AI, Machine Learning & Big Data 2025

Seventh Edition

Contributing Editor:
Charles Kerrigan
CMS LLP

glg Global Legal Group

TABLE OF CONTENTS

Profiling and prohibited practices: A summary of legal requirements for automated decision-making in the EU and UK

Lisa McClory

CMS LLP

Personalised digital services have become an increasingly important aspect of everyday life in recent years, beginning with the gig-economy and use of digital platforms (such as Uber and PayPal) to manage access to work, services and payments, together with recommendation engines and social media feeds (such as Netflix and Spotify) that curate and deliver personalised content, such as news and music. The aspiration of platform services is to replace admin-heavy systems with faster, efficient and objective autonomous systems, and to move away from relying on humans to input data and perform manual tasks.

Until recently, platform-led business models have been the preserve of companies making large investments into planning and building system architecture and shaping new markets for digital products and services. This created a barrier to innovation for smaller organisations, given the time and financial commitment required to engineer digital journeys, overhaul existing workflows and replan legacy data infrastructure. Reliance on hard-coded 'if-this-then-that' logic systems previously also presented a blocker to systems achieving their full potential: sophisticated conditional workflows are hard to plan and time-consuming to maintain.

With the advent of increased, cheaper access to AI and machine learning, there is now much greater ability for businesses to automate more and much faster across all areas, from AI writing code to creating user interfaces, understanding user journeys and automatically monitoring for fraud, security flaws and risks. Businesses can now build digital infrastructure in a cost-effective way and can create increasingly sophisticated digital personalised products and services, opening up the opportunity for consumers to save time and access services in new ways.

This is also combined with far greater access to data than ever before. Sensors and smart personal devices provide new sources of localised real-world data, combined with smart street infrastructure, autonomous vehicles, robots, satellites and drone technology permitting access to contextual and geospatial data. AI speeds up the ability to extract insights from unstructured information and read data across siloes and formats, which in turn has hugely expedited the pace of innovation.

Privacy or convenience?

Customers can benefit from innovative services based on effective use and sharing of data, which can reduce admin and save time, or allow people to access services that they would have previously been unable to reach or afford. For example, large language models ('**LLMs**') can be used with vision simulation to train robots to complete open-ended tasks, allowing assistive robots to help people in home

environments, where spaces and requirements are less predictable. AI can cut down on personal admin and make interactions with the digital world easier across every area: from selecting and purchasing services, to delivery tracking, complaints and refunds, as well as access to essential civil services. Later in 2025, Citizens Advice plan a national roll-out of a GenAI-powered LLM Bot called Caddy that helps front-line support staff provide answers to client legal queries more quickly. There are many further use cases, including fraud detection, personalised shopping recommendations, automated credit-risk assessments and more.

Risks arise, however, where services are over-personalised, for example where a recommendation for something a person has bought pops up later and unexpectedly on unrelated websites, or a system sends excessively personalised messages, or where (as was reported recently in the news), AI models can serve up an individual's 'psychological profile' on demand in a social context. Digital profiles can be seen as a kind of digital identity: sometimes people have control over their identity, where they are granted access to manage attributes and uses, and sometimes they do not. Classifications could be imposed without a person's knowledge or consent, based on the behaviour of others with attributes deemed to be statistically similar, in ways that people are not able to interrogate or correct.

This can give rise to substantial privacy concerns, as well concerns about individual dignity, and security or personal safety risks if data is stolen or misused, for instance through a data breach, or for identity theft or creation of deep-fakes. Where so much data is available, and distributed across a range of corporate actors and via AI models, too, it is at risk of being put to unexpected uses, perhaps with malicious intent, or simply in ways that give rise to unanticipated harmful outcomes.

Individual rights and systemic oversight

Traditionally, decisions were made by rule-based systems, and now these systems are being replaced by AI, which includes probabilities. This is much more difficult for humans to control and oversee. As more decision-making systems move outside human control, and more towards reliance on complex data processing, analysis and insights, it is of paramount importance to preserve individuals' ability to understand and, when necessary, challenge how decisions that affect them have been made.

This right to challenge can take shape as an individual right to transparency and explanation. There are limits of this approach, as enforcement relies on an individual's willingness and ability to bring a challenge, and *ad hoc* interventions are generally insufficient to create system-wide assurance that AI systems are safe, trustworthy, robust and reliable. So alongside individual rights, there is also a need to prevent risks from occurring by focusing on how automated systems and AI are overseen and governed. New laws such as the EU AI Act supplement existing data protection frameworks, but this results in a complex interrelationship, currently the subject of litigation, debate and fast-changing market practice. Transparency, governance and accountability can often be a complex question when considered in the context of data supply chains and multi-layered systems, with a range of organisations often involved in the delivery of a given product or service. Questions include:

- If a human is involved in the process, when is decision-making automated?
- Who is accountable for the system, and for the role of human and machine-driven monitoring within a system's controls?
- Can the system provide meaningful information about the logic involved in profiling?
- What steps do organisations need to take to verify the accuracy of information used in automated decision-making ('**ADM**') and profiling?

Further in this chapter, we therefore consider recent developments in the EU and UK approach to AI and ADM, areas of similarity and divergence, and practical impacts on businesses developing new data-driven products and services.

Data protection law vs AI

Until fairly recently, data protection law has been the main legal safeguard for individual rights in respect of profiling and ADM.

The General Data Protection Regulation (EU) 2016/679 ('**GDPR**') has long provided a principles-based framework to protect individuals' rights where their data is used. Individuals benefit from a specific right under Article 22 GDPR not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them. This could include, for example, being refused access to a service or to credit, or being subject to cv-sifting software without any human intervention.

Article 15(1)(h) GDPR provides individuals with a further right to obtain information about whether they are the subject of ADM, and where this is the case, to access meaningful information about the logic involved and the consequences of such processing for them.

From August 2024 onwards, the EU AI Act is gradually coming into effect as an overarching framework for regulation of all AI systems. The EU AI Act imposes detailed requirements on providers of high-risk systems, alongside a set of comprehensively applicable prohibitions of certain AI use cases that are deemed too risky and harmful to be permissible. The Act also regulates profiling and ADM in specified risk-based contexts and carried out by an AI system, such as in the workplace or when used for social scoring. Certain profiling and ADM activities conducted by means of an AI system are prohibited or high-risk, including in the workplace or in the context of credit-scoring.

Prohibited AI practices, listed in Article 5 EU AI Act, can catch some types of ADM, including in particular 'social scoring' (Article 5(c)), which means the evaluation or classification of natural persons or groups based on their social behaviour or personality characteristics, resulting in unjustified detrimental treatment. Social scoring is prohibited where data is reused in a different, unrelated context, or where the resulting detrimental treatment is unjustified or disproportionate. Recent guidelines of the EU Commission on prohibited AI practices[1] emphasise the need for businesses to put in place processes to monitor for prohibited practices continuously throughout an AI system's lifecycle, and for AI system providers to build safeguards to prevent systems being misused, including where misuse is reasonably foreseeable.

Effectively, this means businesses in the EU must read both GDPR and the EU AI Act together to understand the compliance obligations that apply to any given ADM process and must create a combined governance approach that meets the requirements of both sets of laws. Both GDPR and the EU AI Act require organisations to take a broad view of compliance (including the requirement for security and data protection by design), taking into account the context of an application's deployment and the related risks to individuals, as well as the organisation's management of risks. Often, AI systems use personal data in an integrated way throughout a system's lifecycle, so GDPR will generally be applicable.

Rights to a meaningful explanation

The EU AI Act provides a right of explanation to any person affected by a decision taken on the basis of an output from a high-risk AI system which produces legal or significant effects (Article 86, EU AI Act). This article grants a right to obtain clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken. Pursuant to Article 86(3) EU AI Act, however, where GDPR or other EU laws already provide a right to explanation for fully automated systems, this right does not apply. This has given rise to questions about the exact boundaries between Article 15 GDPR and EU AI Act rights.

In a recent case of the European Court of Justice ('**CJEU**'), *Dun & Bradstreet Austria* (C-203/22, 5 March 2025),[2] the CJEU considered the extent of obligation to provide a meaningful explanation about the logic involved

in automated processing under Article 15(1)(h) GDPR. The case concerned credit-scoring (in future, also a high-risk AI system under the EU AI Act rules) and was based on an application from an Austrian citizen who had been refused a mobile phone contract for 10 euros per month, despite otherwise seeming to have a good credit record. The Viennese Administrative Court referred detailed questions to the CJEU for a ruling to determine what information had to be disclosed to explain how the credit-scoring system reached its decision, and the court also asked the CJEU to consider whether GDPR requires disclosure of all relevant information, including an exhaustive explanation of the whole process leading to a decision.

The CJEU focused on the aim of Article 15(1)(h), which is to allow a person to understand and challenge an automated decision, and clarified that neither the mere communication of a complex mathematical formula or algorithm, nor the detailed description of an ADM process, would satisfy these requirements, as neither is a sufficiently precise and understandable explanation.

The court clarified that data controllers must provide individuals with a concise, transparent, intelligible and easily accessible explanation of the logic involved and the principles that have been applied to the automated processing of personal data for the purpose of obtaining a specific result.[3] The explanation must describe the procedure and principles actually applied in such a way that the data subject can understand which of their personal data have been used in what way in the ADM at issue. Complexity does not relieve the controller of the duty to provide an explanation.

In response to the *Dun & Bradstreet* judgment, the Austrian Data Protection Regulator wrote to the WKÖ (the industry association for financial service providers) to emphasise that the decision means there is a high standard for the provision of information about credit scoring (and ADM generally).[4] The Regulator provided further guidance that:

- a general description of credit-scoring procedures and principles probably does not suffice to comply with GDPR disclosure obligations: information must relate specifically to the individual's case; and
- this could include the extent to which a difference in the personal data taken into account would have led to a different result.

Collision of laws

The *Dun & Bradstreet* decision provides some measure of clarity over the nature of explanation needed in respect of algorithmic decision-making, but there remains a complex and nuanced process for businesses and individuals to understand which legal rights apply in respect of an ADM system. Businesses will also need to consider whether controller–processor relationships align with control over AI systems, where provider-deployer roles may not necessarily match GDPR responsibilities. Where there are gaps, organisations may need to add contractual requirements for system providers or deployers to supply the information necessary to meet Article 15 requirements for explanation.

Alongside the EU AI Act and GDPR, a range of other laws also provide individual rights to explanation, including Article 18(8) of the Consumer Credit Directive (EU) 2023/2225, which (as implemented by Member States) takes priority over the EU AI Act, but defers to GDPR where applicable.

Further laws requiring transparency also apply in other contexts, for instance, Article 76 of the Money Laundering Regulation 2024/1624 provides a right of explanation in respect of automated know-your-customer decisions.

In addition, broader human rights law questions can also apply, as well as consumer law. This results in a confusing overlap of laws that is challenging for businesses to navigate when seeking to launch innovative new products and services.

Between the EU AI Act and GDPR:

- Article 22 focuses on 'solely automated processing', leaving gaps where a system relies partly on ADM, partly on human oversight.

- By contrast, the EU AI Act's product liability focus permits a more comprehensive regulatory approach, focusing on ensuring effective human oversight, and setting detailed procedural, governance and technical requirements for systems classified as higher risk.
- The AI Act only applies where there is an AI system, but GDPR can potentially apply to traditional software systems too (e.g. Case C-634/21 *SCHUFA Holding*, concerning the application of Article 22 GDPR to a decision reached using a probability value).

Notwithstanding the proliferation of laws relating to ADM and profiling, there remains an overall gap in protection for individuals where an ADM system is not high-risk, nor performing a prohibited practice, and yet creates substantial legal effects without reliance on personal data, ADM or profiling.

An example of this is where software outputs are used in the context of criminal evidence. In this context, individuals may be deeply affected by the output of software and AI systems, even where their personal data is not used. The UK Ministry of Justice is conducting a Call for Evidence[5] on the use of evidence generated by software in criminal proceedings. This focuses on the common law rebuttable presumption, operative in criminal prosecutions, that computers producing evidence were operating correctly at the material time, i.e. that '*the computer is always right*' unless someone can show otherwise. The Ministry of Justice notes that 'computer evidence' proliferates in many prosecutions, in particular for crimes such as fraud, rape and serious sexual offences. In *R v Hamilton and others* [2021] EWCA Crim 577, the Court of Appeal suggested that this presumption that a computer was operating correctly was at the heart of the failure of the Post Office, as prosecutor, to disclose evidence regarding the defective Horizon computer system, resulting in multiple miscarriages of justice, with catastrophic outcomes for individuals affected. Horizon was just an accounting program, and rights in respect of personal data processing could not have offered any solution to this issue.

UK–EU divergence?

It is interesting to compare the UK approach with the EU, as the UK has not put in place new laws to regulate AI, but instead has taken a principles-based approach, relying on regulators to update their guidance in line with the UK's cross-sectoral principles on AI, as published in the UK's pro-innovation approach to AI regulation whitepaper.[6]

GDPR has nonetheless been to some extent a unifying factor across both EU and UK legal systems, with Article 22 applicable in both contexts. Post-Brexit, the UK retained a frozen UK version of GDPR. In the past, there have been relatively minor interpretive differences between the approach of EU and UK regulators, including on the level of contractual necessity required to justify ADM. However, increasingly data protection regulation may become a further area of difference between the UK and EU approaches, as case law in the EU and guidance of the European Data Protection Board and UK Information Commissioner's Office ("**ICO**") start to diverge over time, and with a new Data (Use and Access) Bill ('**Data Bill**') introduced to Parliament in October 2024. For the UK, this fits into a broader policy focus on streamlining and cutting regulation, as announced on 17 March 2025[7] by the UK Chancellor, with the aim of saving businesses' costs and fast-tracking innovation. All of this also, of course, takes place against the backdrop of the EU–UK data adequacy decision, which is now pushed back to the end of 2025, for assessment once the UK's legislative process on the Data Bill concludes.[8]

The Data Bill puts forward updates to data law – both personal and industrial – across a range of areas, including smart infrastructure, digital identity, personal data portability and updates to the law on ADM and the enforcement powers of the UK Information Commissioner. The Bill aims to reduce the compliance cost for businesses associated with AI and machine learning, and will also provide a framework for the secure and effective use of data, touching on a broad range of digital society questions, including:

- provision about services consisting of the use of information to ascertain and verify facts about individuals;

- privacy and electronic communication;
- retention of biometric data; and
- electronic signatures, seals and trust services.

There will also be new smart data schemes that give people the ability to obtain and reuse their personal data.

Part 5 of the Data Bill concerns data protection and privacy and amends data protection laws, including reform of provisions relating to ADM, and also proposes some changes to the data protection regulator's enforcement powers.

In this respect, proposed amendments under the Data Bill[9] seek to narrow the legal restraints on ADM, imposing restrictions only where there is processing of special categories of personal data. This will mean that organisations can put in place systems that reach significant decisions regarding an individual (including where there is no meaningful human involvement) without explicit consent, based on the organisation's legitimate interests.

Processing will still need to be subject to the general principles of fairness and transparency, so organisations will have to show that, where there is reliance on the legitimate interests' lawful basis for processing, their interests are not outweighed by the impact on the rights and freedoms of individuals whose data is being processed. In response to this proposal, the ICO has welcomed the additional protection for special category data and the role of 'meaningful human involvement' in the provisions, but has noted concerns about the potential risks of solely ADM and stakeholder views that the general restriction is an important safeguard to keep.

The ICO has also been tasked with preparing a new Code of Practice on solely ADM following passage of the Data Bill.[10]

Holistic approach to ADM regulation

It is unsurprising that laws governing ADM are changing at present, given the emergence of new capabilities and the fast pace of business innovation. The wider geopolitical landscape also plays an important role in shaping the balance between different stakeholders' rights and interests, and therefore between risk and innovation.

In the UK and EU, recent legislative proposals provide some clarity over likely regulatory developments for transparency of ADM systems. However, there are many gaps and questions remaining, which may well be filled though challenge and litigation. This raises implementation challenges for businesses, who will wish to build products around any required technical safeguards, and for individuals, who do not necessarily have the time or resource to bring a challenge. Individuals also do not always know that their data is being used, which can leave an unlevel playing field.

There are also many questions to solve around the effectiveness of human oversight, as the Brussels Privacy Hub has recently said: "*Human intervention alone is not sufficient to achieve appropriate human oversight for AI systems. Human intervention does not work without human governance.*" (Brussels Privacy Hub, Working Paper Vol.8, No32, December 2022.)

As algorithmic decision-making becomes a more fundamental part of our increasingly digital society and economy, a more holistic and joined-up approach is needed in order to cut down on complex legal collisions and ensure that regulation translates effectively into technical standards, processes and safer products. This needs to also allow people a clear and effective right to explanation and challenge in the event issues arise.

Endnotes

1 Guidelines of the EU Commission on Prohibited AI Practices (4 February 2025).

2 *Dun & Bradstreet Austria*, 5 March 2025, https://curia.europa.eu/juris/liste.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-203%252F22&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&a

3 Para. 66.

4 Letter of the *Datenschutzbehörde* to WKÖ of 11 March 2025: https://dsb.gv.at/sites/site0344/media/downloads/dsb_rundschreiben_11.3.2025.pdf

5 Use of evidence generated by software in criminal proceedings: Call for Evidence (Ministry of Justice, 21 January 2025) https://www.gov.uk/government/calls-for-evidence/use-of-evidence-generated-by-software-in-criminal-proceedings/use-of-evidence-generated-by-software-in-criminal-proceedings-call-for-evidence

6 https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

7 Radical plan to cut red tape and kickstart growth: https://www.gov.uk/government/news/radical-action-plan-to-cut-red-tape-and-kickstart-growth

8 Commission proposes to extend adequacy decisions for the UK to 27 December 2025: https://ec.europa.eu/commission/presscorner/detail/en/mex_25_812

9 Article 80 Data (Use and Access) Bill: https://publications.parliament.uk/pa/bills/cbill/59-01/0199/240199.pdf

10 https://ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-updated-response-to-the-data-use-and-access-dua-bill-house-of-commons

Lisa McClory

Tel: +44 207 367 3000 / Email: lisa.mcclory@cms-cmno.com

Lisa is Of Counsel in the fintech team at CMS, specialising in the law of advanced data systems and emerging technology, including AI, crypto, robotics, smart infrastructure, cyber-physical systems and regulation of open-source and decentralised computing systems.

Lisa has a multi-specialist practice as a Lawyer and Technologist, with particular focus on helping businesses find practical, strategic answers to the interpretation and implementation of global emerging tech regulation. She is also Chair of the Digital Assets Subcommittee of the Law Society of England and Wales and an Honorary Reader in the School of Law at Queen Mary University of London.

CMS LLP

Cannon Place, 78 Cannon Street, London EC4N 6AF, United Kingdom

Tel: +44 207 367 3000 / URL: www.cms.law

Global Legal Insights – AI, Machine Learning & Big Data provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Trends
- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

globallegalinsights.com