SHOOSMITHS

Humans in the lead

Data protection law and the current legal landscape in respect of human oversight into automated decision-making (ADM)

JANUARY 2026 | Report for London Councils

FOR WHAT MATTERS

Report for London Councils:

Humans in the Lead: data protection law and the current legal landscape in respect of human oversight into automated decision-making (ADM).

1 Executive summary and key points

1.1 The UK GDPR and Data Protection Act 2018 govern the use of personal data in automated decision-making (**ADM**) in the UK.

1.2 Human review plays two key roles: first, in determining whether a decision is "solely automated", and second, as a compliance task under data protection law.

1.3 ADM is separately regulated under Article 22 of the UK GDPR when it is "solely automated" and has legal or similarly significant effects on individuals. Such decision-making carries rights to obtain human intervention, express views, and contest the decision.

1.4 In many cases ADM falling outside Article 22 will be subject to human review and transparency obligations, whether arising under wider data protection law or other frameworks applicable to the public sector.

1.5 Human review must be more than a token gesture and should be timely, meaningful, and competent.

1.6 The Data (Use and Access) Act 2025 (**DUAA**) will relax Article 22 restrictions except where special category data is used, allowing fully automated decision-making for important public interest tasks in the UK.

1.7 However, controllers must provide clear, intelligible explanations of the logic and consequences of decision-making under Article 22, which may be a barrier to widespread adoption of this new freedom.

1.8 All ADM must comply with wider data protection principles, and equalities and administrative law.

1.9 ADM and artificial intelligence (**AI**) are different concepts though they often overlap. While the UK has no AI Act, the government has issued important guidance for the public sector on the use of AI which is relevant to ADM and considers the role of human review.

1.10 Controllers making automated decisions using personal data should monitor implementation of the DUAA, ICO guidance, and related case law to ensure processes remain compliant as the legal landscape relating to human review evolves.

2 Background

2.1 Explanation of basic concepts and how they are addressed in UK data protection law

2.1.1 The main **data protection laws** are the UK General Data Protection Regulation[1] (**UK GDPR**) and the Data Protection Act 2018 (**DPA 2018).** Data protection law is about individual rights to the protection of personal data. This is a somewhat flexible concept but can broadly be defined as information about an identified or identifiable living person. Such a person is called a "data subject".

2.1.2 The information must be recorded in some way: in the public sector context, data protection law is concerned with the handling of any kind of record, whether in digital or manual form, and whether "filed" systematically or not. Mere thoughts, ideas or unrecorded speech are not generally in scope.

2.1.3 Data protection law imposes obligations on handlers of personal data. Obligations largely fall on data "controllers": broadly, those making key decisions about why and how the information is handled. A data "processor" is a separate organisation used by a controller to carry out operational processing on their behalf, for example a cloud services provider. The law is concerned with how both these kinds of operator "process" personal data. The concept of processing is extremely wide and covers, for example, storing and consulting information as well as amending or sharing it.

2.1.4 This report only concerns the UK GDPR and does not consider the regimes governing personal data use in Part 3 and Part 4 of the DPA 2018 which apply to competent authorities for law enforcement purposes and intelligence services.

2.2 Outline of UK data protection law and the role of ADM within it; ADM distinguished from AI

2.2.1 "Automated decision-making" (**ADM**) is specifically addressed in UK data protection law. The UK GDPR contains prohibitions and safeguards designed to protect people from the uncontrolled or invisible effects of certain sorts of ADM. It also grants rights to people who are subject to it.

2.2.2 UK data protection law has no concept of "Artificial Intelligence" as such. The law developed from concerns in the early 1990s about the increased use of digital tools to record information about people, and the rise of the public internet, and pre-dates widespread access to AI capability.

2.2.3 Decision-making is one possible use of an AI system, but there are many others, such as data analysis, pattern recognition and translation. Not all uses of AI will therefore be covered by the rules about ADM in data protection law. It is also possible that ADM can take place without the use of AI: for example, credit scoring based on digital profiling in ways developed without access to general purpose AI systems.

2.2.4 It is therefore important to consider, for any use case, whether the processing involves personal data, and if so, whether it involves ADM.

2.3 Discussion of ADM meaning and scope under UK law

[1] Strictly, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance) (Retained EU Legislation)

2.3.1 The UK GDPR covers a subset of ADM, which is "a decision based **solely** on automated processing, including profiling, **which produces legal effects** concerning him or her **or similarly significantly affects** him or her" (bold added).

2.3.2 The meaning of "automated processing" is not further defined but covers a wide range of activities in the digital sphere.

2.3.3 The UK GDPR is concerned with "automated processing, including profiling". "Profiling" is defined as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.'

2.3.4 Strictly, profiling is the stage **before** decision-making: the output of profiling is used to inform a decision. ADM with significant effects on a person may be seen as a three-stage process: processing of personal data, profiling, and decision-making.

2.4 The meaning of "solely automated" and "significantly affects"

2.4.1 Data protection laws specific to ADM are only concerned with "solely" automated processing of personal data. Recital 71 of the UK GDPR defines "solely" as meaning "without any human intervention" (noting that recitals are indicative only both under EU and UK law).

2.4.2 The Article 29 Working Party guidelines on automated decision-making for the purposes of the EU GDPR[2] suggest that a decision will be 'based solely on automated processing' unless the level of human intervention 'is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision'.

2.4.3 Recent EU case law from Austria[3] has suggested some relevant factors when considering the scope of "solely" automated processing. The controls which the court found mitigated against "solely" automated processing included training advisers on independent assessment, routine human scrutiny of results, record keeping, discussion of outcomes with data subjects, the right to independent review, and moderation of decisions taken.

2.4.4 Whether a decision will have a legal effect on a person or "similarly significantly affect" them is a question of fact, though the law gives some guidance. A **legal** effect would include a decision whether to allocate public resources such as welfare benefits or housing. A **significant** effect is more difficult to define. Most targeted advertising is out of scope, as buying decisions are unlikely to have a significant effect on a person, although choosing pharmaceutical products might fall within the definition. Recent European Data Protection Board (EDPB) guidance, which still influences UK data protection law, has confirmed that recommender systems on social media may have a significant effect given increasing evidence of harms, particularly to children.

2.4.5 In this discussion, ADM which comes within Article 22 of the UK GDPR by (a) being based on personal data, (ii) being "solely automated" and (iii) having the requisite significant effect, is called "**SS-ADM**" to distinguish it from other forms of ADM which are not regulated in this way.

---

[2] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (WP29 guidelines, later adopted by the European Data Protection Board)

[3] Decision

3 Foundational ADM rights under the UK GDPR

3.1 Article 22 of the UK GDPR

3.1.1 Article 22 of the UK GDPR puts conditions on carrying out SS-ADM.

3.1.2 The conditions in Article 22 require that SS-ADM can only take place if the decision is necessary for entering into or performing a **contract** between the data subject and the controller; is required or authorised by UK **law** and includes necessary safeguards; or is carried out with the data subject's **consent**.

3.1.3 SS-ADM based on special category data[4] can only be carried out with consent, or in the 'substantial public interest': in practice this means for one of the reasons, and subject to conditions, set out in the DPA 2018.

3.2 Rights to an explanation

3.2.1 Articles 13, 14 and 15 of the UK GDPR impose additional notice and information requirements on controllers when SS-ADM is taking place.

3.2.2 The controller must provide the data subject with 'meaningful information about the logic involved' in the decision-making, as well as the 'significance and the envisaged consequences of such processing for the data subject'. This information must be provided when data is collected from an individual, or within the time limits in Article 14 when data is collected from a third party. If the data subject makes a rights request, the information must be provided within the applicable time period, usually within one month of the request.

3.2.3 According to the Information Commissioner's Office (**ICO**), the aim of this exercise is to give individuals the necessary context in which they can assess the decision-making, and any subsequent human review of the decision.

3.3 Rights to human review

3.3.1 Rights to human review apply directly to SS-ADM under Article 22 and indirectly to any processing carried out under Article 6(1)(e), the lawful basis applicable to a public interest task.

3.3.2 SS-ADM under Article 22 carries an express right to "obtain human intervention on the part of the controller", to express their point of view and to contest the decision. This applies to decision-making under any of the three permitted conditions[5].

3.3.3 Any processing of personal data by a public authority carried out on the basis of a public interest task under Article 6(1)(e), which may include processing involved in ADM, carries a general right to object, set out in Article 21. This right must be brought to the attention of the affected individual. On objection, a controller must stop the relevant processing unless it can demonstrate "compelling legitimate grounds" for the processing which override data subject rights (or if the processing is for the conduct of legal claims).

3.3.4 This means that in many cases ADM falling outside Article 22 will be subject to human review in practice. On objection, a controller must establish whether the required threshold (for compelling legitimate grounds) is reached allowing it to

---

[4] 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (Art. 9(1) UK GDPR)

[5] Decision-making required or authorised by domestic law has provisions equivalent to Art. 22 of the UK GDPR in s. 14 of the DPA 2018.

continue the processing. This entails human review, at least of the purposes and nature of the decision-making practice, if not of the individual decision at issue.

3.3.5 A similar analysis can be made of processing carried out in the private sector on the basis of legitimate interests under Article 6(1)(f).

3.3.6 In the same way, it can be argued that the provision of transparency information must in practice entail some human oversight, particularly where there is an obligation to give reasons in intelligible form.

3.3.7 That said, because of the basic prohibition on SS-ADM, controllers currently have an incentive to ensure that their processing falls outside Article 22. One important way to do this is to design systems to ensure there is a significant element of human involvement as part of the decision-making process, for example using the techniques listed at 2.4.3 above.

3.4 Consequences of non-compliance

3.4.1 Any infringement of the UK GDPR, including for failures in relation to SS-ADM, will allow a data subject to **complain** to the regulator (the ICO), and give rise to a right of **compensation** from the infringing controller or processor where there is some form of damage. Controllers in breach of the UK GDPR may be **fined** by the ICO either themselves or through failure to supervise a processor acting on their behalf.

3.4.2 Infringement may also give rise to **contractual liability** for example where compliance with applicable data protection laws is an enforceable contract term. Non-compliance with data protection laws can also give rise to a **breach of statutory duty**.

4 Legal reform

4.1 Proposed changes to Article 22 under the Data (Use and Access) Act 2025

4.1.1 UK data protection laws are undergoing a process of amendment since the Data (Use and Access) Act 2025 (the DUAA) received Royal Assent on 19 June 2025. Some changes are already in effect with others due to be made at an unspecified future date; likely to be in early 2026. At the same time the ICO is consulting on changes to its relevant guidance[6].

4.2 Scope of "solely automated"; changes to prohibitions and conditions

4.2.1 Under the DUAA, Article 22 of the UK GDPR will be amended. The conditions on SS-ADM explained at 3.1.2 above will only apply to decision-making based on special category data. The most significant effect of this change is that SS-ADM **not** using special category data may be carried out relying on any applicable lawful basis.

4.2.2 In the public sector, the DUAA provides additional opportunities to apply SS-ADM when carrying out personal data processing necessary for a public interest task under Article 6(1)(e). This means that incentives to ensure the process falls outside the Article 22 prohibition, discussed at 3.3.7 above, will no longer hold. Arguably, the "human in the loop" will remain key for post-decision-making review and transparency but will not necessarily need to be baked into pre-decision-making stages to ensure lawfulness.

4.2.3 Key additional opportunities for controllers in the private sector will be processing necessary for an organisation's legitimate interests, where these provide a lawful

[6] Automated decision-making and profiling | ICO

basis under Article 6(1)(f). One limitation to this freedom is that controllers will not be able to rely on the new "recognised legitimate interests" to carry out SS-ADM. These are made available in new Article 6(1)(ea) to private sector controllers who are carrying out a specified public interest task, such as sharing personal data with a public authority, or processing for the purposes of safeguarding or crime prevention.

4.2.4 When using special category data the new freedoms will not apply, and controllers will need to consider whether the safest course is to ensure processing falls outside the Article 22 prohibition through meaningful human involvement at the pre-decision stage. Controllers should note that historically, ADM using special category data has proved contentious. In 2022, the ICO fined a private sector controller[7] for unconsented use of sensitive health data in connection with profiling.

4.2.5 The safeguards described at 3.3.2 above will continue to apply to all SS-ADM, regardless of whether it is based on special category data.

4.2.6 New Article 22A of the UK GDPR will specify that a decision is based solely on automated processing if there is no "meaningful human involvement" in the taking of the decision. Consideration must be given, among other things, to whether the decision is reached by means of profiling. The Secretary of State will have power to identify activities deemed to come within or outside the definition.

4.2.7 Article 22A does not materially change the law concerning whether ADM is "significant". Again, the Secretary of State will have power to deem activities within or outside the definition. This will give the UK government power to greenlight different types of processing.

4.2.8 It will be important for public authorities processing under the UK GDPR to keep up to date with such determinations on particular types of processing made under Article 22A. Draft ICO guidance on ADM and profiling was due to be issued for consultation in Autumn 2025, although it has apparently been delayed. When issued, this will be an important guide for controllers navigating the new freedoms with respect to ADM.

4.2.9 Human review exercised as a result of the right to object in Article 21, discussed at 3.3.3 to 3.3.5 above, will not be affected by the DUAA.

4.3 Short overview of other possible changes to UK law

4.3.1 Outside specific technologies such as automated vehicles, the UK government has not passed bespoke laws on AI. In 2023, it introduced an AI White Paper containing cross-sectoral principles for regulators to use in future AI regulation. In 2025, the current government introduced its AI Opportunities Action Plan containing policy initiatives designed to promote the development and use of AI in the UK. Neither of these contain changes to the law affecting ADM.

4.3.2 Several non-government bills concerning AI have been introduced including the Public Authority Algorithmic and Automated Decision-Making Systems Bill[8] which originated in the House of Lords. It aims to mitigate the risks of the use of AI in the public sector, including by obliging public authorities deploying an AI system to publish a prior risk assessment and algorithmic transparency record, auto-generate logs, ensure that final decision-makers can challenge the system's output, maintain a public register of AI-enabled decisions, and only use systems capable of scrutiny.

---

[7] ICO reaches agreement with Easylife Ltd | ICO

[8] Public Authority Algorithmic and Automated Decision-Making Systems Bill [HL] - Parliamentary Bills - UK Parliament

It passed through the Lords in February 2025 but has not yet been tabled for a first reading in the Commons and is unlikely to progress without government support.

4.3.3 The government has signalled possible future legislation on foundation models, and a watching brief on the need to legislate on specific aspects of AI development and deployment. The current direction of travel appears to be selective lifting of current rules to enable innovative AI deployment, for example in its recent Blueprint for AI Regulation[9] which opens a consultation on testing AI capability in controlled environments.

5 Practical issues and difficulties

5.1 Analysis against London Office of Technology & Innovation (LOTI) submitted use cases

5.1.1 LOTI submitted four example situations where member councils might be considering the role of human review:

(a) An officer giving feedback to an AI model in a training stage to improve its performance (e.g. make better predictions)

(i) This activity does not directly invoke Article 22. If the review activity involves processing personal data then it will be subject to the general compliance principles in the UK GDPR outlined at 7.1. Improved performance should help ease data protection and other compliance risks associated with ADM used in individual cases. Careful record keeping will help to satisfy transparency and review obligations arising under the UK GDPR or otherwise, for example under the Freedom of Information Act.

(b) Officers/an organisation deciding at a governance level (e.g. through a governance board or a procurement process) what AI tools to use

(i) The same considerations apply. Officers should be aware of the obligation in Article 32 to ensure secure and state of the art technical and organisational measures in order to prevent personal data breach, and duties to supervise data processors in Article 28, which are outside the scope of this report.

(c) An officer, usually involved in the service delivery process, reviewing outputs from an AI model and correcting their errors. This has been termed a Practical Decision Maker

(i) If this activity concerns individual decision-making, then it will potentially invoke Article 22. Officers should consider whether the underlying outputs constitute SS-ADM and if so whether compliance with Article 22 has been achieved. Once the relevant part of the DUAA is in effect, they should be aware of the importance of identifying whether the decision is based on special category data or not, since this will determine the lawfulness of the activity and likely available lawful basis (see 4.2.1 to 4.2.6 above).

(d) A resident providing feedback to the council that an AI output (or decision) is incorrect or inaccurate, which may then be acted on by the council in some way

(i) For this individual, a council should identify whether the feedback constitutes a request for review or an objection, either under Article 22 (for SS-ADM) or Article 6 (for other ADM - see 3.3.2 to 3.3.4). This will enable councils to understand the actions required of the controller.

5.1.2 For each of these scenarios, there will be important considerations outside data protection law. Some of these are considered in paragraphs 6, 7.1 and 7.2.

5.2 Joint controllers

[9] New blueprint for AI regulation could speed up planning approvals, slash NHS waiting times, and drive growth and public trust - GOV.UK

5.2.1 Identifying processing roles in the context of automated decision-making is difficult, particularly where it involves AI. Ideally, every collaborative venture or procurement process would involve consideration of controller and processor roles, including joint controllership. This occurs, broadly, where two or more controllers are processing the same personal data for the same purposes.

5.2.2 The ICO has published preliminary views [10] on how to address this in the context of AI, although developed guidance is awaited. In January 2026 it issued a report on agentic AI which has high-level consideration of the role of human review[11].

5.2.3 An important principle developed in EU case law is that responsibility for automated decision-making cannot be avoided by arguing that technical parts of the decision-making have been subcontracted to a third party, with the final "decision" resting with a separate controller. This argument has been invoked to bypass rules on SS-ADM in the context of decisions based on credit scoring.

5.2.4 The European court increasingly identifies joint controllership as a solution to complex digital ecosystems. Although not technically binding, UK courts continue to take account of European data protection law and guidance.

5.2.5 Overall, this suggests that controllers carrying out decision-making using third party tools must accept compliance responsibility and must be prepared to act as joint controllers – with the required written agreement on individual responsibilities, and joint accountability for satisfying data subject rights - where they cannot clearly separate roles.

5.3 **Children and the vulnerable**

5.3.1 The DUAA will impose a duty on certain controllers to have regard to children's "higher protection matters". This is aimed at commercial, online providers and will not apply to most public sector activities.

5.3.2 Recital 71 of the UK GDPR notes that children should not be subject to SS-ADM. Although not legally binding, this will make it especially difficult to justify the use of SS-ADM for children. It has not been interpreted as an absolute prohibition by regulators but should be the exception and should only be considered where controllers can demonstrate that its use is in the best interests of the child.

5.3.3 The threshold for what constitutes a "significant" decision will depend on the nature of the affected individual[12]. Decisions which disproportionately affect vulnerable groups are more likely generally to be legally significant.

5.4 **Extent of explanations required and the black box problem**

5.4.1 The European court has considered the extent of explanations legally required to satisfy the transparency obligations which attach to SS-ADM set out at 3.2.2. In February 2025, the Court of Justice of the European Union issued its preliminary ruling in a case[13] referred from the Austrian court about explaining credit scoring decisions. It found that the controller must be able to "explain, by means of relevant information and in a concise, transparent, intelligible and easily accessible form, the

[10] What are the accountability and governance implications of AI? | ICO

[11] ICO tech futures: Agentic AI | ICO

[12] see WP29 guidelines at page 22

[13] CURIA - Documents

procedure and principles actually applied". As an EU case it will not be binding, but will be persuasive, to the UK court's interpretation of the UK GDPR.

5.4.2 The DUAA will slightly expand current Article 22 of the UK GDPR[14] to clarify that the right to human review will be to "obtain human intervention on the part of the controller **in relation to such decisions**". Whether this will mean anything different from the current law (which omits the words in bold) should be clarified in ICO guidance, and any case law which emerges. It highlights that the right to human review is to any aspect of the decision-making process, not just the outcome.

5.4.3 The UK GDPR grants rights to "obtain human intervention" and to "contest the decision" where SS-ADM is carried out. This raises the question of whether this is a right to have the decision re-made by a human, or whether re-running an automated decision process using human-reviewed parameters would satisfy the requirement. Again, guidance and case law are needed to clarify these aspects as automated decision-making becomes more common.

5.4.4 There is widespread acceptance that AI-powered automated decision-making processes are not truly explicable, even to those developing the models on which they rest. The problem of explainability is already acute and may soon become impractical for human agencies to address. In response to this we may see increased call for human decisions to replace automated ones, rather than attempts to "explain" what a machine has done.

5.4.5 The transparency requirement to provide "meaningful information about the logic involved" in SS-ADM may prove a powerful disincentive to undertaking it.

5.5 **Problems with human decision-making: timing, quality and risk**

5.5.1 As explained, the biggest change for the public sector will be new possibilities to carry out SS-ADM to carry out public tasks without consent. The human in the loop can (at least in theory, and from a data protection point of view) more easily step back from actual decision-making, although they must remain ready to carry out review on request and fulfil their transparency obligations.

5.5.2 Many commentators have noted that human oversight carries its own risks. This might be viewed as falling outside data protection law, which strictly is concerned only with the protection and dissemination of digital information. However, the UK GDPR does concern the quality of measures taken by human beings to protect digital data, and enforcement is regularly concerned with human error in processes. This suggests that organisations have an active duty to train and quality assess human reviewers to satisfy the requirements of Article 22. Even if a flawed human review may technically satisfy Article 22 requirements, it is unlikely to satisfy broader obligations of accountability in the legislation. This also suggests that it must also consist of more than a rubber stamp (as also confirmed in European case law). The Dutch data protection authority has issued some practical guidance on managing human review[15] which considers some of these issues further.

5.5.3 Although outside this report, there are also important considerations about protecting human reviewers involved in overseeing harmful content as part of review duties.

5.5.4 A human review must come **after** the decision in question in order to be useful. The ICO says[16] that "in most cases, for human review to be meaningful, human

[14] in new Article 22C(2)(c)

[15] Meaningful human intervention in algorithmic decision-making | Dutch Data Protection Authority

[16] What is the impact of Article 22 of the UK GDPR on fairness? | ICO

involvement should come after the automated decision has taken place and it must relate to the actual outcome". This ICO analysis contains useful consideration of the timing of human review, based on the principle that the first step is to identify the key decision in question, which will determine the timing and role of human review.

5.5.5 This analysis confirms that when a human determines input data this does not change the essential nature of an automated decision, as the **result** is still automated. Input data is an important consideration in practice but is separate and will not take solely automated decision-making into ordinary ADM (see 5.1.1.(a) above).

5.5.6 In time, as automated decision-making becomes prevalent, we may see a different trust profile emerge in which machine decision-making is seen as less "flawed" than the human equivalent: perhaps with a right to a "machine review" granted to adjudicate human decisions.

6 AI Playbook

6.1 Brief reminder of how key principles are addressed in the AI Playbook for the UK Government

6.1.1 The Playbook[17] is a short, voluntary guide last updated in February 2025 with ten principles "which civil servants should uphold when using AI". "It explains what AI is – including its capabilities, limitations and risks – and how to select, buy and deploy AI in government".

6.1.2 The Playbook makes the following recommendations on human oversight in various contexts:

(a) A general prohibition on fully automated decision-making for significant decisions: "Use cases to avoid. Given the current limitations of AI, and their ethical, legal and social implications, there are use cases that are not appropriate and which should be avoided in the public sector. These include […] fully automated decision making: be cautious about any use case involving significant decisions, such as those involving someone's health or safety".

(b) Establishing a human review process for high-impact scenarios: "Where AI is used in situations of high impact or risk, establish a human-in-the-loop process to oversee and validate outputs and decisions. Make sure that these people can effectively identify risks and intervene, where appropriate".

(c) Ensuring GDPR compliance: "Although it is possible to use AI systems for automated decision making where the system makes a decision automatically without any human involvement, this may infringe the UK GDPR. Article 22 currently prohibits decision(s) based solely on automated processing that have legal or similarly significant consequences for individuals. Services using AI that affect a person's legal status or their legal rights must only use AI to support decisions that must be made by a human decision maker".

(d) How to design human oversight processes: "AI systems need to introduce deliberation processes into all stages of the life cycle so that the abilities of humans and machines are combined to reach the best results when performing tasks. However, the human input needs to be 'meaningful'.

[17] AI Playbook for the UK Government

Several factors determine how much human involvement there should be in AI systems, such as the complexity of the output, its potential impact, and the amount of specialist human knowledge (for example, legal and medical) required".

(e) The importance of human oversight for irreversible actions, such as using generative AI outputs: "Prevent generative AI responses automatically leading to destructive or irreversible actions, such as sending emails or modifying records. In these situations a human must be present to review the action".

(f) Taking special care over autonomous AI services that make decisions in social care or healthcare: "The impact of autonomy of an AI service can be mitigated by including human intervention. These decisions need to be made in a controlled environment so as to not reintroduce bias into the AI service. Whether your AI service is autonomous or includes elements of human intervention, it should be evaluated throughout […] all stages of the project life cycle – including design, development and operation. Your risks and mitigation strategy should also cover how your team will manage continuous performance monitoring to prevent biased or inaccurate outputs".

6.1.3 Human review processes for the use of generative AI are also considered in the Generative AI framework for HM Government[18].

6.1.4 The Alan Turing Institute has produced guides on transparency[19], and ethics and safety[20], which are likely to be helpful when developing practical guidance on designing ADM systems.

6.1.5 In 2023, an ICO blog[21] found no then current concerns in the use of automated decision-making by public bodies for benefits and housing allocation, largely because it detected no ADM being carried out without human involvement. This will change if public sector controllers take advantage of the potential new freedom to carry out SS-ADM without consent for public tasks, enabled by the DUAA.

6.1.6 How SS-ADM may be expanded in the public sector is a policy decision which will rest not just on the legal position but also on political and reputational issues. The experience of the Dutch government - which fell in 2021 because of the perceived discriminatory use of ADM systems to detect benefits fraud - underlines the serious political consequences of losing public trust.

7 The wider context

7.1 Brief reminder of data protection obligations applying to all decision-making

7.1.1 The UK GDPR requires key principles to be respected when carrying out any processing of personal data. Key principles for ADM are lawfulness, minimisation, fairness, accuracy, transparency and purpose limitation. These principles must be embedded into all data protection processes by design. This means that even if, for example, the changes to Article 22 mean that some automated decision-making can

[18] Generative AI framework for UK Government

[19] explaining-decisions-made-with-artificial-intelligence-1-0.pdf

[20] understanding_artificial_intelligence_ethics_and_safety.pdf

[21] Blog: Addressing concerns on the use of AI by local authorities | ICO

be carried out without consent, this could be overridden by the overarching need to ensure fairness and transparency.

7.1.2 The UK GDPR principles are based on being proportionate, so context will be vital. It requires controller accountability, so those carrying out ADM must be able to demonstrate their compliance with the principles, notably through carefully documenting system design, data protection impact assessments (DPIAs), and thorough ongoing record-keeping.

7.1.3 ADM use is very likely to trigger the need for a DPIA[22]. This assessment will help to benchmark the nature of the activity against other UK GDPR requirements including security of processing, data protection by design and default, purpose limitation, retention limitation, accuracy, and lawfulness of processing.

7.2 **Overview of other relevant rights and duties under UK equalities and administrative law**

7.2.1 Actions taken in reliance on ADM will be subject to the non-delegable public sector equality duty in s.149 of the Equalities Act 2010. This was confirmed by the Court of Appeal in 2020[23]: "There is evidence […] that programs for [automated facial recognition] can sometimes have such a bias. […] for reasons of commercial confidentiality, the manufacturer is not prepared to divulge the details so that it could be tested. That may be understandable but, in our view, it does not enable a public authority to discharge its own, non-delegable, duty under section 149".

7.2.2 Duties at common law not to delegate statutory powers, and to follow principles of administrative law in decision-making are likely to have a direct interplay with human review. Other principles of public law may also mandate human review, in particular challenges on the grounds that the quality of decision-making breaches human rights law, and public procurement rules.

7.2.3 The intense difficulty of addressing these problems in the context of increasingly adaptive systems is discussed in a recent Law Commission paper on AI[24].

7.2.4 On the question of transparency, there is not much established case law. There is a likely common law duty of transparency, particularly in relation to the criteria used to determine the legal rights of individuals. There are also probable common law (and applicable statutory) duties to publish policies, and a duty to give reasons, including how a recommendation was considered by a human decision-maker.

7.2.5 The Algorithmic Transparency Recording Standard[25] is a requirement on central (but not yet local) government to log technical reports on algorithms used in public decision-making. Although one of the aims of the Standard is to "drive public understanding and trust" and includes logging "risks relating to the outputs and decisions", the ATRS may not be sufficient or appropriate to guarantee public understanding to the required legal standard. Use of the standard involves balancing openness with intellectual property, confidentiality, and cyber threats, which "could compromise the operational effectiveness of the tool".

7.2.6 In the context of AI-enabled ADM, the UK has not yet imposed a statutory legal mechanism requiring transparency from the AI supply chain along the lines of the

[22] confirmed in Article 35(3) of the UK GDPR, WP29 criteria and ICO guidance

[23] Bridges, R (On the Application Of) v South Wales Police [2020] EWCA Civ 1058 (11 August 2020)

[24] Microsoft Word - 2025-07-29 - Column AI Discussion Paper (v4) from p.19

[25] Algorithmic Transparency Recording Standard Hub - GOV.UK

EU AI Act, so procurers must impose contractual obligations sufficient to enable public bodies to fulfil transparency duties.

7.3 Overview of how the EU AI Act deals with rights to human review in high-risk AI systems and an indication of extra-territorial effect

7.3.1 The EU AI Act[26] is a regulation currently in force and partial effect in EU member states. It will apply to both public and private sector deployment of AI tools across the EU. The provisions on high-risk AI systems will come into effect on 2 August 2026, with a grace period of four years for high-risk AI systems intended to be used by public authorities, which must be compliant by 2 August 2030. It will complement the GDPR, the EU's foundational data protection law which remains similar to the UK GDPR.

7.3.2 High-risk AI systems consist broadly of certain high-risk AI uses including for biometric identification and categorisation, education, services and benefits, critical infrastructure, credit scoring, health and life insurance, employment, law enforcement, border control, and the judiciary. There is also a short list of safety critical products such as AI-enabled lifts, explosives, and toys, which are deemed high-risk.

7.3.3 High-risk AI systems under the EU AI Act are subject to special rules about human decision-making in Article 14. This imposes a proportionate duty to design systems to enable human oversight to prevent or minimise risks to health, safety or fundamental rights. Methods for human oversight may apply both to system providers (broadly, suppliers and manufacturers) and to deployers (users). Systems must enable human reviewers to understand and monitor them, to remain aware of automation bias, to interpret output correctly, to override the system, and to safely stop it operating.

7.3.4 Although both providers and deployers must carry out their obligations, the emphasis is on human oversight being designed into the system by providers. This stems from the fact that the Act is product compliance law which regulates how systems must be designed before being put on the market, rather than a law imposing additional duties in areas regulated separately, such as public sector activity.

7.3.5 High-risk remote biometric identification systems (notably, real time facial recognition systems) also require that identification must be subject to independent review by two competent people before being used to take decisions of any kind.

7.3.6 The existence and timing of human input is an important factor in considering whether an AI system is high risk. There is scope for automated processes to perform preparatory tasks, check, and improve human-led decisions in high-risk areas without becoming subject to the rules affecting high-risk systems.

7.3.7 The Act imposes duties on the public sector to carry out a "Fundamental Rights Impact Assessment" of some high-risk deployments and this assessment must include an analysis of human oversight involved in the system.

7.3.8 The Act applies to providers and deployers of AI systems located outside the EU "where the output produced by the AI system is used in the Union" (Article 2(1)(c)). While this may catch many private sector entities outside the EU, it is not likely to affect the activities of UK local authorities. However, it will influence future laws, and it will indirectly determine the design of systems made available on non-EU markets

[26] L_202401689EN.000101.fmx.xml

including the UK. We may therefore see AI systems increasingly designed to accommodate human review within their processes.

7.4 Overview of other global jurisdictions: Colorado; South Korea

7.4.1 Non-European jurisdictions are considering bespoke law to regulate AI models and systems.

7.4.2 In the US, there is no prospect of a federal AI law. A patchwork of state laws is beginning to emerge, led by California, Colorado and New York. In general, these laws have a much narrower focus than the EU AI Act and are either sectoral, covering issues such as the deceptive provision of healthcare, or concern a specific issue like recruitment or algorithmic pricing. They include laws covering various aspects of public authority decision-making.

7.4.3 The most developed bespoke AI law is in Colorado, where the state's "Act concerning consumer protections in interactions with AI systems"[27], or "Colorado AI Act", is due to come into effect in August 2026. This applies to the public and private sectors, and controls developers or deployers of high-risk AI systems, defined as those which make or help make "consequential decisions" in housing, insurance, legal services, health care, financial services, public services, employment or education. Duties include appeal rights as well as transparency, labelling, opt-out, and a non-discrimination duty of care.

7.4.4 In December 2025, the White House issued an Executive Order[28] purporting to overrule state legislation on AI development. It is designed to put limits on laws which may hinder AI development and standardise AI regulation at a federal level. It will face significant legal barriers given the limits on US executive power, but the future of state level AI regulation is uncertain for the moment. The White House has also issued instructions to federal agencies putting limits on their use and oversight of AI systems.

7.4.5 In the US, the lack of overarching data protection and AI laws is likely to lead to less transparent adoption of AI capability, including in the public sector. That said, there are still important controls on discriminatory use of AI systems, notably under equalities, employment and consumer law.

7.4.6 The "AI Basic Act" in South Korea is scheduled to take effect on 22 January 2026, with a one-year grace period for enforcement. It covers "high impact" systems in certain sectors including healthcare, energy, biometrics and public services, and various deployments of generative AI. It includes provisions which largely mirror Article 22 of the UK GDPR, requiring AI systems with significant legal effects to allow for human oversight, and carry rights of human review, transparency and challenge.

7.4.7 The Act sits alongside guidelines on automated decision-making issued in September 2024 by the South Korean data protection regulator which broadly reflect provisions in Article 22 of the UK GDPR. Together, these will constitute a similar framework to the EU; South Korea is the second jurisdiction to pass this kind of EU-influenced framework.

7.4.8 Many countries have data protection frameworks strongly influenced by the GDPR which include limitations on automated decision-making. In addition, there are

---

[27] 8ae60739b2b5dac9235add08baebc925 (note this is the bill wording before clean up and codification)

[28] Ensuring a National Policy Framework for Artificial Intelligence – The White House

advanced plans for a comprehensive AI law in Brazil, with Japan and China declaring an intent to legislate in 2026.

Alice Wallbank
SENIOR PROFESSIONAL SUPPORT LAWYER

+44 (0)3700 864 276
+44 (0)7514 731 187
alice.wallbank@shoosmiths.com

FOR
WHAT
MATTERS