again, this is true of Workday's relationship with our customers, where given the sensitive nature of the information they store in our system, they do not want our direct involvement in their use of the technology beyond security and maintenance activities.
- The AI Act ultimately allows regulators to order a product off the market, even if the product is otherwise compliant with the Act. Again, this makes sense in the context of an unsafe physical product. However, software and systems are different. The existing authority for ordering removal of unsafe products from the market will be more than sufficient to protect against malfunctioning AI systems that pose a risk to physical safety, while other remedial measures can address purely software-based systems which do not present a risk of physical harm. This is especially true where the system is otherwise completely compliant with the AI Act, but the Act nonetheless gives the authority to remove it from the market.

Ultimately, the Commission should adopt a framework more closely tied to ethical and trustworthy AI rather than product safety. Such a regulation would be more actionable and more impactful on the industry. This is because the regulation would be better suited to the nature of AI in its various forms and to the real need for regulation in the marketplace. In addition, it would make it easier to harmonize with regulations in other jurisdictions, given they too are likely to take an ethical and trustworthy AI approach.

Allocation of responsibilities

Relatedly, we think it is important to make the AI Act more workable in a business-to-business context. As noted above, it is critical that the AI Act reflect the fact that developers of AI often provide the technology to deployers and not directly to end users. In Workday's case, we include ML-enabled features in our services, which our customers then deploy and use in their operations. As described above, our customers configure the service, which may impact how those ML-enabled features work (or if they are used at all). And our customers, because they include personal data and sensitive business information in our systems, do not want us monitoring their use beyond certain essential cybersecurity protections. Indeed, Workday contractually commits to not access client data aside from very limited cases and with their permission.

As currently drafted the AI Act places many more obligations on developers of AI systems than on deployers. Deployers must simply follow the developer’s instructions, monitor system operation, inform the developer if there is an issue with respect to the market obligations of the system, and retain logs. But in many cases, including those related to software as a service, the data that the AI system acts upon is provided by the deployer, and the developer has limited insight into how its system acts on that data set as opposed to the training data used to develop the AI system. Certainly, obligations with respect to testing for bias, ensuring that data sets are appropriately accurate and unbiased, and so on should rest with the deployer in these circumstances, as well as, or in place of, the developer of the system.

Similarly, the conformity assessment that the developer must provide pursuant to the Act should be limited to the operation of the system at the time and in the condition in which the developer puts it on the market. Although the developer should be cognizant of how the system will be used by deployers—including foreseeable misuse—it should not have to account in its conformity assessment for potential issues related to how the deployer implements and utilizes the AI system or the data on which the system operates, aspects over which the developer has no control. Put simply, where the deployer makes changes to the system then it should be responsible for assessing conformity from that point. This is true in other product safety contexts, where for example a car manufacturer does not bear responsibility for after-market modifications, particularly where they defeat safety features originally built into the car. The AI Act seeks to do this in Article 28, but that language should be expanded beyond modifying the system’s purpose or making a substantial modification to a high-risk system to include where the data provided by the deployer changes how the system operates, even without modification.

Further, as noted above, the monitoring requirement on the developer should be limited to requesting periodic feedback on the functioning of the AI system, keeping track of issues escalated to it, and taking reports (including public reports) regarding how the system operates. Real-time monitoring would be overly intrusive, exposing sensitive business information of the deployer to the developer, and would interfere with contractual relationships where providers of AI systems have committed to confidentiality with respect to the information of their customers entered into their systems. And as noted above, such monitoring might also interfere with legal requirements not to access data (or by the deployer to protect data from access). This is particularly true as relates to AI systems using employee data, as often works councils strictly control access to such data. Monitoring obligations would override those agreements, ultimately changing the negotiated relationship between developers and deployers and reducing AI uptake in business-to-business software contexts where there is concern about the scope and nature of the monitoring. That impacts not only us but our customers, who would forego the benefits of ML-enabled products and services out of concern that another company might monitor how they use them, revealing business information.

The AI Act also requires companies to retain training data. This obligation should be clarified so that it applies only to documentation specifying the sources and nature of training data. Machine learning systems require large amounts of data to train them, and they are constantly being refined and improved. Having to keep that data for an indefinite period would require untenable storage investment. And to the extent the data involved are personal data, keeping that data beyond the time needed to develop the system would be counter to the data minimization provisions of GDPR. Moreover, it isn’t necessary to access the actual data in order to assess how the AI or ML system was developed or how the data might have influenced expectations associated with the system. It is the nature of the data set, not the substance of the data itself, which is most relevant and important for that purpose. In instances where the deployer provides the data used to train the models, it should bear the documentation requirements, with a provision to share that information with the developer in the event of a regulatory inquiry. Where the deployer trains the system with its own data, the deployer should bear these documentation responsibilities.

Regulatory model

As noted previously, the AI Act will be transformative: the first major piece of horizontal legislation anywhere in the world governing AI development and deployment. As such, it will have a significant impact on a wide range of organizations that create and use AI. Given its horizontal nature, we support the Commission’s approach to use standards to flesh out requirements in specific areas, rather than adopt one-size-fits-all rules. That said, the AI Act imposes significant requirements that apply three months after adoption, so companies will not be in a position to wait for standards before needing to comply. As the Act moves through the legislative process, it will be vital to ensure that the requirements around accuracy, transparency and the like are clarified so that companies have a clear understanding of their obligations and responsibilities at the time the Act goes into effect. In addition, clarity around those requirements will help with harmonization with rules adopted by other jurisdictions, helping to create a coherent global regulatory framework.

Definitions

Beyond these operational concerns, we have some specific concerns with the definitions that govern what AI systems fall within the scope of the Act’s definition of AI, and which are classified as high risk.

Definition of AI. With respect to the definition of AI, a technology must both use a technique listed in Annex I and generate an output specified in Article III. In defining those outputs, Article III includes “software that is developed...for a given set of human-defined objectives…[to] generate any outputs such as content, predictions, recommendations, or decisions.” This is broader than the OECD definition of AI on which it is based, which 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.” The Act’s definition significantly broadens the OECD’s in that it includes not only decision-making systems and those designed to assist with decision making, but also systems designed to broadly produce “content.”

Similarly, the techniques in Annex I further broaden the scope of the definition. The OECD definition says that AI systems are “machine-based” and are “designed to operate with varying levels of autonomy.” However, Annex I sweeps far more broadly, including systems based not only on machine learning or computer science (which are the only types of systems designed to operate with a degree of autonomy) but also any software based on any type of knowledge, logic-based, statistical, or Bayesian approaches. This definition reaches far beyond a typical definition of artificial intelligence, which is generally limited to a type of machine-based system with the ability to engage in human-like processes such as learning, reasoning, or self-correction.

We would recommend that Article III be limited to predictions, recommendations, and decisions, striking "content." We would further recommend that Annex I be limited to section (a), focusing specifically on machine-learning techniques and striking logic, knowledge, statistical and Bayesian approaches. These two changes would bring the definition of AI more in line with OECD's definition and better align with more common definitions of AI as "human-like" or in some way "intelligent."

Definition of User. Beyond the definition of AI, the definition of "user" lacks precision in a way that could impact the Act's allocation of responsibilities within multi-actor business relationships, like in enterprise software. Importantly, the AI Act conflates individual end users and deployers. These roles should be clarified and separated. There are AI systems that a company develops and deploys, and that are used only by end users. Separately, there are AI systems, particularly in the B2B context, that one company develops and another deploys, wherein end users interact only with deployers. The Act defines "user" as any natural person, public authority, agency or other body using an AI system, except where the system is used in the course of personal or non-professional activity. This conflates deployers of AI with end users of the system. Given the importance of protecting the fundamental rights of EU citizens, it would be helpful to clarify whether end-users are considered users in the Act. The best way to do this would be to make clear these three roles: developer, deployer, and user. In some cases, the developer and deployer will be the same entity, and that entity will have all of the responsibilities of both. In others, those roles will be separate, as described above.

Definition of High-Risk Employment System. Similarly, as a company focused on the implementation of machine learning technologies in the human capital management space, we have concerns about how the AI Act defines what constitutes a high-risk employment system. We would agree that certain systems designed to assist in employment *selection* or *decision-making* should be designated high-risk. These are important decisions that make a material difference in people's lives and it is vital that strong rules apply to decisions made about hiring, employment opportunities, promotions, and terminations.

The current language, however, reaches more broadly than these core decision areas, sweeping in technologies that don't impact fundamental employment rights. The AI Act seeks to regulate high-risk scenarios, and it is important that its coverage be clear with respect to those scenarios, and not just sectors where some uses of AI will pose risk. In the employment space, something like our Skills Miner technology, which helps identify additional skills individuals may have and gives them the option, for example, of adding these skills to their worker profile, should not fall within the high-risk category. After all, it doesn't preclude workers from adding additional skills not suggested, or rejecting suggested skills; control over the employee's profile remains with the employee. For this reason, we would recommend that Annex III (4)(a) be deleted and that (4)(b) be edited so that it reads: "AI intended to be used for making decisions on hiring, promotion, or termination of employment or work-related contractual relationships."

Data attributes

Another concern is the requirement that data sets used to train the AI and operate it be error-free or complete. Put simply, this is an impossible standard to meet: any data set will have some errors. Furthermore, error-free datasets are not necessary to preserve individuals' fundamental rights. Instead, what is necessary is that the data sets be fit for purpose. That is, any incompleteness or errors don't impact materially how the AI affects individuals' rights or make it less accurate than needed for the purpose for which the AI is used.

Similarly, the AI Act imposes several requirements around accuracy of the AI system. The requirements around documentation and transparency make sense and are aligned with advanced AI ethics and compliance programs, such as the program that Workday operates. However, the standard for assessing accuracy is not set out. This may be due to different standard requirements by AI application. We understand that the Commission plans for sector-specific standards to define detailed system requirements. However, as noted above, those standards won't be in place before the AI Act comes into effect, leaving businesses with uncertainty about their obligations and how to comply.

Our recommendation is that the definition of AI be limited to ML-based systems (see above) and that the Commission should specify reasonable, quantitative requirements for accuracy metrics that can be demonstrated at the time of model build, such as recall and precision requirements. Such standards should be determined based on consultation with data scientists and should avoid recommendations that would lead to over-fitting—that is, where the machine learning model fits exactly against the training data and as such is less likely to generalize to outside datasets. The Act should include a statement on the benefits associated with balancing accuracy and fairness at the time of model build, noting that developers may optimize for both types of metrics depending on the availability of demographic data and the fairness metrics and standards that are most relevant locally. With specific guidance such as this, on how to comply with accuracy requirements at the time the Act is adopted, the Commission may also leave room for standards developments around best practices which may emerge over time from external bodies.

As argued above, the enforcement and regulatory structure for the Act should shift slightly away from a product safety structure to an ethical or trustworthy AI structure, at least for standalone systems. As such, requirements should be focused mainly on transparency as to how the system was built and what it was designed to do, as well as appropriate and complete documentation of such. A stricter focus on these types of requirements, and associated enforcement, are needed and would be welcomed by ethical corporate actors.

For this reason, and assuming that more specific guidance will be given regarding the definition of accuracy and other changes as suggested here, Workday is supportive of the requirements included in Article 13, *Transparency and provision of information to users*, as well as Article 11, *Technical Documentation* to support and facilitate that transparency. As developers of AI systems, we see it as one of our core responsibilities to provide deployers with as much information as possible regarding how the AI systems are developed and how they work, so that the deployers (our enterprise customers) can trust and feel comfortable and confident to use the AI systems. The information required in the Technical

Documentation, as described in Annex IV, is quite detailed and thorough, and should provide deployers and regulators with more than enough information to understand the system and determine whether it is trustworthy, as well as whether the system complies with the regulation.

Data access

Workday strongly advises against the requirements to provide Market Surveillance Authorities with source code and APIs to training and testing data, as described in Article 64. Access to this type of information introduces significant data protection and trade secrets risks and should not be necessary to evaluate how a system works. Disclosures about the nature and types of data used to train the system should be more than sufficient for an evaluation of whether an AI system met the obligations under the Act with respect to its development. Further, the technical requirements and expertise needed to securely store, review, and understand the data and source code would likely outstrip the capacity of authorities, given the number of AI systems falling under their purview. Furthermore, as described above, certain developers of AI systems will be unable to provide APIs to training and testing data, where that data is owned and controlled by deployers. In addition, the market withdrawal procedures as currently drafted could pose issues of breach of contract and interference with customers' business operations, particularly for software-as-a-service applications that are provisioned continuously through the cloud, and are unnecessary to safeguard users' rights.

Instead, required transparency to deployers and users, along with technical documentation of such, should more than suffice in the context of an ethical/trustworthy AI regulation. These types of requirements, along with specific guidelines regarding measures and metrics, will positively impact the AI market and will be welcomed by companies wishing to provide trustworthy, ethical, and quality products and services to customers and to the public. This type of focus may have the added benefit of introducing competition in the AI market in the direction of ethical and trustworthy AI.

Transition period

Finally, a brief note about the transition period. The AI Act takes effect three months after adoption. Given that it is such a significant piece of legislation, imposing new regulatory requirements across the use of AI and ML across industry sectors, a longer transition period of up to a year should be provided.