

Insights

CAN YOU HOLD THREE FINGERS IN FRONT OF YOUR FACE? AI TRANSPARENCY AT WORK

Aug 20, 2026

Summary

Do your employees understand when and how they are being exposed to/monitored by AI in the workplace?

What happened?

A recent viral video from scam-baiter, Jim Browning, provides a startling (if not slightly amusing) illustration of how life-like AI may appear to the un-trained eye. Suspecting that a scammer was using a real-time AI deepfake, Browning calmly asked the scammer to hold three fingers up in front of his face, knowing how this would disrupt the deep-fake facial image. The scammer refused and abruptly ended the call.

Why is this relevant for employers?

This viral clip raises an interesting question around AI transparency for employers: are you being sufficiently transparent with your employees and applicants about when and how they are being exposed to/monitored by AI systems in the workplace?

This is now a formal requirement in the EU. From 2 August 2026, EU businesses have been subject to increased transparency obligations in respect of their development and/or deployment of AI systems which interact directly with individuals, via Article 50 of the EU AI Act.

These new obligations include the need to inform individuals if content has been AI generated or manipulated and when individuals are subject to emotion recognition or biometric categorisation software. Separately, the EU AI Act already prohibits the use of emotion recognition software to infer emotions in the workplace (in force since February 2025), save for narrow medical or safety exceptions.

The UK, by contrast, has no dedicated AI Act (yet...), but that does not mean UK employers are unregulated.

Where AI involves the processing of personal data, the use of automated decision-making (**ADM**) technology is subject to specific provisions of the GDPR. Since 5 February 2026, the Data (Use and Access) Act 2025 (**DUAA**) replaced the previous near-prohibition on solely automated decision-making with a new permission-based regime.

Employers may therefore utilise ADM tech, provided a lawful basis for processing has been identified at the outset. However, where a decision is based solely on automated processing and has a legal or similarly significant effect on an individual, e.g. whether a candidate progresses to interview, the level of an employee's pay or bonus, or who and employer selects for redundancy, employers need to build in the following safeguards: transparency about the decision, the ability for the individual to make representations, to obtain human intervention, and to contest the outcome.

Decisions involving special category data also remain more tightly restricted.

Earlier this year, the ICO took an active interest in how this regime works in the real world. Following engagement with more than 30 employers using ADM in recruitment, the ICO identified a greater need for transparency, stronger safeguards, meaningful human involvement, and better monitoring for bias.

It subsequently wrote to 16 organisations making recommendations for improvements in their use of ADM technology, including clearer information for candidates about how AI is being used, ways of challenging automated decisions, how individuals can request human intervention, and regular monitoring for discriminatory outcomes. The ICO also developed further its ADM guidance around this time.

What should you do now?

Organisations operating AI systems in the EU should review any use of emotion recognition or biometric categorisation technology against Articles 5 and 50 of the EU AI Act.

For UK employers, it is important that management and HR have a working understanding of how their ADM tech operates so that they are equipped to identify biases, can intervene at any stage of the ADM process and can explain clearly to individuals how and why decisions have been reached by the ADM. This should form the basis of a data protection impact assessment (**DPIA**) undertaken, ideally, before deployment of an ADM tool.

Failure to do so could result in intervention from the ICO, damage to employee relations, claims of discrimination and, in extreme cases, fines (and perhaps three fingers from your employees).

What is the most alarming AI glitch you have encountered?

If you have any questions about this development or its implications for your business, please contact [Paul Sands](#) or another member of [BCLP's UK Employment team](#).

If you have any questions regarding data privacy compliance (including data protection impact assessments and data subject access requests), cybersecurity, or AI/data protection issues more generally, please contact our [Data Protection & Cybersecurity team](#). For broader insights into recent developments in data privacy, digital regulation and deployment of AI, see our most recent update [BCLP's Data Privacy, Digital Regulation & AI: 2026 Mid-Year Round-Up](#).

Related Capabilities

- Employment & Labor
- Data Privacy & Security

Meet The Team



Paul Sands

Counsel, London

paul.sands@bclplaw.com

[+44 \(0\) 20 3400 4084](tel:+442034004084)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.