Volume 10, No. 1 | January-February 2027

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: Contrasting Strategies
Victoria Prussen Spears

AI, Intellectual Property, and National Security: Understanding the Administration's Contrasting Strategies
Armin Ghiam and Andre Earls

The Evolving AI Patchwork: Balancing U.S. State Shifts and EU Mandates in Deal Negotiations
David A. Toy, Thomas J. Petrie, and Colin Harris

Adapting Error Resolution to Agentic AI Payments
David A. Stein

AI Is Making Phishing Scams Almost Impossible to Spot—5 Steps Employers Should Take to Combat Latest Threat
Daniel Pepper and Michael Steele

Indian Gaming and Prediction Markets: On a Collision Course?
Blaine I. Green and Allan C. Van Vliet

Prediction Markets Are Creating a New Insider Trading Frontier for Biotech and Pharmaceutical Companies
Chelsea Anderson and Noah Solowiejczyk

CFTC Targets George Santos for Manipulative Trading in State of the Union Event Contract
John C. Murphy, Katherine R. Goldstein, James Joseph Benjamin Jr., Michael A. Asaro, Peter I. Altman, Parvin Daphne Moyne, and Lance Jasper

Different Shoppers, Different Prices: The Federal Trade Commission Takes Aim at Personalized Pricing
Allyson L. Chavez, Anna M. Behrmann, and Kathy L. Osborn

Third Circuit Revives Algorithmic Price-Fixing Suit Against Atlantic City Hotels
Alexis Gilman and Drew Wilson

Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?
Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff

Automating the Impact Assessment, and the Limits of AI Compliance
Adilson Fernandes Braga Junior

The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI
James Castro-Edwards

FULL COURT PRESS
part of Clio

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 10, No. 1 | January–February 2027

7 **Editor's Note: Contrasting Strategies**
Victoria Prussen Spears

11 **AI, Intellectual Property, and National Security: Understanding the Administration's Contrasting Strategies**
Armin Ghiam and Andre Earls

17 **The Evolving AI Patchwork: Balancing U.S. State Shifts and EU Mandates in Deal Negotiations**
David A. Toy, Thomas J. Petrie, and Colin Harris

23 **Adapting Error Resolution to Agentic AI Payments**
David A. Stein

33 **AI Is Making Phishing Scams Almost Impossible to Spot—5 Steps Employers Should Take to Combat Latest Threat**
Daniel Pepper and Michael Steele

37 **Indian Gaming and Prediction Markets: On a Collision Course?**
Blaine I. Green and Allan C. Van Vliet

43 **Prediction Markets Are Creating a New Insider Trading Frontier for Biotech and Pharmaceutical Companies**
Chelsea Anderson and Noah Solowiejczyk

49 **CFTC Targets George Santos for Manipulative Trading in State of the Union Event Contract**
John C. Murphy, Katherine R. Goldstein, James Joseph Benjamin Jr., Michael A. Asaro, Peter I. Altman, Parvin Daphne Moyne, and Lance Jasper

55 **Different Shoppers, Different Prices: The Federal Trade Commission Takes Aim at Personalized Pricing**
Allyson L. Chavez, Anna M. Behrmann, and Kathy L. Osborn

61 **Third Circuit Revives Algorithmic Price-Fixing Suit Against Atlantic City Hotels**
Alexis Gilman and Drew Wilson

67 **Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?**
Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff

75 **Automating the Impact Assessment, and the Limits of AI Compliance**
Adilson Fernandes Braga Junior

85 **The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI**
James Castro-Edwards

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Jennifer A. Johnson
Partner, Covington & Burling LLP

Paul B. Keller
Partner, Allen & Overy LLP

Garry G. Mathiason
Shareholder, Littler Mendelson P.C.

James A. Sherer
Partner, Baker & Hostetler LLP

Elaine D. Solomon
Partner, Blank Rome LLP

Edward J. Walters
Chief Strategy Officer, vLex

John Frank Weaver
Director, McLane Middleton, Professional Association

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, an imprint of Clio and Themis Solutions, Inc..
Copyright 2027 Full Court Press, an imprint of Clio and Themis Solutions, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Full Court Press, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: David Nayer
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Full Court Press)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2027 Full Court Press, an imprint of Clio and Themis Solutions, Inc.

All Rights Reserved.

A Full Court Press, Clio, Publication

https://www.fastcase.com/

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

David Nayer, Publisher, Full Court Press at david.nayer@clio.com or at 202.999.4777

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI

James Castro-Edwards*

In this article, the author explains that, given the formal Code of Practice on artificial intelligence (AI) and automated decision-making being prepared by the UK's data protection regulator, businesses that use AI or automated tools to make or support decisions about people and that are subject to the UK General Data Protection Regulation should start assessing their use now.

All companies that are subject to the UK General Data Protection Regulation (UK GDPR) and develop or use artificial intelligence (AI) should begin assessing their AI and automated decision-making use now, in anticipation of the Code of Practice that the Information Commissioner's Office (ICO) is required to produce, and should monitor ICO guidance and the Code as it develops to ensure compliance.

In short: the UK's data protection regulator, the ICO, is preparing a formal Code of Practice on AI and automated decision-making, and expects businesses to act well before it takes effect. This is not only a developer issue; any organization that uses AI or automated tools to make or support decisions about people, including tools bought from a third party, and that is subject to the UK GDPR, including organizations with no UK presence at all, where they offer AI-enabled goods or services to, or monitor the behavior of, individuals in the United Kingdom, should start assessing that use now. The legal detail behind this is technical, and is set out below for those who want it, but the practical message is straightforward: businesses that map, assess, and document their AI and automated decision-making use now will be considerably better placed than those that wait.

On May 12, 2026, the Data Protection Act 2018 (Code of Practice on Artificial Intelligence and Automated Decision-Making) Regulations 2026 (SI 2026/425)[1] came into force, requiring the

Robotics, Artificial Intelligence & Law / January-February 2027, Vol. 10, No. 1, pp. 85-90
© 2027 Full Court Press. All rights reserved
ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Information Commissioner, under section 124A of the Data Protection Act 2018 (DPA) (as inserted by section 92(2) of the Data (Use and Access) Act 2025 (DUAA)), to prepare a Code of Practice on the processing of personal data in relation to developing and using AI and automated decision-making (ADM), including a mandatory children's data component. The Regulations also modify the independent panel process under section 124B of the DPA (inserted by section 93 DUAA) to exclude national security matters from the panel's remit. For these purposes, "automated decision-making" is defined by reference to Article 22C(1) of the UK GDPR and section 50C(1) of the DPA, both also inserted by the DUAA. Most of the data protection reforms introduced by the DUAA took effect on February 5, 2026. The duty on the Information Commissioner under SI 2026/425 is a separate, later development, and arguably the most significant AI-related instrument the ICO has been given to date.

The ICO had already opened a consultation on March 31, 2026, on updated draft guidance on ADM and profiling, its first detailed reading of the ADM reforms introduced by the DUAA. That consultation[2] closed on May 29, 2026. At the time of writing, the ICO has indicated that final guidance will follow in winter 2026-27, ahead of the statutory Code itself, which is not expected to take effect until 2027. For businesses that build AI models, this is a familiar story. For businesses that simply use AI tools bought or licensed from someone else, it is less well understood and, in our experience, considerably more likely to be overlooked.

Background

SI 2026/425 does not itself impose new obligations on businesses. It gives effect to the duty on the Information Commissioner, under section 124A DPA, to prepare the Code, and modifies the section 124B independent panel process to exclude national security matters from its remit before the Code is laid before Parliament. Section 50C DPA and Article 22C UK GDPR, both inserted by the DUAA, are referenced only to define "automated decision-making" for the purposes of the Regulations; they are not themselves the source of the duty. Once finalized, the Code is expected to carry the same statutory weight as the existing Children's Code and Data Sharing Code: courts must take it into account in relevant

proceedings, and the ICO must have regard to it in enforcement decisions. That is a materially different order of obligation from non-binding guidance.

In the meantime, the ICO's draft ADM guidance, though not yet final and not itself the statutory Code, is the clearest available signal of the ICO's thinking, including on what will count as "meaningful human involvement" in an automated decision (active review before a decision takes effect, not a token sign-off) and on the documentation the ICO will expect organizations to hold.

Who Does This Affect?

This is not limited to UK-based companies: it includes organizations with no UK presence at all, where they offer AI-enabled goods or services to, or monitor the behavior of, individuals in the United Kingdom. A common misconception is that AI regulation is primarily a problem for the businesses that build AI models. It is not. The ICO's ADM rules attach to the controller that uses an automated or AI-assisted output to make a decision about an individual, regardless of who built the underlying tool. Buying or licensing a third-party AI system does not transfer that responsibility to the vendor. In practice, this reaches:

- Recruitment and human resources functions using AI-assisted curriculum vitae screening, candidate ranking, or recruitment platforms;
- Financial services and insurance businesses using AI or automated systems for credit decisions, pricing, or fraud and risk scoring;
- Customer-facing businesses using AI chatbots or automated triage tools that affect service outcomes, refunds, or complaint handling;
- Life sciences and healthcare organizations using AI to prioritize, triage, or flag patient cases; and
- Any business procuring third-party AI tools in the ordinary course of vendor and supplier assessment.

The ICO's own research, published in its Recruitment Rewired report[3] alongside its draft ADM guidance, found that many employers relying on automated recruitment tools were likely conducting solely automated decision-making, without meaningful human

involvement and without adequately telling candidates so, in circumstances where several were not aware, or did not acknowledge, that this was what they were doing. The obligation can therefore apply even where a business regards itself as simply using a tool, rather than deploying AI.

The Risks of Non-Compliance

- *Regulatory enforcement*. Enforcement for ADM or AI-related breaches sits within the existing UK GDPR penalty regime, fines of up to the higher of £17.5 million or 4 percent of global annual turnover. Once finalized, the Code is likely to become the benchmark the ICO uses to assess what "good practice" looks like.
- *Individual rights and litigation risk*. Individuals affected by an automated decision have rights to be informed, to obtain meaningful human review, and to challenge the outcome. Unmanaged AI or ADM use is accordingly a direct source of individual complaints, and potentially litigation.
- *Priority-sector scrutiny*. The ICO's AI and biometrics strategy names three priority areas: foundation model development, ADM in recruitment and public services, and police use of facial recognition technology,[4] meaning these areas are more likely to attract proactive regulatory attention rather than only complaint-driven investigation. Agentic AI sits outside these three formal priorities for now, but the ICO has flagged it as an emerging area and dedicated guidance is expected as part of its 2026/27 work program.
- *Vendor and procurement risk*. AI-specific contractual terms, covering training-data rights, model updates, output ownership, and sub-processing, are increasingly expected in due diligence, but are not yet standard in many existing supplier agreements.
- *Reputational exposure*. Unmanaged AI use is increasingly treated as a board-level issue, and being seen to react only after a complaint or investigation is materially worse, from a regulatory and reputational perspective, than being able to demonstrate a documented, proactive governance process.

What Should Businesses Do Now?

- Map AI and ADM use across the organization, including tools procured from third-party vendors, not only internally developed systems.
- Review, or create, Data Protection Impact Assessments where AI or ADM use is likely to result in high risk to individuals, in line with the ICO's draft guidance, with particular attention to the "meaningful human involvement" test.
- Audit vendor and procurement contracts for AI-specific terms, including training-data rights, model updates, and output ownership.
- Benchmark AI use in recruitment, financial decision-making, and any context involving children's data against the ICO's stated priority areas.
- Monitor for the ICO's final ADM guidance, expected in winter 2026-27, and the statutory Code itself, expected in 2027, and revisit governance documentation once each is published.

Conclusion

SI 2026/425 is, on its face, a narrow procedural instrument: a duty on the Information Commissioner to produce a Code, not a new set of obligations on business. In practice, it is a foundational step toward the most significant AI-specific instrument the ICO will have produced, and the draft ADM guidance already gives a reasonably clear preview of its likely direction. Businesses that treat AI governance as a developer problem, rather than a deployer problem, risk being caught out when the Code and the enforcement expectations that come with it take effect. Those who map, assess, and document their AI and ADM use now will be considerably better placed than those who wait.

Notes

* The author, counsel in the London office of Arnold & Porter Kaye Scholer LLP, may be contacted at james.castro-edwards@arnoldporter.com.

1. https://www.legislation.gov.uk/uksi/2026/425/made.
2. https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2026/03/ico-consultation-on-the-draft-guidance-about-automated-decision-making-including-profiling/.
3. https://ico.org.uk/about-the-ico/what-we-do/recruitment-rewired/.
4. https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/artificial-intelligence-and-biometrics-strategy/where-we-will-focus/.