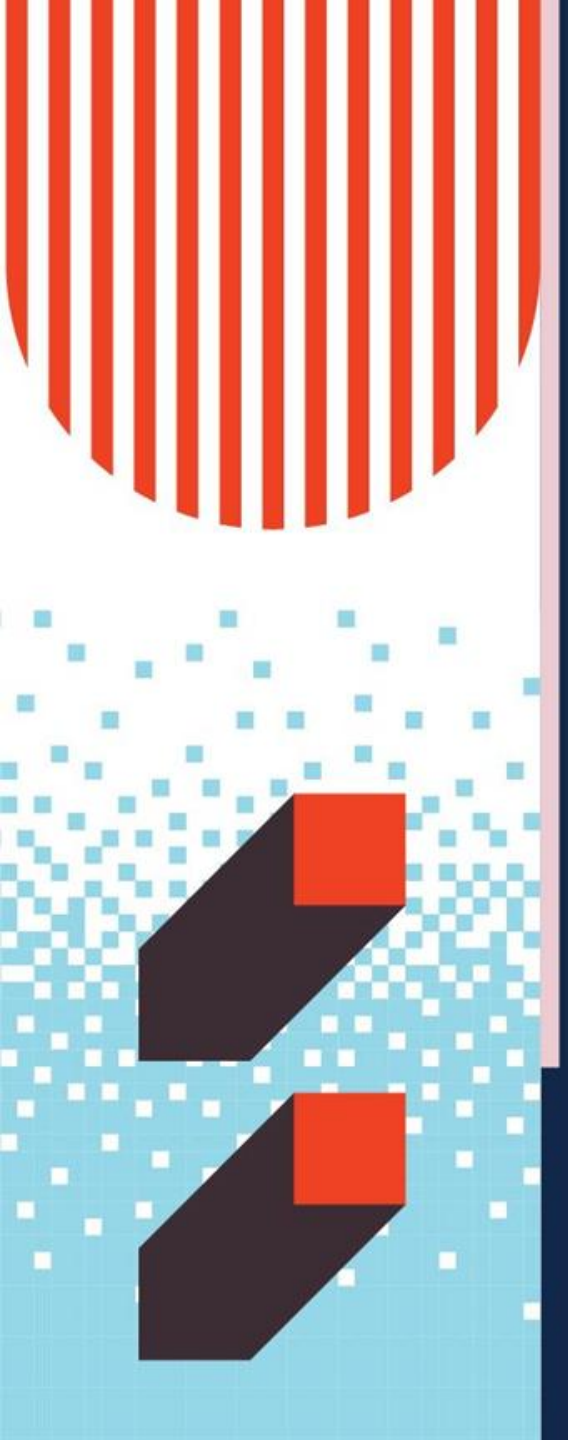


IAPP **AI Governance Global Europe 2026**

Training 1-2 June
Workshop 2 June
Conference 3-4 June
DUBLIN

#IAPPAIGG26

Algorithmic Bosses and Digital Colleagues

Transatlantic Lessons in Workplace AI Governance

WELCOME AND INTRODUCTIONS

Natalie Barnfield,
Petabyte Lawyer, Of Counsel,
Digiphile

Jennifer Ruehr, CIPP US, Co-Managing Partner, Hintze Law PLLC and Co-Chair Workplace Privacy and AI practice groups

AGENDA OUTLINE

I. Introduction: The state of Workplace AI

II. Comparative Regulatory & Legal Landscape

III. Case Studies:
   i. What is an automated decisions (and…what's the impact)
   ii. Profiling and vendor risk management

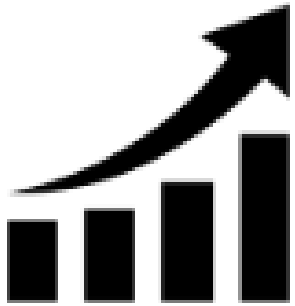
IV. Closing Remarks

V. Q&A

State of Workplace AI and ADMT

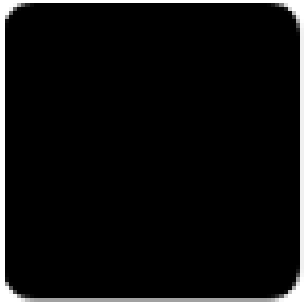
Workplace AI pose unique challenges

Employment decisions affect livelihoods



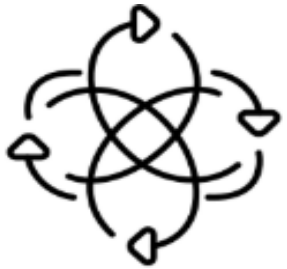
AI can scale bias rapidly and invisibly

Power imbalance amplified



Decisions opaque or technically complex

Shifting legal landscape



Complexity in 3P ecosystem

Misalignment on ADM vs decision support

New accountability + auditability obligations

#IAPPAIGG26

Comparative Regulatory & Legal Landscape: EU - UK

EU

EU AI Act (+ Omnibus + Guidelines)

- *AI used in recruitment or employment - default "high risk"*

EU GDPR (+ Omnibus + Guidelines)

- *AI in HR generally triggers ADM considerations.*

EU Platform Work Directive

Local Member State Considerations

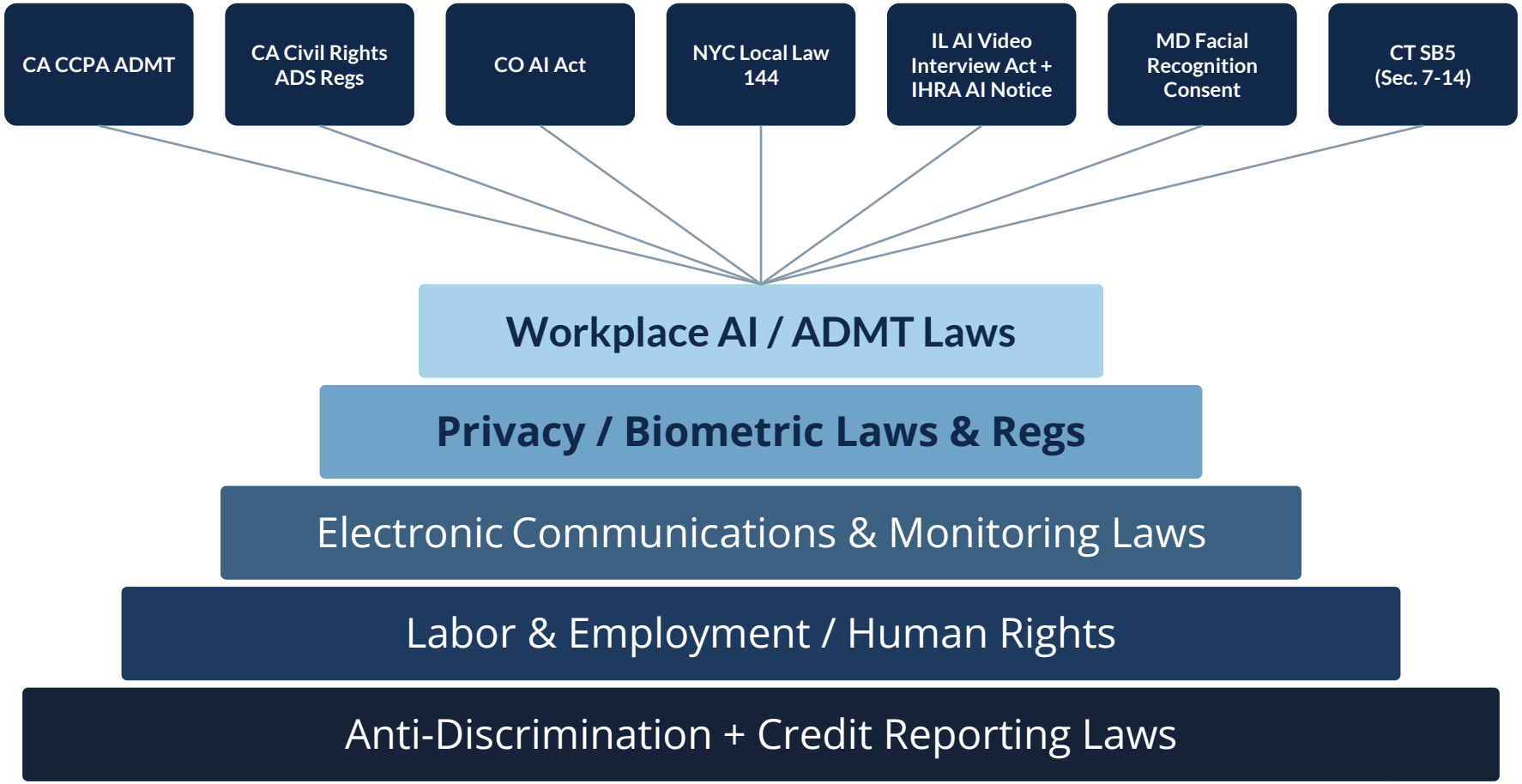
UK

UK GDPR (+ DUAA + ICO Guidelines)

- *AI in HR often trigger ADM considerations.*

UK Equality Act

Regulatory & Legal Landscape: the U.S. Patchwork

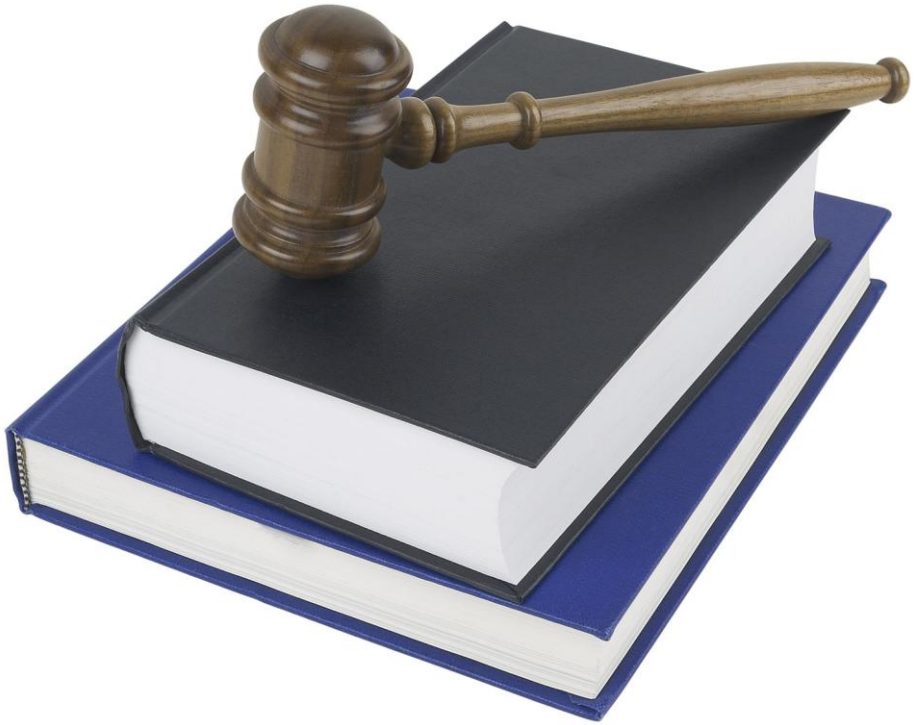


Key risk triggers? EU/UK vs US

- Automated decision making with legal or similar effects
- Special category data
- Monitoring or interception of comms
- Biometrics
- Emotion recognition
- Works council territories

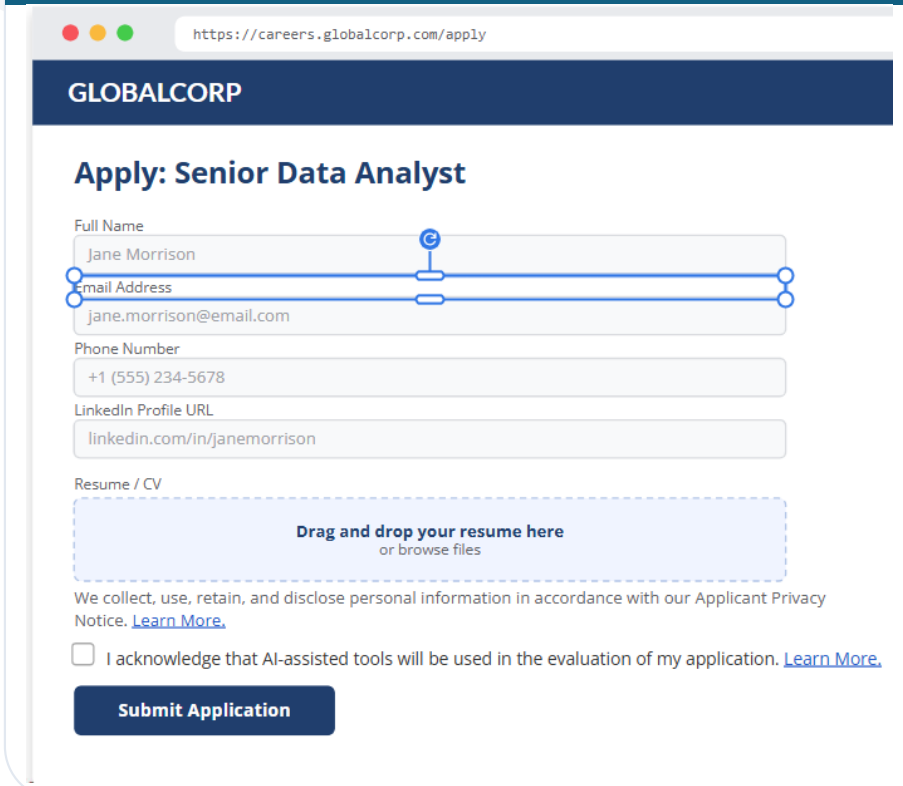
- Automated decision making re: protected characteristics
- Bias/ Discrimination
- Monitoring/ Electronic Comms
- Biometrics (CA, CO, IL, TX, WA)
- Unfair / deceptive practices
- Fair Credit Reporting laws

Case Studies



Case Study #1: What is an Automated Decision?

The Scenario



The Scenario:

A multinational company is looking to deploy an applicant tracking system that includes AI resume screening and comparing resumes to LinkedIn and other social media profiles across its European and U.S. operations.

Business Leader's starting assumptions:

- Screening tool marketed as "assistive"
- Humans will be involved in hiring decisions
- Goal is efficiency

Automated Decision Making Nuances

EU GDPR	UK GDPR	US

ADM Definition

1. Processing of personal data (including profiling)
2. By solely automated means (i.e. no meaningful human involvement)
3. Resulting in a decision that producing "legal" or "similarly significant" effects

ICO: Not a "decision" if there's no "consideration" e.g. binary eligibility criteria

ADM Definition

1. Tech processing **personal information**
2. Uses computation to replace or substantially **replace human decisions**
3. For "**consequential**" or "**significant" decisions** or that result in an "**adverse outcome"**

Consequences

- **Prohibited *unless*** an exemption applies (e.g. explicit consent) and **implement safeguards** (right to human review, to contest and express views)
- **Transparency:** meaningful information about logic, and consequences

Omnibus proposals?

Consequences

- **Permitted** if provide info about ADM logic and consequences **+ implement safeguards** (right to human review, contest decision and express views)
- **ADM + SCD prohibited** unless extra condition satisfied e.g. explicit consent.
- **Transparency:** meaningful information about logic, and consequences

Consequences

- **Permitted** subject to safeguards including: provide notice prior to use; access to logic, and in some cases consent and/or opt out or notice of adverse action
- **Prohibited** for use for discriminatory purposes or purposes that have a discriminatory effect.
- **Transparency**: meaningful information about logic, and consequences

The different concepts of “legal”, “significant”, “consequential” decisions

EU & UK GDPR

“Decision” producing "legal" or "similarly significant effects":

- Affecting legal status or rights
  - e.g. employment relationship, compensation
- Equivalent impact to personal circumstances, behavior, or choices
  - E.g. job / recruitment / pay opportunities

ICO: Not a “decision” if there’s no “consideration” e.g. binary eligibility criteria

CCPA Regulations

"Significant decision" means results in provision or denial of:

Employment/contracting opportunities or compensation:

- Hiring
- Allocation/assignment of work
- Compensation (salary, bonus, etc.)
- Promotion
- Demotion, suspension, & termination

CO AI Act (2026)

"Consequential Decision" means a decision, determination, or action made about a consumer that relates to

- the provision of or a consumer’s access to, eligibility for, selection for, or compensation for a covered domain; OR
- that relates to…compensation, or other material terms in a manner that is reasonably likely to materially limit, delay, effectively deny, or otherwise fundamentally alter…access, eligibility, or opportunity

“Meaningful” Human Review

(1) Understand the Output

The reviewer must know how to **interpret** and use the **AI tool’s results** to inform the decision.

(2) Analyze in Context

Review the AI output alongside **other relevant information** before making or changing the decision.

(3) Authority to Override

The reviewer **must have real power to change or reject** the AI’s recommendation.

Rubber-stamping does not count.

Case Study #1 ADM Risks + Requirements

Where an AI tool is **ranking**, **scoring**, **recommending** or **profiling** in the recruitment contexts and there is **NO meaningful human review**, likely to be automated decision making (system) triggering...

In the EU/UK:

- Explicit consent(?)
- Transparency about logic
- Safeguards:
  - Right to human review
  - Information about logic + consequences
  - Right to contest and make representations
- Broader GDPR obligations - DPIA, DSRs

In the US:

- Notice, choice, individual rights
- Risk assessments/bias audits
- Data retention
- Vendor obligations
- Ongoing monitoring
- CA: Attestation to CalPrivacy re cybersecurity audits and risk assessments

EU AI Act - HRAI

Is it high-risk AI system? (Likely) - see draft HRAI Guidelines

- Used for "*recruitment or selection… to analyse and filer job applications… " [Annex III 4(1)]*

Derogation?: *Arguable* - depending on providers "intended use" of AI system - but starting assumption should be high risk

System Requirements

- Risk management system
- Data and data governance
- Technical documentation
- Record-keeping (Logs)
- Transparency and use instructions
- Design for human oversight
- Accuracy, robustness & cybersecurity

Provider Requirements

- Comply with system requirements
- Indicate name, TM, contact address
- Quality Management System
- Documentation & Logs
- Conformity Assessment & Registration
- Corrective action / duty of information
- Regulatory cooperation (demonstrate conformity)
- Accessibility requirements

Deployer Requirements

All Deployers

- Follow instructions for use
- Human oversight
- Data relevance/representation
- Risk & incident monitoring
- Keep logs (6m+)
- Conduct DPIA
- Regulatory cooperation

Some Deployers

- Workplace: Inform workers

#IAPPAIGG26

US: Old Requirements – New ADMT Risks

FCRA

THRESHOLD
3P "consumer report" bearing on character, reputation, or credit for employment purposes

NOTICE + CONSENT
Pre-use notice and written consent required

ADVERSE ACTION
Notice and information access required before adverse action taken

CRA OBLIGATIONS
Contract, accuracy, and individual rights obligations for credit reporting agencies

Anti-Discrimination

DISPARATE IMPACT
Must not disproportionately exclude protected groups; test outcomes with 4/5ths rule

DISABILITY ACCOMMODATIONS
Reasonable accommodations required; offer alternatives where AI tools disadvantage

EMPLOYER LIABILITY
No vendor shield; employers must independently validate AI tools

TRANSPARENCY
AI hiring notice required; state/local laws may mandate bias audits (e.g., NYC LL144)

Where EU/UK and U.S. align and diverge

Alignment	Divergence
Screening Resumes Generally engages ***high risk*** considerations – can be mitigated based on implementation and meaningful human review	**U.S. Patchwork Complexity** Creates complexity around policies and procedures in addressing individual rights and transparency.
Applicant / Individual Rights Generally aligned where they apply (but patchwork in U.S. on *when* these rights apply)	**Vendor Agreement Misalignment** Agreement requirements don't line up 1:1 with EU/UK standards.
Risk Assessments Generally aligned where they apply (but patchwork in U.S. on *when* these are required)	**EU vs. UK Patchwork Complexity** UK is more permissive subject to safeguards; EU prohibits ADM subject to exemptions.
Transparency Generally aligned where they apply (but patchwork in U.S. on *when and how often* notices are required)	
ADM Interpretation Different levels of business understanding of "ADM" and what constitutes a "decision" (e.g. automation vs. decision support vs. automated-decision-making)	

Case Study #2: Profiling & VRM

The Scenario

The sales team onboarded a new vendor whose product has features to **monitor and analyze team communications** (video, audio, email, and chat) either **in real time or by transcript** and can **provides immediate coaching** to help global sales teams improve their communications and and rate their performance. The suggestions can range from "speak more slowly" or "consider recommending…" Sales has already signed the contract and comes to privacy to see if there is anything they need to do for their global rollout next week.

Starting assumptions:

- procured on basis it would st be used for coaching
- The vendor was reviewed by infosec
- There's a DPA in place

#IAPPAIGG26

Case Study #2 Global Considerations

Biometric data collection (voiceprints)

Emotion Recognition

Profiling/ Monitoring

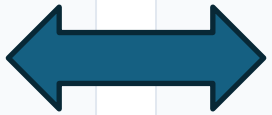
Electronic communications / interception of communications

Privacy governance (DPIAs, Individual Rights)

Vendor Risk Management

Case Study #2 Global Considerations

Biometric data collection (voiceprints)



Emotion Recognition

Profiling/ Monitoring

Electronic communications / interception of communications

Privacy governance (DPIAs, Individual Rights

Vendor Risk Management

Case Study #2 Global Considerations

Biometric data collection (voiceprints)

Emotion Recognition

Profiling/ Monitoring

Electronic communications / interception of communications

Privacy governance (DPIAs, Individual Rights

Vendor Risk Management

Case Study #2 Global Considerations

Biometric data collection (voiceprints)

Emotion Recognition

Profiling/ Monitoring

Electronic communications / interception of communications

Privacy governance (DPIAs, Individual Rights

Vendor Risk Management

Case Study #2 Global Considerations

Biometric data collection (voiceprints)

Emotion Recognition

Profiling/ Monitoring

Electronic communications / interception of communications

Privacy governance (DPIAs, Individual Rights

Vendor Risk Management

AI Vendor Governance: Through the VRM Lifecycle

1. INTAKE & SCOPING

The Guardrail: Implement a mandatory AI-Risk Trigger Questionnaire at the RFP stage.

Practical Check: Do not rely on business unit descriptions (e.g., "just a chatbot"). Force vendors to disclose: biometric processing, real-time comms analysis, or automated performance scoring.

2. DUE DILIGENCE

The Guardrail: Demand structured AI technical documentation (EU AI Act Arts. 11–13 compliant), regardless of vendor jurisdiction.

Practical Check: Validate training data for systemic bias, review algorithmic validation methods, and map where processing shifts from decision support to solely automated decision-making.

3. CONTRACTUAL GUARDRAILS

The Guardrail: Supplement standard DPAs with an explicit AI Governance Addendum.

Practical Check: Secure independent bias audit rights, description of anticipated/expected use cases, mandatory notifications if vendor retrains models, use limitations on model training, fine tuning, and similar activities, and clear indemnification for algorithmic bias, material hallucinations, and personal data breach claims.

4. DEPLOYMENT RISK MAPPING

The Guardrail: Conduct a context-specific DPIA before the contract is finalized.

Practical Check: Map local triggers — wiretapping/two-party consent laws (CA, IL), biometric identifiers under BIPA, and Works Council consultations in the EU.

5. CONTINUOUS MONITORING + ESCALATION WORKFLOWS

The Guardrail: Establish an ongoing framework for Meaningful Human Review.

Practical Check: Don't "rubber-stamp" AI scores. Audit annually against protected characteristics (4/5ths rule), maintain logs to catch model drift creating new exposure.

KEY TAKEAWAY

Shared Accountability is the model and DPAs alone aren't sufficient. Standard InfoSec and uptime reviews are blind to algorithmic risks. An AI-aware VRM lifecycle stops unauthorized high-risk deployments *before* they require a costly global rollout halt.

Wrapping Up

Employer Checklist

Scoping & Governance

Understand AI Use Case Scope

- Purpose / necessity
- Territorial scope
- Personal data processed
- 1P or 3P tool?
- Provider or deployer?
- Is 3P controller/business or processor/service provider?

Review Assessments for regional requirements including

- AI Assessments (High Risk?)
- DPIA/Privacy Risk Assessment
- Bias Testing, Audits, Mitigations

Vendor Management

Vendor due diligence/contracts: (AI+DP) (including update Qs for ADMT, FCRA)

- DPA + AI Addendum or specific terms re bias audit rights, model retraining, indemnities for bias)

Security Assessments

DP & AI Risk Assessments

3P tool/system implementation procedures,

Workflows for vendor escalation, assistance

Ongoing Oversight

Transparency (Notice + Choice)

Data Subject Rights (Opt-outs, Corrections, Explainability)

Retention/deletion process/policy

Establish/log meaningful human review

Monitoring & Escalation Process

Training / Literacy Programs

Complaints / contesting decisions

California: Certification/attestations requirements by exectuive for cybersecurity audits/risk assessments

Key Takeaways

- Workplace AI is an emerging enterprise risk
- Meaningful human review is harder than it looks and not always practical to avoid ADMT
- Think globally, act locally – adopt a global baseline with local flexibility
- Know your use cases and third-party ecosystem to manage risk
- Transparency, stakeholder engagement, risk assessments, and training are universal requirements

Q&A

RESOURCE LIST - EU/UK

- EU AI ACT
- EU GDPR
- Digital Omnibus
- UK GDPR + UK Data Protection Act
- UK Equality Act
- WP Guidelines on ADM and profiling WP251rev.01
- UK ICO's *"Recruitment Rewired: an update on the ICO's work on the fair and responsible use of automation in recruitment"*

RESOURCE LIST - US

- California Consumer Privacy Act + Regulations
- California Civil Rights Council Employment ADMT Regulations
- Colorado AI Act (2026)
- NYC Local Law 144
- NY Employers Engaged in Electronic Monitoring
- Illinois Human Rights Amendment + Draft Regulations
- Illinois AI Video Interview Act
- Maryland An Act concerning Labor and Employment – Use of Facial Recognition Services – Prohibition
- Connecticut Act Concerning Online Safety (new 2026 - not yet signed)
- CFPB Circular 2024-06: Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions
- U.S. Fair Credit Reporting Act (FCRA) -
  i. California ICRAA (California's "FCRA" law)
  ii. NY Fair Credit Reporting Act

Appendix: FCRA: Employer Obligations

✓	FCRA Activity	Employer Obligation
✓	**Vendor assembles applicant profiles from multiple data sources** CFPB: Algorithmically assembled dossiers from public + proprietary data = "consumer reports" regardless of technology used	Vendor classified as CRA → employer must verify CRA compliance, obtain permissible purpose certification, ensure vendor follows all CRA obligations
✓	**Vendor generates scores or rankings for employment decisions** AI-generated scores bearing on character or personal characteristics = consumer report, even if vendor self-identifies as "talent intelligence"	Standalone FCRA disclosure + written authorization required before any report is procured; employer certifies permissible purpose to CRA
✓	**Applicant rejected or ranked unfavorably based on AI output** Eightfold ranked candidates without triggering adverse action notices; applicants never knew AI scores influenced their rejection	Pre-adverse notice + copy of report + waiting period, then adverse action notice identifying CRA. Two-step process with no GDPR equivalent
✓	**AI makes probabilistic inferences treated as reportable facts** CFPB: "Maximum possible accuracy" standard applies to AI inferences; probabilistic scores may inherently fail this threshold	Employer must ensure vendor maintains reasonable procedures to assure accuracy; dispute investigation + correction within 30 days required
✓	**Vendor contract lacks FCRA-specific terms** DPA or standard SaaS terms ≠ FCRA compliance; employer must certify permissible purpose and FCRA obligations in vendor agreement	Dual liability: both vendor (as CRA) and employer (as user) face FCRA exposure. $100–$1,000 statutory damages per violation, per applicant

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP AIGG Europe 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!