VORYS

New thinking. Since 1909.

VORYS

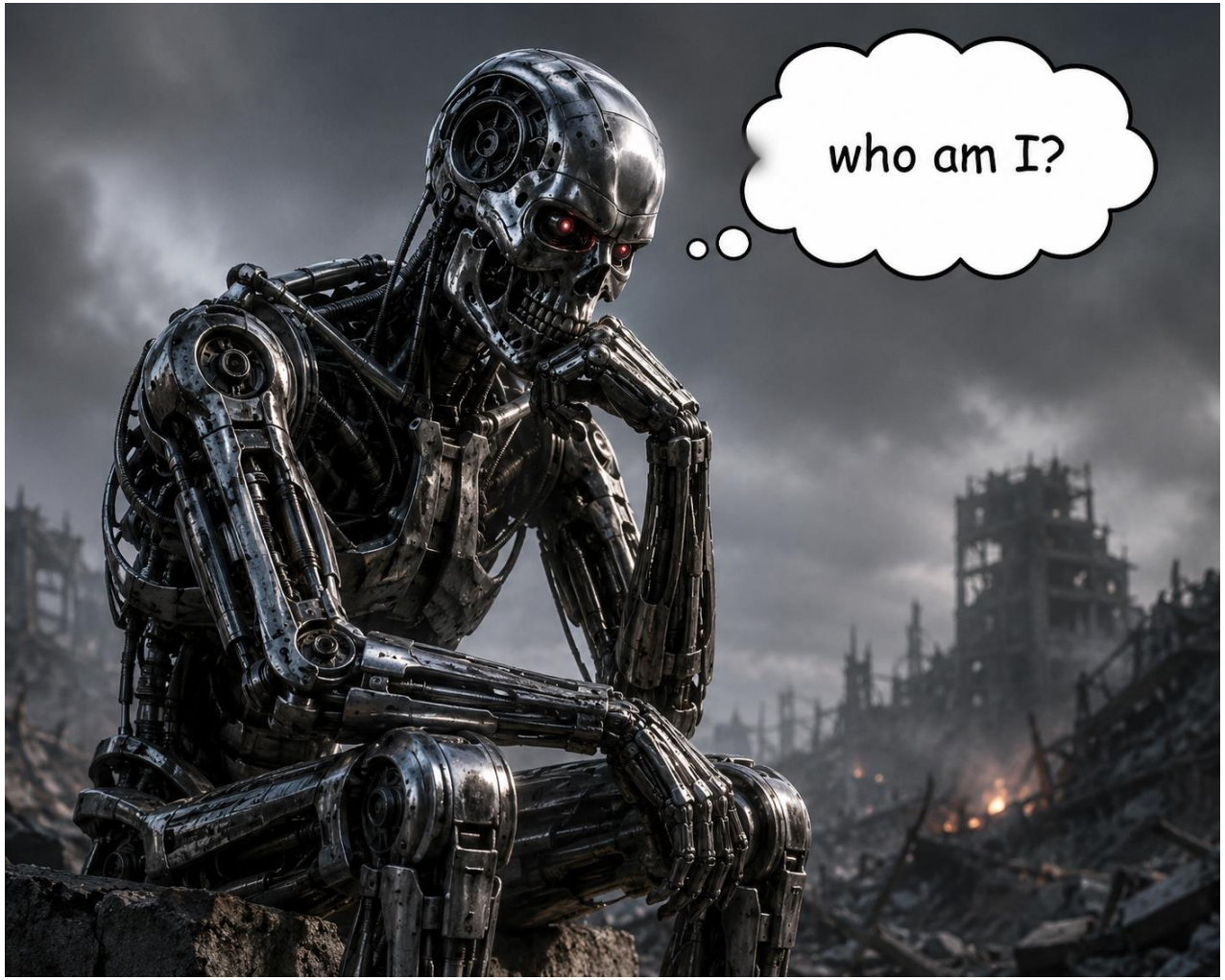
New thinking.
Since 1909.

HR Data Audits & AI Compliance: Managing Employee Data, Vendor Risks and Legal Exposure

Agenda

- What is AI?
- AI risks in the workplace
- AI vendor onboarding
- New AI liability
- AI controls and governance
- Next steps

What is AI?



Basics of AI

AI refers to computer systems that **perform tasks that typically require human intelligence**, such as:

- Recognizing patterns
- Predicting outcomes
- Understanding language
- Generating novel content

Basics of AI

- Predictive AI Examples
  - Estimate the likelihood of escalation during a customer service call
  - SPAM filters in an email inbox
  - Estimating time of arrival for a GPS-mapped journey
  - Identifying likely candidate matches for a specific role
- Generative AI Examples
  - ChatGPT/other open chats against Large Language Models (“LLMs”)
  - Auto-generated suggestions in an email response
  - Writing a job description or interview questions from a role profile
  - Creating a draft of a document

Basics of AI

A **Large Language Model** is an AI system trained on massive amounts of text to predict the next words and generate human-like language.

You are all LLMs!

- “Once Upon a ___”
- “Roses are Red, Violets are ___”
- “Peanut Butter and ___”

AI in the Workplace

- Risks associated with AI in the Workplace arise from two scenarios:
  - Employee use of AI: unsanctioned use on personal devices or
  - Organizational use of AI: apps/vendors/services sanctioned by the organization.
- Each has different, unique risks. That is a different webinar.

AI Vendor Onboarding — Where Pilots Fail

- Change management and executive sponsorship
- Poor user experience or output quality concerns
- General resistance to change
- Poor Data Quality or Curation
- Inadequate Risk Controls
- Escalating Costs
- Unclear Business Value

AI Vendor Onboarding — Where Pilots Succeed

- Start small, then expand
- Non-critical, then critical
- Strong Focus on Data Quality and Curation
- Strong partnership between business and tech
- Back-office focus can be an easy win

AI Vendor Onboarding — High Level

- Where is the information coming from?
- Where is user input/data going?
- Raise any confidentiality/data privacy concerns

AI Vendor Onboarding – Checklist

1. Vendor & Data Profile

- Vendor legal name, jurisdiction, and primary business function documented.
- Clear description of the AI product/service being evaluated.
- Identify the **types of data** the AI tool will access or process (e.g., PII, PHI, financial, proprietary).
- Confirm whether data is **stored, used, or transmitted** outside your systems.

2. Data Flow & Processing

- Do they provide a **data flow diagram** showing where customer data travels (ingress→processing→egress)?
- Is data **encrypted in transit and at rest**?
- Are there **sub-processors** (third parties the vendor uses)? If yes:
- Vendor must list sub-processors and security controls in place.
- Confirm contract clause requiring prior notice for new sub-processors.
- Can you restrict or limit data retention to what's necessary?
- Is data deleted upon contract termination? (specify timeline)

AI Vendor Onboarding – Checklist (ctd.)

3. Data Ownership & Rights

- Does your organization **retain ownership** of uploaded/processed data?
- Does vendor claim any **rights to derive insights** or use your data for training models?
- If yes, confirm whether such usage is **explicitly authorized, time-limited, and reversible**.
- Any rights granted to vendor should be **non-exclusive and revocable**.

4. Security Controls & Certifications

- Vendor has documented **security policies and procedures**.
- Confirm whether vendor holds recognized certifications such as **ISO 27001, SOC 2**, or similar.
- Does vendor conduct **regular vulnerability assessments / penetration tests**?
- Confirm **access control** rules (e.g., least-privilege, MFA, role-based access).
- Is there **incident detection & response capability**?

AI Vendor Onboarding – Checklist (ctd.)

5. Privacy & Compliance

- Confirm compliance with relevant laws (GDPR, CCPA, HIPAA, etc.).
- Is vendor's **privacy policy publicly available and clear** about data use?
- Does vendor provide a **Data Processing Addendum (DPA)** consistent with applicable privacy laws?
- Can you support **data subject rights** requests (access/delete) through the vendor?

6. Intellectual Property (IP)

- Confirm that **your organization retains all IP rights** in your data and any derivatives.
- Clarify what IP rights vendor retains in their software.
- Check for any claims by vendor that your data or outputs are used to **train their models** for other customers.
- If present, require explicit consent and limitations in contract.
- Ensure **usage rights** for outputs are clearly defined (e.g., you can use model outputs without restrictions).

AI Vendor Onboarding – Checklist (ctd.)

7. Legal Protections

- Contract includes **indemnity clause** protecting you from vendor breaches/responsibilities.
- Confirm **limitations of liability** are fair and balanced.
- Include warranty that vendor complies with applicable laws and industry standards.
- Have a **data breach notification clause** specifying timeframe (e.g., within 72 hours).

8. Operational Resilience

Does vendor maintain a **business continuity plan**?

☐ What is vendor's **uptime commitment** (e.g., SLA for availability)?

☐ Can you get **service credits** for downtime / performance failures?

AI Vendor Onboarding – Checklist (ctd.)

9. Audit & Monitoring

- Vendor allows **third-party audits** or provides audit reports (e.g., penetration tests, SOC reports).
- Confirm ability to monitor ongoing vendor performance and risk post-onboarding.

10. Ongoing Risk Management

- Establish a **review schedule** (e.g., annual risk reassessment).
- Track and document any changes in data usage, sub-processors, security posture, or regulatory status.

New AI Liability

- **The law is 10 years behind technology**
- We’re seeing new, creative ways plaintiffs are creating liability with AI.
- An emerging trend: FCRA Liability

New AI Liability

- **What is the FCRA?** The Fair Credit Reporting Act.
- Federal law that regulates how consumer credit information is collected, used, and shared, and gives individuals rights to access and correct their credit reports.
- For employers, it imposes strict requirements when using background checks for employment decisions, including obtaining written consent from applicants, providing pre-adverse action notices, and ensuring accuracy and fairness in the hiring process.

New AI Liability

- So what? In January 2026, a landmark lawsuit was filed against Eightfold AI.
- Eightfold AI is an enterprise AI platform that manages the talent lifecycle—from recruiting and hiring to upskilling, retaining, and promoting employees. It is primarily used by large organizations to match people with optimal roles or projects based on their specific skills and potential.
- The plaintiffs claim Eightfold is acting like a background-check company, even though it presents itself as an AI hiring platform.

New AI Liability

- Specifically, the complaint alleges Eightfold creates hidden "background dossiers" on candidates, scoring them regarding their "likelihood of success," all without the individual’s knowledge or consent.

New AI Liability

- Naturally, Eightfold disagrees. It claims:
  - It sells software, not consumer reports, i.e., Microsoft is not the author of every document created in Word, and Eightfold says it is not the creator of a consumer report just because its software is used in hiring.
  - It is not a CRA because it trains on anonymous data.
  - It does not assemble or evaluation information for general use purposes.
  - It does not create consumer reports: the info comes from the applicant and the score does not bear on character or general reputation.

AI Controls and Governance

- Get a grip on usage
- Include multiple stakeholders, i.e., not just legal and HR
- Define AI and give examples
- Link to other policies (you have stuff on point, I'd guess)
- Provide broad dos and don'ts
- Appoint a lead (or a committee) to handle questions
- Have some consequences
- Address BYOD or personal devices
- Train your people

Stay up to date!

Sign up for a free trial of AIV Labor

Sign up to receive Vorys' labor & employment updates and invitations

VORYS
New thinking.
Since 1909.

Chaz Billington
Partner
cfbillington@vorys.com

Adam Borgman
Associate
amborgman@vorys.com