Workday

SEC Risks
vs
Public-Facing Marketing

Integration Partners

Workday's public ecosystem and marketing materials do **acknowledge certain third-party integrations** like Lightcast and HireVue, though not always explicitly by name in all contexts. For example, Workday's certified integration with **Lightcast (formerly EMSI/Burning Glass)** is highlighted in partner channels. A Lightcast announcement notes *"Lightcast's integration with Workday HCM…offers customers seamless access to comprehensive talent insights"*, enriching Workday's Skills Cloud with global labor market data (hrtechedge.com). Lightcast emphasizes that *"Workday customers [can] harness comprehensive talent insights from Lightcast more easily"* through this integration, gaining *"real-time data on over 1,900 occupations, 33,000 skills, and 75,000 job titles worldwide"* to **enhance job profiles and talent strategies (**linkedin.com). This indicates Workday's platform can directly ingest Lightcast's labor market datasets for skills inference and benchmarking.[1,2,3]

Similarly, **HireVue** – a video interviewing and assessment provider – is an official Workday integration partner. Workday's Marketplace listing (and HireVue's own materials) describe a *"HireVue for Workday"* module that **embeds on-demand video interviews and AI-driven assessments into Workday Recruiting workflows (**hirevue.com). HireVue touts that recruiters can *"enable assessments with one click inside Workday – all within a single hiring workflow,"* eliminating manual resume screens (hirevue.com). HireVue also notes it uses Workday's APIs natively, implying a close technical alignment (hirevue.com). In other words, Workday recognizes HireVue as a plug-in service to streamline recruiting, even if these mentions appear primarily in partner catalogs and solution briefs rather than Workday's own press releases.[4,5,6]

[1] Cvetkoska, V., Trpeski, P., Ivanovski, I., Peovski, F., İmrol, M., H., Babadoğan, B., Ecer, H., Görür, D., Z., Selvi, U., Hunde, A., B., Gemeda, F., T., Dubi, Y., B., Melnyk, S., Lytvynchuk, A., Tereshchenko, H. (2025) Comparative Analysis of Skill Shortages, Skill Mismatches, and the Threats of Migration in Labor Markets: A Sectoral Approach in North Macedonia, Türkiye, Ethiopia, and Ukraine *Social Sciences*
[2] Lakhamraju, M., V. (2025) The strategic role of workday payroll in addressing enterprise challenges *Computer Science and Engineering Research*
[3] Pandey, S. (2022) Advanced Integration of ATS and HCM Systems: Leveraging SaaS-Driven Recruitment Analytics for Optimizing Strategies through Greenhouse BIC and Workday Prism *Journal of Engineering and Applied Sciences Technology*
[4] Kazim, E., Koshiyama, A., Hilliard, A., Polle, R. (2021) Systematizing Audit in Algorithmic Recruitment *Journal of Intelligence 9*
[5] Chiang, J., Berkoff, R. (2017) How are Pre-Hire Assessments Contributing to Unbiased and More Targeted, Successful Hires?
[6] Zhou, F. (2024) AI System Report: Hirevue's AI-Driven Assessment Tool *Innovation in Science and Technology*

In contrast, **People Data Labs (PDL)** – a broker of personal and professional data – is *not prominently advertised* by Workday in public-facing content. There is no readily found Workday Marketplace app or press release for PDL. **However, external analyses strongly suggest** that Workday's talent intelligence features draw on data from brokers like PDL behind the scenes. For instance, an industry investigation reported that *"data is routinely shared between brokers like Lightcast.io, People Data Labs, Acxiom, and platforms like Workday...to construct AI-based hiring decisions without notification"* to users. Workday's **Skills Cloud and AI recruiting models** are said to integrate such third-party data feeds to build "dynamic profiles" of candidates. *Workday itself does not explicitly name People Data Labs* on its website or marketing brochures – instead it might generically reference use of "public professional data" or "third-party sources" when describing these features. This stands out as a notable omission given that PDL's massive dataset (e.g. hundreds of millions of scraped personal profiles) could be powering Workday's AI-driven skill inferences and candidate scoring. In summary, **Workday openly promotes certain partner integrations (like Lightcast, HireVue)** as value-adds for customers, but **other data services like PDL remain unmentioned by name**, even if they play a role in Workday's products.

SEC Filing Gaps

SEC Risk Disclosure (10-K)	Public-Facing Statements (Website/Blog)
10-K Risk Factor: **Warns that integrating AI into Workday's products "can present new risks and challenges" including a "quickly evolving legal and regulatory environment" around ethical issues. Notes that many Workday AI use cases "could potentially impact human, civil, privacy, or employment rights and dignities," and that failure to address ethical and social issues or misuse of AI could lead to reputational harm, regulatory action, or litigation. Indeed, Workday discloses it** *"already [is] defending against a lawsuit alleging that our products and services enable discrimination,"* **acknowledging that even if meritless, such claims can be disruptive and damage its brand.**	*Marketing & Blogs*: Emphasize **"ethical AI"** and trust. Workday touts a *"robust responsible AI program"* with governance measures: a Responsible AI Advisory Board (led by the General Counsel and including the Chief Compliance and Diversity Officers), an independent AI ethics team, strict AI design guidelines (extra review for high-risk uses like hiring), and transparency/disclosure to customers about AI use. In public blog posts, Workday officials stress they *"act responsibly and ethically in [the] design and delivery of AI solutions to support equitable recommendations,"* with *human-in-the-loop* oversight and bias mitigation strategies in place. One Workday article even states that *"some risks should be deemed unacceptable from the start, such as the presence of bias or discrimination in AI models that could lead to unfair or discriminatory outcomes"*, underscoring a zero-tolerance message for AI bias.[1]

[1] *Source:* Workday smart CIO blog, *"How Companies Can Thrive With Trusted AI."* (Workday Blog, 2023).

Workday's **SEC filings (e.g. annual 10-K reports)** discuss third-party data and partnerships only **in broad, generic terms**, with **no specific mention** of Lightcast, HireVue, People Data Labs, or similar vendors. In its business overview and risk factors, Workday acknowledges

that its **growth and products depend on third-party technologies and content** – but these entities are described abstractly. For example, the 10-K states: *"We depend on relationships with third parties such as … technology and content providers … and are also dependent on third parties for the license of certain software and development tools that are incorporated into or used with our applications."*(sec.gov). This **"technology and content providers"** category presumably **includes data brokers and AI services**, yet **no individual partner is named**. The filing warns generally that if any of those third-party providers fail, or if partnerships aren't maintained, Workday's operations and ability to deliver features could suffer (sec.gov) (sec.gov). Workday also notes the need to integrate with third-party software and that undetected defects in such external software could impair its platform (sec.gov). Again, this is framed in general "third-party" language.[7,8,9]

Notably, **nowhere in recent SEC filings do the names Lightcast, HireVue, or People Data Labs appear**. A search of Workday's 2023 and 2024 10-Ks yields no direct references to these companies. Instead, Workday uses umbrella terms like *"third-party data"* or *"strategic relationships with third parties"*. For instance, in describing its Planning application, the 10-K says Workday's tools can *"incorporate historical and third-party data, like economic data and labor statistics,"* for forecasting (sec.gov). This implies external data feeds (e.g. labor market info such as Lightcast provides) without naming the source. In risk factors, Workday mentions *"our ability to establish or maintain strategic relationships with third parties"* and to integrate with third-party technologies as a key uncertainty (sec.gov). It also discloses reliance on cloud hosting partners like AWS and others for infrastructure (sec.gov) – one of the few times specific third parties (Amazon, Google, Microsoft) are named in filings, likely because those are material to operations. By contrast, **data/AI partners are not individually identified as material risks** – suggesting Workday either does not consider any single data partner to rise to the level of requiring disclosure, or it prefers to group them into a generic risk category.

This gap between **public partner naming vs. SEC disclosure** means that an investor reading Workday's annual report would only learn that Workday uses unnamed "content providers" and licensed data/software from third parties (sec.gov). They would not see that Lightcast's labor market taxonomy or PDL's people data are part of Workday's product capabilities. Such information is only found in marketing collateral or partner press

[7] Ethirajulu, B. (2023) Enhancing digital experiences in banking imperative: A study *International Journal of Multidisciplinary Research and Growth Evaluation*

[8] Jackson, D., A., Ferns, S., Rowbottom, D., Mclaren, D. (2017) Improving the work-integrated learning experience through a third-party advisory service *International Journal of Training Research 15*, 160-178

[9] Sharma, M. (2024) Empowering Innovation with Workday AI: Building Intelligent Applications for the Future of Work *International Journal For Multidisciplinary Research*

releases, not in the SEC-filed description of the business. In essence, **Workday's SEC filings treat these integrations as part of the background fabric** (covered by general statements on third-party reliance), **without detailed discussion** of the nature of the data being integrated or potential issues it might introduce (e.g. data accuracy or bias). When describing AI features in regulatory filings, Workday speaks generally about using *"large data sets"* and notes broad ethical considerations (like AI ethics, privacy, anti-bias laws)([sec.gov](sec.gov)) ([sec.gov](sec.gov)), but stops short of detailing which external data sources fuel those AI models.[10,11]

SEC Filing Excerpt (10-K example): *"Our growth depends on the success of our strategic relationships with third parties as well as our ability to successfully integrate our applications with a variety of third-party technologies. We depend on relationships with third parties such as ... technology and content providers... If we are unsuccessful in establishing or maintaining our relationships with these third parties...our ability to compete in the marketplace or to grow our revenues could be impaired."(*[sec.gov](sec.gov)) ([sec.gov](sec.gov))

In summary, **Workday's investor filings provide only generalized acknowledgement** of third-party data/services, **unlike the more explicit partner names found in marketplace listings and press releases.** The role of companies like Lightcast, HireVue, and PDL in Workday's offerings is only **implicitly covered** under broad terms ("content providers", "third-party data") in SEC reports, which may gloss over the specifics of how external data streams drive Workday's AI and analytics capabilities.

Risk & Harm Analysis

Integrating third-party data brokers and AI services into HR workflows brings significant **algorithmic bias, privacy, and discrimination risks** – concerns that have been documented by researchers and even reflected in legal action against Workday. **One major harm is the potential for algorithmic bias and unjustified candidate filtering**. Data brokers like Lightcast and People Data Labs aggregate enormous quantities of personal data (résumé details, online profiles, demographic indicators, etc.) from the web, often **without the subjects' explicit consent (**linkedin.com**)**. These data are used to train machine

---

[10] (2022) [Budgetierung in Organisationen – heftig umstritten und heiß geliebt für das Masterseminar im Wintersemester 2022/2023 Better budgeting or beyond budgeting? In: Measuring Business Vol. No. pp.](#)
[11] Chukwuma-Eke, E., C., Ogunsola, O., Y., Isibor, N., J. (2023) [A Conceptual Framework for Ensuring Financial Transparency in Joint Venture Operations in the Energy Sector](#) *International Journal of Management and Organizational Research*

learning models that power tools such as Workday's Skills Cloud and recruiting analytics. **Bias can creep in at multiple stages**:

- **Skewed or Incomplete Data**: As reported in a Harvard Business Review study and other research, automated hiring filters often rely on "shadow profiles" or inferred attributes. If the underlying data from brokers is **inaccurate, outdated, or demographically skewed**, qualified candidates can be erroneously screened out. Indeed, a 2022 study estimated *over **27 million** qualified U.S. job seekers are filtered out by algorithmic hiring systems* – frequently due to inaccurate or proxy data that doesn't reflect their true fit. The **lack of data transparency** means candidates often don't even know why they were rejected.[12,13]

- **Embedded Social Biases**: Workday's AI tools, by the company's own admission, can analyze *"625 billion data points"* including job histories and "adjacent skills" to predict candidate success. If these data points reflect historical biases (e.g. certain roles historically filled by one gender or ethnic group), the AI may **perpetuate or even amplify those biases**. A 2023 Center for Democracy & Technology paper found that **Black, disabled, formerly incarcerated, and neurodivergent candidates** are disproportionately harmed by such data-driven screening. In Workday's case, a class-action lawsuit (Mobley v. Workday) alleges that its AI-powered screening system systematically **discriminated against Black, older, and disabled applicants**, by using algorithms that replicatively favor profiles similar to a company's existing (potentially homogeneous) workforce (reuters.com) (reuters.com). The suit claims Workday's models were trained on customers' current employee data without proper adjustments, thus **reinforcing existing discrimination** in hiring outcomes (reuters.com). This highlights how third-party data and AI can introduce **proxy discrimination** – for example, seemingly neutral attributes or "skill gaps" inferred from data may correlate with race, age, or disability, resulting in **disparate impact**.[14,15,16]

- **Privacy Violations & "Shadow Profiles"**: Services like People Data Labs compile profiles from many sources (social media, resumes, public records) and sell them as enrichment data. When Workday or its partners incorporate these data, candidates

[12] Daltayanni, M. (2015) Reputation Systems in Labor and Advertising Marketplaces - eScholarship

[13] Daltayanni, M. (2015) Reputation Systems in Labor and Advertising Marketplaces , 1-80

[14] Poe, R., L., Mestari, S., Z., E. (2024) The Conflict Between Algorithmic Fairness and Non-Discrimination: An Analysis of Fair Automated Hiring *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*

[15] Nandal, A., Yadav, V. (2025) Ethical Challenges and Bias in AI Decision-Making Systems *Journal of Science & Technology*

[16] Jenks, C., J. (2024) Communicating the cultural other: trust and bias in generative AI and large language models *Applied Linguistics Review 16*, 787-795

may be **assessed on information they never provided to the employer** – e.g. a side project from GitHub, or an old social media post. This happens **without the candidate's knowledge or consent (**linkedin.com**)**. From a privacy standpoint, this is troubling: individuals cannot easily opt out or correct errors in these brokered datasets. As one analysis put it, *"platforms like Workday [use brokered data] to construct AI-based hiring decisions **without notification or transparency to the job seeker**"* (linkedin.com). This lack of transparency means **candidates are unaware that a "shadow profile" may be influencing their job prospects,** and they have no opportunity to contest or update that data. Such practices can run afoul of data protection principles. Under laws like GDPR or CCPA, individuals have rights to access and correct data – but those rights are hard to exercise when neither the employer nor Workday directly collects the data (it comes via third parties) and when candidates aren't even aware it's being used (linkedin.com). This creates an **accountability gap**: employers might claim they simply licensed data and algorithms from Workday, while Workday might argue it's the employers who decide how to use them, leaving candidates in a limbo when seeking recourse (linkedin.com).[17,18,19]

- **Ethical and Psychological Impacts**: The use of AI recommendations based on big data can lead to **self-fulfilling feedback loops**. For example, if an algorithm – fed by Lightcast's predictive analytics – concludes a candidate lacks "career stability" because of an inferred pattern in their employment history, that candidate could be auto-rejected from dozens of jobs without any human review. This not only harms the individual's opportunities but also **bypasses the human-centric nuance that hiring decisions ideally require**. There are concerns about **"shadow profiling"** where candidates are evaluated on factors they never knew were in play – effectively a form of **automated reputation scoring** that can be both inaccurate and discriminatory. From an ethical standpoint, this raises questions of fairness and consent: is it fair to eliminate someone based on an AI's prediction of "cultural fit" or inferred skill, especially if those inferences come from tenuously related data? Many argue it is not,

---

[17] Alakbarzadeh, V. (2025) Beynəlxalq hüquq kontekstində süni intellekt - insan hüquqları və hüquqi hesabatlılıq çağırışları *Azerbaijan Law Journal*

[18] Ramokapane, K., Bird, C., Rashid, A., Chitchyan, R. (2022) Privacy Design Strategies for Home Energy Management Systems (HEMS) *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*

[19] Kollnig, K., Shuba, A., Kleek, M., V., Binns, R., Shadbolt, N. (2022) Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*

and that it may entrench systemic biases under the guise of objective data-driven decision-making (linkedin.com).

Importantly, **Workday appears cognizant of these risks**, at least to some extent, and has taken steps in product development and partnership oversight to mitigate them (described more below in *Transparency Assessment*). The company's marketing to customers emphasizes that its AI integrations are **audited for bias and designed for fairness**. For instance, Workday's partner HiredScore (another AI recruiting tool integrated with Workday) advertises *"intuitive bias audits"* and **explainable AI outputs** that accompany its scoring of candidates (suretysystems.com).

HiredScore's Workday datasheet claims the AI was tested to ensure *fair outcomes across gender and ethnic groups*, using an explainable A–D grading system for candidates rather than opaque scores (workday.com). This suggests Workday and its partners **recognize the bias issue and are marketing their solutions as bias-mitigating** ("designed with candidate and employee privacy in mind" in HiredScore's case (suretysystems.com). [20]

Regulatory Compliance (GDPR, CCPA, CPRA, global privacy laws

SEC Risk Disclosure (10-K)	Public-Facing Statements
10-K Risk Factor: Emphasizes that the global privacy landscape is "increasingly complex, fragmented, and financially relevant." Workday warns of "increased regulatory compliance costs, government enforcement actions... and reputational harm" due to expanding privacy laws. It cites the EU's GDPR (effective 2018) as a standard with harsh penalties (up to 4% of global revenue) and notes that failure to comply – by Workday or its subprocessors – could lead to fines, lawsuits, and loss of customers. Workday acknowledges new laws (e.g. Russia/China data localization, U.S. state laws, and the California CCPA/CPRA effective 2020/2023) that create a "patchwork" of requirements, increasing compliance challenges. Uncertainty around mechanisms like the EU–US Data Privacy Framework is also noted. Overall, the filing makes clear that ever-changing privacy laws could force Workday to modify services, limit data use, incur heavy costs, slow sales, or even stop serving certain markets. It also flags that even the *perception* of privacy issues can damage customer trust.	*Website/Blog Claims*: Emphasize **trust, compliance, and proactive privacy protection**. A Workday blog by the Chief Privacy Officer proclaims Workday is *"committed to safeguarding global privacy by anticipating regulatory changes and supporting customers with compliance across diverse privacy laws worldwide."*. The company highlights a *"proactive approach"* – including a dedicated privacy team, ongoing employee privacy training, and integration of privacy principles (and even AI ethics principles) into its products and practices. On its Trust Center pages, Workday assures customers that "Workday manages data privacy and supports compliance" for global laws. Marketing materials stress that Workday provides the tools and encryption needed to keep data secure and meet regulations: *"Workday... gives you the foundation you need to maintain human resource compliance,"* whether GDPR, U.S. laws, or future rules. In short, public content focuses on how Workday *enables* compliance and protects data, rather than on the risk of non-compliance.
10-K Risk Disclosure: Implies that operating globally entails compliance risks with labor and employment laws. In the	*Public-Facing (Products & Values)*: On its website, Workday assures global companies that its software helps them **comply with labor**

[20] Cocheo, S. (2000) Public Thoughts on Privacy from Minnesota's Attorney General *ABA Banking Journal 92,* 24

context of international expansion, Workday notes challenges of "adhering to local laws and regulations" including employment laws, and the complexity of **"multiple, conflicting, and changing"** regulations across jurisdictions. It also emphasizes that increased compliance requirements (such as ESG or local labor rules) can raise costs or liability. While not a standalone risk factor, it's clear that failing to **comply with** global employment regulations **or adapting HR practices per local law could expose Workday to legal and financial risk.**	**regulations**. For example, Workday's HCM marketing notes: *"Whether you're faced with GDPR, ACA, OFCCP, [or other] regulations, Workday gives you the foundation you need to maintain human resource compliance."* This suggests Workday's tools are built to handle diverse legal requirements (ACA and OFCCP relate to U.S. employment laws on healthcare and federal contractor nondiscrimination). In terms of corporate stance, Workday's Ethics page states: *"Workday is committed to following all applicable global regulations,"* explicitly including labor standards, anti-corruption laws, etc.. Publicly, Workday positions itself as a law-abiding, ethical employer and vendor. Any difficulties in compliance are not front-and-center in marketing; instead, the message is that Workday **simplifies** compliance for everyone..

Additionally, Workday's **security and compliance documents** likely impose that data from brokers is used in compliance with privacy laws – for example, by requiring that any personal data usage via Workday's platform be disclosed by the customer to end-users as appropriate.[21,22,23]

Nonetheless, the potential for **algorithmic harm remains a serious concern**. Regulators have taken notice: the U.S. Equal Employment Opportunity Commission (EEOC) has warned that employers (and by extension, vendors like Workday) can be held liable if their AI screening tools result in discriminatory impact (reuters.com). The fact that **Workday is now facing a class-action lawsuit over AI bias** underscores the real-world implications of these third-party data integrations. Harms like **systemic exclusion of certain groups, privacy invasions, and erosion of candidate trust** are not just hypothetical – they are being alleged in court and studied by experts. In sum, while Workday's incorporation of Lightcast, PDL, and similar data promises more "data-driven" HR decisions, it also **imports the biases and inaccuracies of that data**, raising significant **ethical and legal challenges**. The onus is on Workday and its customers to ensure these tools are used in a way that **complies with anti-**

[21] Amin, M., A., Tummala, H., Shah, R., Ray, I. (2024) Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing , 211-223

[22] Sharma, M. (2024) Security and Compliance in Cloud ERP Systems: A Deep Dive into Workday's Framework *International Scientific Journal of Engineering and Management*

[23] Naik, S. (2023) Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy *The Eastasouth Journal of Information System and Computer Science*

discrimination laws and privacy regulations, and that **appropriate bias testing, disclosures, and overrides** are in place to prevent adverse impacts.[24,25,26]

Transparency Assessment

There is a clear **discrepancy between Workday's public-facing promotions of these integrations and the transparency actually afforded to stakeholders (customers, regulators, job candidates) about their use and risks.** On one hand, Workday's marketing and **product materials trumpet the capabilities** gained from partners: for example, showcasing how Lightcast data gives **"market-validated" skills insights** or how HireVue provides **seamless automated screening**. These descriptions, however, tend to gloss over or **omit the potential downsides**. Nowhere in a glossy brochure does Workday warn a customer, "By the way, the labor data we pull in from Lightcast was scraped from the web without those individuals' consent," or "These AI rankings might inadvertently screen out qualified minority candidates." The **tone of customer-facing content is overwhelmingly positive**, focusing on efficiency and intelligence gains, with only minimal allusion to safeguards.[27,28,29]

By comparison, Workday's **SEC filings and legal disclosures use careful, vague language** that arguably sacrifices clarity for liability management. Referring to key data sources only as *"third-party content providers"* (with no specific mention of how their data is obtained or used) can be seen as **lack of transparency**. While understandable from a materiality and concision standpoint in SEC documents, this approach means an informed outsider must connect the dots to realize that "third-party content" covers everything from labor market taxonomies to massive personal data warehouses. **There is no explicit acknowledgement**

[24] Pandey, H., S., K., Kumar, N. (2025) ETHICAL CHALLENGES IN AI USE IN SCHOOLS: A STUDY OF DATA PRIVACY, SURVEILLANCE, AND BIAS *EPRA International Journal of Multidisciplinary Research (IJMR)*

[25] Sacramed, M., T. (2024) Reviewing the Philippines Legal Landscape of Artificial Intelligence (AI) in Business: Addressing Bias, Explainability, and Algorithmic Accountability *International Journal of Research and Innovation in Social Science*

[26] Qureshi, N., I., Choudhuri, S., S., Nagamani, Y., Varma, R., Shah, R. (2024) Ethical Considerations of AI in Financial Services: Privacy, Bias, and Algorithmic Transparency *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS) 1*, 1-6

[27] D'Souza, R., F., Mathew, M., Mishra, V., Surapaneni, K., M. (2024) Twelve tips for addressing ethical concerns in the implementation of artificial intelligence in medical education *Medical Education Online 29*

[28] Albalawi, A., F., Yassen, M., H., Almuraydhi, K., M., Althobaiti, A., D., Alzahrani, H., Alqahtani, K., M. (2024) Ethical Obligations and Patient Consent in the Integration of Artificial Intelligence in Clinical Decision-Making *JOURNAL OF HEALTHCARE SCIENCES*

[29] Qureshi, N., I., Choudhuri, S., S., Nagamani, Y., Varma, R., Shah, R. (2024) Ethical Considerations of AI in Financial Services: Privacy, Bias, and Algorithmic Transparency *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS) 1*, 1-6

in investor filings of the *nature* of data being ingested (e.g. personal profile data, public social media scraping), nor of the specific **ethical risks** that accompany it. The filings do acknowledge *"AI ethics and machine learning"* as areas of regulatory concern broadly (sec.gov) and even note that failing to address *"ethical and social issues"* in AI use cases could harm the business (sec.gov). However, these statements remain **abstract**. They don't inform the reader that Workday's AI might be making hiring recommendations based on algorithmic inferences from third-party data. In short, **the SEC disclosures are technically truthful but not richly informative** about these integrations.

Workday's 10-K and other SEC filings do flag "AI ethics and machine learning" as an area of regulatory and reputational risk, but they never go so far as to say, for example, "We ingest public social-media profiles, résumé databases and data-broker feeds (e.g. People Data Labs) to generate automated hiring recommendations." In other words, the risk disclosures are accurate but highly generic—they warn investors that third-party content could expose the company to bias or privacy claims, without spelling out the precise data flows or the associated ethics challenges.

Why this matters:

1. Lack of granularity leaves job-seekers—and even investors—in the dark about how decisions are actually made. When you read that Workday "relies on third-party data," you don't know whether that's labor-market salary surveys, scraped LinkedIn profiles, or a commercial data broker selling inferred attributes (gender, education level, socioeconomic status, etc.).
2. Abstract risk language gives the firm legal cover but does little to build trust. By couching everything in boilerplate about "regulatory changes" or "ethical and social issues," Workday complies with SEC requirements yet sidesteps real transparency.
3. Without naming partners or data types, it's impossible to evaluate how serious algorithmic-bias or privacy risks really are—and whether the company's mitigation measures are sufficient.

By moving from abstract references to specific disclosures about the kinds of data used, the partners involved, and the concrete steps taken to manage ethical risk, Workday would not only strengthen its compliance posture but also deepen investor and user trust—making its public statements as informative as its marketing claims are enthusiastic.

From a **customer transparency and trust** perspective, Workday does make some efforts to address concerns but primarily **aimed at its direct clients (employers)** rather than end-users (job seekers or employees in the system). Workday has published Responsible AI principles and even *bias testing results for certain AI features* in collaboration with partners. For example, Workday's documentation on the HiredScore integration highlights that the

AI's outputs are explainable and that the tool was tested for equal effectiveness across different demographic groups (workday.com).

Workday's **Chief Privacy and AI officers have blogged** about *"Safeguarding Privacy while Innovating with AI"* and *"Continued Diligence to Ethical AI and ML Trust,"* indicating the company is publicly positioning itself as mindful of these issues (congress.gov) (congress.gov). In an official comment to regulators, Workday outlined a *Responsible AI program* with an advisory board, independent AI ethics team, bias review processes, and customer disclosures (congress.gov) (congress.gov). Notably, Workday says it provides **"disclosure to equip our customers with a clear understanding of how our AI tools are developed and assessed,"** and even gives customers *"the means to access their own data for bias testing and the choice of whether to use an AI tool at all."* (congress.gov). This indicates that **Workday at least strives for transparency with its enterprise clients**, allowing them to see under the hood to some degree and opt out if desired. Indeed, Workday emphasizes that any AI used for consequential decisions (like hiring) is treated as high-risk internally and subject to extra scrutiny (congress.gov).[30],[31],[32]

However, there remains a **transparency gap when it comes to job candidates and employees affected by these tools**. Workday's disclosures to its **enterprise customers** do not automatically translate into transparency for individual end-users. For instance, if a candidate is rejected due to a Workday/Lightcast-derived "fit score," Workday's obligations for bias testing and disclosure are to its paying client (the employer). The candidate **may receive no explanation** that *data from a third-party broker and an AI model were behind the decision*. This opacity undermines user trust: individuals cannot easily trust a system that aggregates data about them from unknown sources and makes unseen evaluations. The **vague references in Workday's public statements** – e.g. saying AI will "unlock human potential" while recognizing risks generally – do little to enlighten the average user about what's really happening behind the scenes.[33],[34],[35]

---

[30] Leta, F., M., Vancea, D. (2023) Ethics in Education: Exploring the Ethical Implications of Artificial Intelligence Implementation *Ovidius University Annals. Economic Sciences Series*

[31] Mehmet, A. (2024) THE ETHICS OF ARTIFICIAL INTELLIGENCE IN EDUCATION: CHALLENGES AND OPPORTUNITIES *Bulletin of Zhetysu University named after I.Zhansugurov*

[32] Kumar, C. (2025) From Automation to Ethics: Responsible AI in Human Resource Management across Industries with Insights from the Power Sector *RESEARCH REVIEW International Journal of Multidisciplinary*

[33] Henry, J., Obaid, H. (0) Demystifying Explainable Artificial Intelligence: a Comprehensive Guide

[34] Falvo, F., R., Cannataro, M. (2024) Ethics of Artificial Intelligence: challenges, opportunities and future prospects *2024 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 5860-5867

[35] Adeniran, A., A., Peace, A., William, P. (2024) Explainable AI (XAI) in healthcare: Enhancing trust and transparency in critical decision-making *World Journal of Advanced Research and Reviews*

In terms of **legal compliance**, these discrepancies could be significant. Regulators are increasingly pressing for *algorithmic transparency and accountability*. If Workday markets its AI as fair and responsible but does not clearly communicate the involvement of data brokers and the steps taken to mitigate their risks, it could invite regulatory scrutiny. For example, the EU's draft AI Act would likely classify an AI used in hiring as "high-risk," requiring detailed documentation of training data provenance, bias mitigation, and even registration in an EU database. If Workday or its clients were asked to produce such documentation, they would need to be far more explicit about integration with firms like People Data Labs and Lightcast than they are in public brochures. **Omissions or euphemisms** ("third-party data sources") might not satisfy regulators' demand for transparency about **where training data comes from and how algorithms are tested for fairness**.[36,37,38]

From a **user trust** standpoint, the incomplete narrative can also backfire. Savvy customers and activists do notice the omissions. The very question we're exploring suggests a skepticism: why doesn't Workday openly list People Data Labs as a partner, given its likely role? This could lead one to suspect that either Workday doesn't want to draw attention to the **origins of its AI's data** (perhaps because scraping-based data brokers carry a whiff of privacy invasiveness or legal risk), or that the integration is unofficial. **Either case can erode trust**. If the data is being used, users and regulators expect candor about it; if it's not "official" enough to mention, why is it in the product? There's a fine line between simplifying marketing messages and **obfuscating key details**. Workday's public content tends to celebrate the benefits of AI and big data, while its SEC filings and legal pages hedge with general risk factors – leaving a gray area where specifics are hard to find.[39,40,41]

In conclusion, **Workday's handling of these third-party data partnerships reveals a transparency tension**. The company is eager to leverage and advertise the *power* that Lightcast and others bring to its platform (to remain competitive in the skills-based HR tech

[36] Katoch, N. (2025) Addressing Bias in AI: Ethical Concerns, Challenges, and Mitigation Strategies *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*

[37] Samala, A., Rawas, S. (2025) Bias in artificial intelligence: smart solutions for detection, mitigation, and ethical strategies in real-world applications *IAES International Journal of Artificial Intelligence (IJ-AI)*

[38] Bahangulu, J., K., Owusu-Berko, L. (2025) Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency and compliance in AI-powered business analytics applications *World Journal of Advanced Research and Reviews*

[39] Cosmin-Iulian, I., Adrian, I. (2024) Decentralized Infrastructure for Digital Notarizing, Signing, and Sharing Documents Securely Using Microservices and Blockchain *IEEE Access 12*, 195816-195829

[40] Manjunath, P., Herrmann, M., Sen, H. (2019) Implementation of Blockchain Data Obfuscation *Innovation in Medicine and Healthcare Systems, and Multimedia*

[41] Mitrea, D., Cioara, T., Anghel, I. (2023) Privacy-Preserving Computation for Peer-to-Peer Energy Trading on a Public Blockchain *Sensors (Basel, Switzerland) 23*

market), but it is *cautious* about publicly associating too closely with "data brokers" that might raise eyebrows. The result is that **marketing materials are upbeat but often vague, and SEC filings are detailed about generic risks but silent on specific players**. This can lead to **omissions and euphemisms that obscure the full picture**. For stakeholders who dig deeper, this discrepancy might signal a need for more forthright disclosure. Bridging this gap – through clearer communication about how third-party data is used and governed – would likely improve **Workday's transparency, legal positioning, and user trust**. As AI regulations tighten and public awareness of data ethics grows, Workday may be compelled to be more explicit about partnerships like Lightcast and People Data Labs in both customer-facing and official disclosures, ensuring that the **promise of AI-driven innovation doesn't outpace the commitment to fairness and accountability**.[42,43,44]

[42] Żywiołek, J. (2024) Building Trust in AI-Human Partnerships: Exploring Preferences and Influences in the Manufacturing Industry *Management Systems in Production Engineering 32*, 244-251

[43] Wang, J., Cao, Q., Zhu, X. (2024) Privacy disclosure on social media: the role of platform features, group effects, trust and privacy concern *Library Hi Tech*

[44] Goldshtein, M., Chiou, E., K., Roscoe, R., D. (2024) 'I Just Don't Trust Them': Reasons for Distrust and Non-Disclosure in Demographic Questionnaires for Individuals in STEM *Societies*