



Public
Law
Project

Missing Pieces: Transparency and Accountability in Public Body Automated (and Automated Assisted) Decision Making

Annexes 1 - 3



Annex 1 – Potential Grounds of Challenge (Judicial Review)

This Annex sets out examples of potential grounds of challenge in judicial review and how they may apply in the context of automated (or automated assisted) decision making.

1. Common law grounds of challenge

Ground		Potential application to ADM	Real-world examples
Ultra vires	If a public body has no power to take an action or decision, or has acted beyond its powers (ultra vires), the decision or action will be unlawful.	If a public body does not have the power to use an automated system to make a decision and / or where the applicable legal framework precludes the use of an automated system, the decision to use it will be ultra vires.	<i>Khan Properties Ltd v HMRC [2017] UKFTT 830 (TCC)</i> : the court found that as a matter of statutory interpretation a decision to impose a tax penalty had to be taken by a human.
Failure to follow a published policy	Public bodies are obliged under the common law to follow their published policy guidance unless there is a good reason to depart from it.	If a public body is using an automated decision-making system in a way that is inconsistent with its published policy. For example, if a policy envisages that certain actions will be taken by a human decision maker which are instead taken by the automated system or if a system applies factors in a way that differs from how it is articulated in published policy.	<i>DWP policy on human involvement in decision making</i> : the Department for Work and Pensions applies a policy that it will not use artificial intelligence to replace human judgment to determine or deny a payment to a claimant, and that a final decision in these circumstances will always involve a human agent ¹ . In 2024, the Director General for Work & Pensions indicated that the department had been suspending benefit claims flagged by its model for

¹ DWP, [Personal information charter](#)



			enhanced checking. He stated that this approach had now been changed ² .
Unpublished policy	Public bodies are required to publish policies which either (i) are relied upon to guide their decisions, or (ii) replace or amend their existing policies.	If a public body is relying on an unpublished policy to guide their use of automation in a decision-making context, or which amends its published policies, this may be a breach of a requirement to publish their policy. This could be the case where a public body is relying on an unpublished policy which guides their use of automation and / or which amends or replaces published policy on how decisions are taken. It has also been speculated that where an ADM system utilises reinforcement learning (where the machine learning model learns through ‘trial and error’) it may start to apply an approach that departs from published policy³.	
Failure to give reasons	While there is no general duty to give reasons for decisions, one can be imposed by statute. The courts have also identified a wide range of circumstances where such a duty	A public body that fails to provide reasons for a decision reached using an ADM system may be in breach of a duty to give reasons where one applies. It has been suggested that the particular transparency concerns that apply in relation to some forms of automated decision-making technology, may make it	

² House of Commons Work and Pensions Committee, [Oral evidence: DWP's annual report and accounts 2022-23](#), 10 January 2024, HC417 of session 2023-24

³ Brendan McGurk KC and Joe Tomlinson, *Artificial Intelligence and Public Law*, (1st edn, Hart Publishing, 2025) p. 169



	applies as a matter of common law. Where a duty applies, reasons must be adequate. What adequacy requires will be context dependent, but reasons should facilitate an understanding of what was decided and why and to facilitate an assessment of whether a decision is unlawful.	more likely that courts will imply a duty to give reasons⁴. Depending on the technology used, public bodies may not be able to explain why or how they reached a decision. The field of 'Explainable AI' seeks to develop techniques to understand machine learning outputs. This can include techniques that seek to retrospectively apply reasoning to decisions. As has been noted in extra-judicial writing, courts have been resistant to accepting retrospective rationalising of decisions in a human decision-making context.⁵	
Procedural fairness – duty of transparency	A decision-maker must give those affected by a decision an informed prior opportunity to have a say. As set out above if they use a policy to guide their decision-making, they should generally make	If a decision-maker fails to disclose sufficient information about how an automated system works, this may render the decision procedurally unfair. The extent of disclosure required is likely to depend on what specific role the system plays in the decision-making process.	<i>R (Ames) v Lord Chancellor</i> [2018] EWHC 2250 (Admin), the claimant successfully challenged the Legal Aid Agency's refusal to disclose an algorithm on which it relied to make fee offers on the basis that this breached the duty of transparency and resulted in procedural unfairness.

⁴ McGurk and Tomlinson (2025), n4

⁵ Lord Sales, '[AI and Public Law: Automated Decision-Making in Government](#)', (5 November 2025) Keynote Lecture for the Government Legal Department's Annual Conference



	that policy public, and it should be sufficiently clear to enable those affected to regulate their conduct.		<i>Used Car Importers of Ireland Ltd v Minister for Finance</i> [2020] IECA 298: The government's failure to disclose its algorithm for assessing tax payable on imported used cars was unlawful.
Procedural fairness - right to make representations	Depending on the context, a fair decision-making process may require a public body to give decision subjects an opportunity to make representations before a decision is taken or to contest the decision after it has been taken.	If a public body uses an automated decision-making system, depending on the context, there may be a requirement to provide decision subjects with an opportunity to make representations before or after the decision has been made. As set out above in relation to the duty of transparency for a party to be able to make representations, there is likely to be a corresponding requirements regarding transparency.	<i>2020 A-level algorithm</i>: during the Covid-19 pandemic Government adopted an algorithm to predict A-level results in place of exams. When the results were first announced, the appeal process only facilitated appeals by schools, not pupils, and grades couldn't be challenged on the merits of the algorithm's assessment of the student's academic performance. Pre-action correspondence published by the Good Law Project included grounds of challenge regarding systematic procedural unfairness; that Ofqual was acting in breach of its statutory duty and in breach of s. 29 of the Equality Act 2010. The published letter before claim argued that each of these was exacerbated by the absence of an effective appeal process for the final decision⁶.

⁶ Good Law Project, [Legal action over A-Level results fiasco](#), 16 August 2020



Procedural unfairness – inadequate consultation	In some circumstances public bodies are required to consult with interested parties before making a decision. Such a duty may be imposed explicitly or implicitly by statute or as a matter of common law, for example, where there is a legitimate expectation. If a consultation is undertaken, whether voluntarily or in compliance with a specific duty, it must be carried out in a way that is legal, adequate and fair. For example, proposals should be accompanied by sufficient reasons to enable proper understanding and comment on the proposals.	Where a public body is consulting on how it will make decisions or apply a policy, and part of that approach will involve use of an algorithmic model, there may be a need to disclose sufficient information about the model so as to facilitate informed responses. For example, where an important consideration as part of a consultation is whether a model will be reliable, it may be necessary to publish an executable version of the model to enable testing of its reliability.	<i>R (Eisai Ltd) v National Institute for Health & Clinical Excellence [2008] EQCA Civ 438</i>: The public body's failure to publish an 'executable version' of a model it was proposing to use to assess the cost effectiveness of drugs was found to be procedurally unfair.
--	--	--	---



Error of law	A decision-maker must not materially misunderstand or misapply a hard-edged (as opposed to discretionary) question of law.	If an automated system misapplies a hard-edged question of law, for example by misapplying a statutory test, it will be unlawful. An error of law could also potentially occur where an ADM system treats an element of a legal test as being met on the basis of: a. Incorrect labelling of data at the training stage, or b. Incorrectly treating a fact or set of facts as a proxy for a relevant condition being met⁷.	<i>R (Johnson) v SSWP [2019] EWHC 23 (Admin)</i> in the first instance decision of Johnson, the Court found that the decisions resulting from an automated system for calculating universal credit payments were based on an error of law as they reflected a misinterpretation of the relevant Regulations. This position was overturned on appeal, where the Judge instead found that the method of calculation in the Regulations themselves was irrational and unlawful.
Error of fact	A decision-maker must not make a material error of fact in reaching a decision.	If the outcome produced by an automated system is based on a misunderstanding of or incorrect material fact. This could occur, for example, if the input data used by the algorithm was incorrect (and that input data was material to the decision reached). It could also occur where a self-learning system identified and applied an incorrect correlation between a fact or set of facts and an output⁸.	<i>R (Ames) v Lord Chancellor [2018] EWHC 2250 (Admin)</i> , the court found that there had been significant errors in the data inputted into the algorithm used by the Legal Aid Agency (LAA) to make a legal aid fee offer, and that there had been no reasonable explanation for those errors or for the failure to correct them when drawn to the LAAs attention.
Fettering of discretion	A decision-maker must properly exercise their power, rather than delegating it to someone	If a decision-maker has their decision dictated by an automated system, rather than simply taking advice from the system in reaching their own decision, this may be unlawful.	<i>R (Blundel) v Secretary of State for Work and Pensions [2021] EWHC 608 (Admin)</i> : The government's use of a 'rigid arithmetical formula' to govern the exercise of its discretion

⁷ McGurk and Tomlinson (2025), pp. 171- 172, n3

⁸ McGurk and Tomlinson (2025), pp. 179 – 181, n3



	else or fettering it (e.g. by an inflexible policy).		to deduct money from benefit payments was unlawful.
Relevant & irrelevant considerations	A decision-maker must consider all relevant factors and no irrelevant factors.	Where a statistical system cannot use certain types of information directly (for example, because the information is unavailable or relates to a protected characteristic), it will often use other types of information that are a good proxy. This may raise issues of relevancy, such as where (i) the training data includes irrelevant factors, which are then incorporated into the machine learning model, (ii) the data inputted for decision includes irrelevant factors, or (iii) the algorithm relies on statistical correlations that seem to have no rational basis (for example, a correlation between red hair and suitability for employment).	<i>2020 A-level algorithm</i> : one of the grounds reported as advanced in one of the challenges of the A-level algorithm was that the algorithm failed to take account of relevant considerations, such as teacher's predictions, and took into account irrelevant considerations, such as the historical success of the school ⁹ .
Insufficiency of inquiry	Decision makers have a duty to take reasonable steps to inform themselves of the relevant facts.	This ground has the potential to apply both in relation to: • Individual decisions produced by an automated system, and • The decision to use the automated system to make the decision in the first place. The first could be the case where due to the design of the automated decision-making system, or the processes around it, it was irrational not to make further	<i>R. (on the application of Timson) v Secretary of State for Work and Pensions [2022] EWHC 2392 (Admin)</i> : related to a scheme to deduct amounts from people's benefit payments to pay off third party debts. The relevant legislation provided that such deductions could only be made if they were in the interests of the claimant. In practice decisions were made in bulk, with utility providers sending an excel spreadsheet, sometimes generated automatically by their internal systems, listing

⁹ Cornerstone Barristers, [Legal action threatened over model 'standardising' A-level Grades](#), 16 August 2020



		enquiries to ensure they were informed of all the relevant facts. The second could apply in relation to a failure to make inquiries, for example of the developer of an automated system so as to understand how the system was designed and evaluated.	claimants to be subject to a deduction. The court found that a failure to provide decision subjects with the opportunity to make representations relevant to whether the decision was in their interests was a breach of the government's duty of inquiry.
Equal treatment and consistency	Decision makers should treat like cases alike and unlike cases differently according to their difference.	Automated decision-making systems may be well placed to ensure consistent decision making due to the fact that they may operate through: • A fixed, pre-determine set of rules, or • Operate on the basis of assessing whether a particular case is sufficiently 'like' previous decisions. However, they may be less well placed to identify nuances or circumstances that require a departure from fixed criteria (a difference in treatment)¹⁰.	
Wednesbury reasonableness	A decision must be within the range of reasonable decisions open to the decision-maker.	Computers are not inherently rational. If a decision would be irrational if it were made by a human, it should also be irrational if made by a computer. An automated decision could be irrational where (i) the outputs do not provide a reasonable basis for a human	<i>2020 A-level algorithm</i>: one of the grounds set out in pre-action correspondence included that the weighting given to historical performance data in respect of cohorts of different sizes produced substantively irrational results.¹¹

¹⁰ Sales (2025) n6

¹¹ n8



		decision-maker to make a decision, or (ii) the outputs are themselves bizarre, irrational or disproportionate.	
Systemic unlawfulness	A policy is unlawful if it creates a real risk of more than a minimal number of unlawful decisions.	It may be possible to show that an automated system is systemically unlawful, based on (i) its technical details (e.g. the fact that it unlawfully uses a particular dataset) or (ii) evidence about its outcomes or consequences (e.g. the fact that it produces large numbers of errors or creates lengthy delays).	<i>2020 A-level algorithm</i> : one of the grounds set out in pre-action correspondence included that the system gave rise to an unacceptable risk of procedural unfairness at a systemic level ¹² .

Human Rights

It is unlawful for a public bodies to act incompatibly with human rights protected by the European Convention of Human Rights (ECHR)¹³.

To determine whether an action is incompatible with human rights, it is necessary to consider whether the action interferes with a human right protected by the ECHR. Whether a right is relevant in any particular case will depend on the operation and impact of the system in question. Examples of human rights that may be engaged are included in the table below. Other rights that could potentially be relevant, depending on the context, include the right to a fair trial (Article 6), the right to property (Article 1 Protocol 1) and the right to education (Article 2 Protocol 1).

Ground		Potential application to ADM	Real-world examples
Article 8 – right to privacy	Article 8 protects peoples’ right to respect for their private life, family life	Where an automated system involves the processing of data relating to a person’s private life, it is likely to interfere with rights under Article	<i>R (Bridges) v Chief Constable of South Wales (2019)</i> ¹⁴ , the use of automated facial recognition technology (AFR) was found to engage Article 8 ECHR, because it enabled

¹² n7

¹³ section 6(1) Human Rights Act 1998

¹⁴ *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) [57]



	home and correspondence. The right to respect for your private life includes the right to live privately without government interference.	8. Many AI systems involve the processing of large amounts of data. Many ADM systems are also utilised for the purpose of surveillance and protection and detection of fraud.	the extraction of ‘unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances’ and that the AFR-derived biometric data was information of an ‘intrinsically private’ character¹⁵. Outside of the UK, in <i>NJCM v The Netherlands</i>¹⁶, the Hague District Court held that the Dutch Government’s automated system for detecting benefits fraud, known as ‘SyRI’, interfered with Article 8 rights to private life. The system processed large amounts of personal data to identify those most likely to commit fraud, who could then be targeted by public bodies, prosecutors and police.
Articles 10 (freedom of expression) & 11 (freedom of assembly and association)	Article 10 protects peoples’ right to hold their own opinions and express them freely without	Where a public body is using ADM technology, such as live facial recognition technology, to police protests or demonstrations, or otherwise survey freedom of expression it may constitute an interference with people’s Article 10 or Article 11 rights.	<i>R (Thompson and Carlo) v the Commissioner of Police of the Metropolis</i> [2026] EWHC 915 (Admin) the court found that the use of Live Facial Recognition technology may engage Articles 10 and 11 of the ECHR particularly in the context of

¹⁵ [57], n14

¹⁶ *NJCM v The Netherlands* C-09-550982-HA ZA 18–388 (English)



	government interference. Article 11 protects people's right to protest by holding meetings and demonstrations with other people		protests and demonstrations (although it went on to find that the interference was lawful in that case).
Art 14 - discrimination	Article 14 requires that all rights and freedoms set out in the HRA must be protected and applied without discrimination. It is not a freestanding right – it must be shown that discrimination affects one of the other rights under the Act.	As with the provisions on discrimination under the Equality Act 2010 (see further below), an ADM system can be: • Directly discriminatory, or • Indirectly discriminatory Unlike the Equality Act 2010, discrimination under Article 14 is not limited to a set list of protected characteristics. It instead applies to wide ranging and non-exhaustive set of characteristics including 'sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status'.	<i>R (Johnson) v Secretary of State for Work and Pensions</i> [2020] EWCA Civ 778 the grounds advanced by the Claimants included that the Regulations to which the system related were unlawfully discriminatory contrary to Art 14 ECHR, in conjunction with A1P1. The Secretary of State accepted that the case fell within A1P1 so that Art 14 was engaged, and recognised that being a woman and a parent could each constitute an 'other status'. However as the case was determined on the basis of irrationality (see above), the ground was not considered by the court.



Some human rights (like freedom from torture (Article 3)) are ‘absolute’ rights. This means that public bodies can never justify interfering with those rights. However most (including the rights identified in the table above) are ‘qualified rights’ which means public bodies can justify interfering with them in some circumstances.

If so, interference must be ‘in accordance with the law’.

Condition for ground to apply		Potential application to ADM	Real-world example
Legality	Interference with a qualified human right must be in accordance with the law. This means it must have some basis in domestic law which is sufficiently accessible and foreseeable. In practice, this is likely to mean that the system must be governed by a legal framework which is published and comprehensible and which provides safeguards against arbitrariness.	If a public body adopts an ADM system that interferes with a qualified human right it may be unlawful if it is not governed by a suitable legal framework. ADM systems may involve new and fast evolving technologies. As such, there may be no specific or detailed legal framework in place for that system yet.	<i>R (Bridges) v Chief Constable of South Wales (2020)</i>¹⁷, the use of AFR was found not to be in accordance with the law as the legal framework (comprising the Data Protection Act 2018, a statutory code and various policy documents) gave individual police officers too much discretion as to where it could be deployed and who could be placed on police watchlists. In contrast in <i>R (Thompson and Carlo) v the Commissioner of Police of the Metropolis (2026)</i>¹⁸ the court found that the policy used in that case and applied by the police force for its deployment of Live Facial Recognition technology was sufficient for

¹⁷ *R (Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058

¹⁸ *R (Thompson and Carlo) v the Commissioner of Police of the Metropolis* [2026] EWHC 915 (Admin)



			deployment to be considered in accordance with the law.
--	--	--	---

Interference with a qualified right must also be proportionate to a legitimate aim:

Condition for ground to apply		Potential application to ADM	Real-world example
Proportionality	Interference with a qualified human right must be proportionate to a legitimate aim.	In determining whether an automated system is proportionate to a legitimate aim, it is necessary to consider: • Whether the system is actually capable of achieving its stated objectives (e.g. a risk assessment tool which is justified on the ground that it will reduce the role of human bias in decision-making, but which in fact entrenches that bias through negative feedback loops) • Whether there is any less intrusive alternatives to the system, either technical or non-technical (this may require consideration of the other options available to the government when it designed or procured the system)	<i>NJCM v The Netherlands</i>, the Hague District Court held that the Dutch Government had not demonstrated that the 'SyRI' system was a proportionate interference with the legitimate aim of identifying fraud. In doing so it pointed to the large amounts of data (including personal data) processed, the risk that it created links based on bias (such as lower socio-economic status or immigration background) and the inadequacy of the safeguards and associated transparency. However in <i>R (Bridges) v Chief Constable of South Wales (2020)</i>¹⁹, the use of AFR was found to constitute a proportionate interference with Article 8 (although as

¹⁹ n17



		Whether the system strikes a fair balance between the rights of the individual and the interests of the community.	noted above it was found not to be in accordance with the law)
--	--	--	--

Equality Law

The Equalities Act 2010 (EqA 2010) sets out the legal framework for protecting the rights of individuals and advancing equality of opportunity for all. It sets out the personal characteristics that are protected by law (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation) and the behaviour that is unlawful.

Ground		Potential application to ADM	Real-world examples
Direct discrimination (s. 13 EqA 10)	Direct discrimination is where a person treats someone less favourably because of a protected characteristic.	If an automated system expressly takes into account a person's protected characteristic and gives them a less favourable outcome, this is likely to constitute direct discrimination (e.g. a risk assessment tool gives a person a high risk rating because of their nationality).	<i>Visa streaming challenge</i> : one of the grounds advanced was that the automated streaming system was directly discriminatory on the basis that it used nationality as an apparently significant factor ²⁰ . The case was subsequently settled.
Indirect discrimination (s. 19 EqA 10)	Indirect discrimination occurs where a provision, criterion or practice (PCP), while neutral on its face,	If an automated system has a systematic negative impact on members of a protected group, it may be indirectly discriminatory (e.g. a facial recognition system that mistakenly identifies women's faces at a higher rate than men's faces, which leads to	<i>R (Thompson and Carlo) v the Commissioner of Police of the Metropolis (2026)</i> the court accepted that, if a policy governing the use of Live Facial Recognition were to authorise discriminatory

²⁰ R (The Joint Council for the Welfare of Immigrants) v Secretary of State for the Home Department, Statement of Facts and Grounds of Judicial Review, available here: <https://www.ein.org.uk/news/home-office-suspends-use-digital-streaming-tool-visa-applications-after-legal-action-jcwi-and>



	puts people with a protected characteristic at a disadvantage. It is sometimes described as equality by results.	women being stopped by police at a higher rate than men).	or arbitrary decision-making, that could undermine its legality (however the ground was not advanced in that case).
Public Sector Equality Duty (PSED) (s. 149 EqA 10)	The PSED requires public bodies to have regard to, among other things, eliminating (direct and indirect) discrimination and advancing equality of opportunity.	If a public body is considering adopting an ADM system, under the PSED they are required to consider whether it might raise issues of discrimination. If a system is potentially discriminatory, the PSED will require them to consider those risks, and how they might be addressed. This includes a requirement to take reasonable steps to make enquiries about what may not yet be known about the potential discriminatory risks, for example, getting a private developer to provide access to the system's technical details and conducting expert analysis of the system.	<i>R (Bridges) v Chief Constable of South Wales (2020)</i> the court found that the police force had failed to make sufficient enquiries about the AFR system it was deploying so as to discharge it's PSED.

Data Protection Law



Data protection law regulates the processing²¹ of personal data²² by data controllers²³. The key sources of data protection law in the UK are the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UKGDPR). The UKGDPR is the version of the EU data protection law retained as UK law following Brexit and modified by the Data (Use and Access) Act 2025.

Ground		Potential application to ADM	Real-world examples
Data protection principles	Data Controllers must generally comply with seven data protection principles when processing personal data: • Lawfulness, fairness and transparency: personal data shall be processed fairly, lawfully and transparently • Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.	The use of ADM systems is likely to involve the processing of personal data. That processing must comply with the data protection principles. For example, an automated decision-making system that is discriminatory is unlikely to be considered fair ²⁴ .	<i>Home Office algorithms ICO complaint:</i> In August 2025, Privacy International submitted a complaint to the Information Commissioner's Office alleging that two algorithms used in immigration enforcement operations failed to comply with 5 of the 7 data protection principles. ²⁶

²¹ Processing is defined as any operation which is performed on personal data, including collection, organisation, storage, alteration, retrieval, use, disclosure, erasure and destruction, Art 4(2) UKGDPR

²² any information relating to an identified or identifiable natural person, known as a data subject. An 'identifiable natural person' is a person who can be identified, directly or indirectly, by reference to an identifier (e.g. a name, an identification number, etc.) or one or more factors specific to their identity (e.g. physical, mental, economic, etc.), Art 4(1) UKGDPR

²³ 'the natural or legal person, public body, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data', Art 4(7) UKGDPR

²⁴ ICO, [What about fairness, bias and discrimination?](#)

²⁶ Privacy International, [Complaint against the UK's automated recommendation tools in immigration operations](#)



	• Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. • Accuracy: Personal data shall be accurate and, where necessary, kept up to date. • Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary. • Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	The ICO has published guidance on how the principles apply in relation to Artificial Intelligence ²⁵ .	
--	---	---	--

²⁵ ICO, [Guidance on AI and Data Protection](#)



	• Accountability: The controller shall be responsible for, and be able to demonstrate compliance with the data protection principles		
Restriction on solely Automated Decision Making (using special category data)	Under Articles 22A-D UKGDPR, significant decisions using special category data may not be taken based solely on automated processing unless (a) the data subject has explicitly consented, (b) it is necessary for the performance of a contract, or (c) it is required or authorised by law. A decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision (Art 22A(1)(a)).	A public body will not be able to make decisions using solely automated decision making systems using special category data unless one of the specific conditions apply. The ICO has recently consulted on draft guidance regarding the application of this in practice²⁷.	
DPIA	Under Article 35 UKGDPR Data Controllers are required to undertake Data Protection Impact Assessments (DPIAs) before undertaking processing, in particular using new technologies, which are likely to result in a high risk to the rights and freedoms of natural persons.	It may not be enough for a public body to rely on a DPIA completed by the private developer of an automated system. The burden of demonstrating compliance rests with the controller, and the private developer may not be in a position to assess the impact of 'the envisaged processing operations' on the protection of personal data.	<i>R (Bridges) v Chief Constable of South Wales</i> the court found that the DPIA was inadequate due to its failure to reflect that the interference with Article 8 rights was not in accordance with the law.

²⁷ ICO, [ICO consultation on the draft guidance about automated decision-making, including profiling](#) 31 March 2026



			<i>Visa streaming challenge:</i> one of the grounds advanced by the claimants were that the defendant had failed to conduct a lawful DPIA on the basis that the DPIA included irrational conclusions ²⁸ .
--	--	--	--

In addition to the restrictions on solely Automated Decision Making under Article 22B, the UKGDPR provides for a number of additional safeguards (Article 22C UKGDPR) and information rights (Articles 13(1)(f), 14(1)(f), 15(1)(f)) that apply to these types of decision-making system. These are discussed in Annex 2 below.

²⁸ Electronic Immigration Network, [Home Office suspends use of digital streaming tool for visa applications after legal action by JCWI and Foxglove | Electronic Immigration Network](#)

Annex 2 – Transparency Mechanisms

This information sets out the detail regarding existing information rights and requirements and their limitations in relation to their effectiveness for providing information about automated decision-making systems. Part A sets out rights and requirements which require a claimant taking some form of action in order for information to be provided. Part B sets out requirements which require proactive provision of information without a claimant having to take action.

A. Reactive information provision (provision of information conditional on a claimant initiating action)

	FOIA Requests	Subject Access Requests	Duty of Candour
Information in scope	Section 1 of the Freedom of Information Act 2000 (FOIA) gives people making a request for information to a public authority the right to be: (a) Informed in writing by the public authority whether it holds information of the description specified in the request, and	Article 15 UK Data Protection Regulation (UKGDPR) provides data subjects³¹ with the right to obtain from a data controller³²: (a) Confirmation as to whether or not their personal data is being processed³³, (b) A copy of their personal data, (c) Other supplementary information (which largely coincides with the information	The duty of candour is a common law duty that requires parties to judicial review proceedings to ensure that all relevant material is put before the court. This includes material that would undermine their case. The duty applies before the Court's consideration of whether to grant permission for judicial review³⁷ – however there is case law that suggests that what is

³¹ A data subject is an identified or identifiable individual to whom personal data relates (Art 4(1) UKGDPR)

³² a data controller refers to any person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data (Art 4(7)UKGDPR)

³³ personal data refers to any information relating to the data subject (Art 4(1) UKGDPR)

³⁷ Treasury Solicitor's Department, *Guidance on Discharging the Duty of Candour and Disclosure in Judicial Review Proceedings*, 2010, para 1.2



	(b) If that is the case, to have that information communicated to him. It only applies to information that the public authority already holds in recorded form at the time of the request²⁹. Public authorities are not required to create new information in order to comply with a FOIA request. They only need to consider information already in existence at the time the request is received³⁰. Section 3(2) sets out the criteria for when information is "held" for the purposes of the Act.	required to be provided under Articles 13 and 14 UKGDPR – see table below) - this includes information about the existence of automated decision-making, including profiling, which is subject to the requirement to provide safeguards under Art 22C and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject. Automated decision-making to which Article 22C applies are defined as significant decisions based a) entirely or partly on personal data³⁴, and b)	required to discharge the duty at the substantive stage will be more extensive³⁸. However, case law also provides that while the duty at the stage of application for leave is likely to be less extensive, it none-the-less requires defendants to provide such information as is necessary to understand why the decision under challenge was made and to identify issues which may arise in relation to that decision³⁹. A lack of candour can also be taken into account when deciding whether to grant permission⁴⁰. Depending on the context, the duty can include requirements to disclose documents, provide explanations of those documents and provide relevant facts not evident from the disclosed documents.
--	---	--	--

²⁹ sections 1(4) and 84 FOIA

³⁰ para 1.3, Cabinet Office, [Freedom of Information Code of Practice](#) (4 July 2018) (FOI CoP)

³⁴ unlike the restrictions on automated decision-making contained in Art 22B UKGDPR (see Annex 1), the requirement to provide safeguards is not restricted to decisions made using special category data.

³⁸ R (on the application of Police Superintendents' Association) v The Police Remuneration Review Body [2023] EWHC 1838 (Admin) [15]

³⁹ [National Bank of Anguilla \(Private Banking and Trust\) Ltd & Anor v Chief Minister of Anguilla & Ors \(Anguilla\) \[2025\] UKPC 14 \(24 March 2025\) \[92\]](#)

⁴⁰ National Bank of Anguilla v Chief Minister of Anguilla (2025) [93], n29



	based solely on automated processing (solely ADM). A decision is based solely on automated processing if there is no meaningful human involvement in the making of the decision³⁵. At the time of writing, there is no case law in England and Wales regarding the scope of the information requirements that apply in relation to solely ADM under Article 15. However, a judgment of the Court of Justice of the European Union (CJEU) regarding the equivalent provision under the (EU) GDPR, has held that it includes providing an explanation of the procedure and principles “actually applied” in order to use the data subject’s personal data with a view to obtaining a specific result.³⁶	However in practice, there is a lack of clarity and variation in approaches to: • The extent of the duty in the pre-permission stages, • The provision of underlying documents⁴¹.
--	---	---

³⁵ Art 22A(1)(B) UKGDPR

³⁶ *CK v Dun & Bradstreet* (Case C-203/22) [66]

⁴¹ O'Loughlin, E. (2024, October 7). Transparency and Judicial Review: An Empirical Study of the Duty of Candour. <https://durham-repository.worktribe.com/output/2990498>



Exemptions	The FOIA sets out exemptions that may allow public authorities to withhold information from a requester. These include 'absolute exemptions' where public authorities can automatically withhold the information if the exemption applies. Other exemptions are 'qualified exemptions', which only apply if, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information (the 'public interest test'). Examples of exemptions include: • Section 22 (information is intended for future publication)	Article 15(4) UKGDPR provides that the right to obtain a copy under Article 15(1) shall not adversely affect the rights and freedoms of others. Recital 63 refers to this as including trade secrets or intellectual property, in particular the copyright protecting the software. A judgment of the CJEU regarding the equivalent provision under the (EU) GDPR, has held that where a data controller considers that the information includes data of third parties or trade secrets, it must provide the information to the competent supervisory authority or court which must then balance the rights and interests at issue and	A party can apply to the court to withhold relevant material if they can demonstrate that disclosure would damage the public interest⁴⁷. Where material cannot be disclosed, the Court can instead consider whether the material can be disclosed in summarised form or disclosed to a restricted number of recipients in a confidentiality ring.⁴⁸ If pre-permission duty of candour would require disclosure of material the party considers it attracts public interest immunity, the party would need to claim it at that stage. However, the Judicial Review Guide notes that given that the duty may be less extensive at this stage, a defendant may instead conclude that it isn't required to be disclosed at this stage⁴⁹.
-------------------	---	--	--

⁴⁷ R (Public and Commercial Services Union) v Secretary of State for the Home Department [2022] EWHC 823 (Admin), [14]; CPR 31.19; section 19.2 Judicial Review Guide 2025

⁴⁸ R (Public and Commercial Services Union) v Secretary of State for the Home Department [2022] EWHC 823 (Admin), [14]; CPR 31.19; section 19.2 Judicial Review Guide 2025

⁴⁹ para 19.2.6, Courts and Tribunals Judiciary, The Administrative Court Judicial Review Guide 2025, (August 2025)



	• Section 24 (withholding required to safeguard national security) • Section 31 (disclosure would prejudice law enforcement) • Section 35 (information relates to the formulation of Government Policy) • Section 36 (disclosure would prejudice the effective conduct of public affairs) • Section 43 (information constitutes a trade secret or would prejudice commercial interests). Public authorities are also not required to disclose information if it estimates that the cost of complying would exceed a limit (£600/24 hours for central government	determine the extent of the data subject's right of access⁴⁴. The Data Protection Act 2018 (DPA 2018) provides for a number of further exemptions from the requirements under Article 15 UKGDPR These include the following exemptions set out in Schedule 2 DPA 2018: • Para 2 (prejudice to crime and taxation): personal data processed for the purposes of: - o The prevention, investigation or detection of crime - o The apprehension or prosecution of offenders, or	In practice there is also a risk of being redirected at pre-permission stage to alternate sources of information⁵⁰ (FOIAs and SARs (see previous columns) - although provision of redacted documents under those routes could support a subsequent order for disclosure of unredacted versions by the court.⁵¹ Documents can be redacted if the redacted section a) attracts public interest immunity; b) are confidential and irrelevant, c) attract legal professional privilege, or d) are subject to statutory restrictions.⁵²
--	--	---	---

⁴⁴ *Dun & Bradstreet* [76], n32

⁵⁰ *R (Buav) v Secretary of State for the Home Department* [2012] EWHC 2696 (Admin) 3-4; *British Union for the Abolition of Vivisection v Secretary of State for the Home Department* [2014] EWHC 43 (Admin)

⁵¹ *R (Plantaganet Alliance Ltd) v Secretary of State for Justice and others* [2013] 1 Inquest LR 204 [35]

⁵² *R (on the application of Police Superintendents' Association) v The Police Remuneration Review Body* [2023] EWHC 1838 (Admin) [15]; para 15.5.1 Judicial Review Guide 2025



	departments, Parliament and the armed forces; £450/18 hours for all other public authorities) (s. 12 FOIA). Public authorities can only include certain activities when estimating whether these limits would be breached. These are: • establishing whether information is held • locating and retrieving information and • extracting relevant information from the document containing it⁴² Other factors including redaction time or any other expenses likely to occur in cost limit calculations cannot be included when estimating whether the response would exceed the limit.	- o The assessment or collection of a tax or duty, To the extent that it would be likely to prejudice those matters. • Para 3 (crime and taxation: risk assessment): where access would disclose a person's classification within a risk assessment system to the extent that it would prevent the system from operating effectively. The risks assessment must be operated: - o by a government department, a local authority or another authority administering housing benefit and, - o for the purposes of (a) the assessment or collection of a tax or duty or an imposition of a similar nature, or (b) the prevention, investigation or detection of crime or apprehension or prosecution of	
--	--	--	--

⁴² Regulation 4, [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulation 2004 SI 2004 No 3244](#) (the Fees Regulation)



	When calculating the cost limit public authorities can aggregate requests which are for the same or similar information and are received within a 60 day period⁴³.	offenders where the offence concerned involves the unlawful use of public money or an unlawful claim for payment out of public money. Para 4 (immigration): where access would be likely to prejudice (a) the maintenance of effective immigration control, or (b) the investigation or detection of activities that would undermine the maintenance or effective immigration control. This exemption must be applied on a case-by-case basis and balance the risk to immigration control against the risks to the person's rights and freedoms (taking into account their potential vulnerabilities). Application must be necessary and proportionate to the particular case.⁴⁵ Additional exemptions apply in relation to data processed by competent	
--	--	---	--

⁴³ Section 5, the Fees Regulation n29

⁴⁵ paragraphs 4A and 4B Schedule 2 Data Protection Act 2018



		authorities for criminal law enforcement processes (for example, where the police are investigating a crime). The processing of data in these circumstances is outside the UKGDPR's scope and is instead subject to Part 3 DPA 2018. This allows the data controller to restrict the equivalent access rights if necessary and proportionate to (a) avoid obstructing an official or legal inquiry, investigation or procedure, (b) avoid prejudicing the prevention, detection investigation or prosecution of criminal offences or the execution of criminal penalties, (c) protect public security, and (d) protect the rights and freedoms of others⁴⁶.	
Timings	Public authorities should respond promptly and within 20 working days to requests,⁵³	Data Controllers have one month to reply to Article 14 requests, which can	There are a number of stages in a judicial review.

⁴⁶ s. 45(4) DPA 2018

⁵³ section 10(1) FOIA



	• If more information is needed to identify and locate the information requested, and the public body has communicated this to the applicant, the time limit runs from when that additional information is provided, • If a qualified exemption applies, and the public body needs more time to consider the public interest test, they can extend the limit up to a 'reasonable time'⁵⁴ (under the FOIA Code of Practice, this is generally considered to be no more than an additional 20 working days⁵⁵) • It is best practice for public bodies to have a procedure in place to deal with disputes about FOIA	be extended to up to 3 months for complex requests⁵⁸. If a data controller needs more information to understand the request, they can “stop the clock” until they receive that information from the requester⁵⁹. If a data subject does not receive a response within the time limits, or is unhappy with the response received, the ICO recommends complaining to the data controller before submitting a complaint to the ICO. The data controller should acknowledge the complaint within 30 days. Data protection law doesn't provide a specific time limit to provide an	• Letter before claim: in most cases, the claimant should send a letter to the defendant (often referred to as a pre-action protocol letter). The purpose of the letter is to identify the issues in dispute and establish whether they can be narrowed or litigation can be avoided. It should contain details of any information the claimant is seeking and an explanation of why this is considered relevant⁶¹. • Letter of response: the defendant then has 14 days to respond but where necessary they can ask the defendant for extra time⁶². The response should set out the defendant's answer to the requests made in the letter before claim including reasons why any requested information or
--	--	--	--

⁵⁴ s.10(3) FOIA

⁵⁵ para 4.5, FOI CoP, n20

⁵⁸ Articles 12(3) and 12A UKGDPR

⁵⁹ Art 12A(5) and (6) UKGDPR

⁶¹ paras 14 – 19 Pre-Action Protocol for Judicial Review

⁶² Paras 20-24, Pre-Action Protocol for Judicial Review



	responses (internal reviews) ⁵⁶ - under the FOI Code of Practice, responses to internal reviews should normally be provided within 40 working days . ⁵⁷	outcome to complaints. Data controllers are required to provide it without an “unjustifiable or excessive delay” ⁶⁰ .	documents are not being disclosed ⁶³ . • Filing the claim form: if the issues are not resolved at pre-action stage, the claimant needs to file a claim form, statement of facts and grounds, any witness statements, relevant documents of correspondence and then serve the issues claim on the defendant, • Acknowledgment of service: within 21 days, the defendant should file acknowledgment of service and summary grounds of defence. • Post-permission: If permission is granted by the court, the court may also give case management directions³⁴. Typically this will include directing:
--	--	--	--

⁵⁶ Section 5, FOI CoP, n46

⁵⁷ para 5.5, FOI CoP, n20

⁶⁰ ICO, [How to deal with data protection complaints](#)

⁶³ Annex B, Pre-Action Protocol for Judicial Review



			- o The Defendant to file with the Court and serve on the Claimant detailed grounds for contesting the application and any written evidence within 35 days, - o That any reply and application by the Claimant to adduce further evidence must be filed within 14 days of service of the detailed grounds contesting the application, - o The Claimant must file with the Court and serve on the Defendant a skeleton argument and trial bundle no later than 21 days before the hearing of the judicial review, - o The Defendant must file with the Court and serve on the Claimant a skeleton
--	--	--	--



			argument not later than 14 days before the hearing of the judicial review.
Enforcement	- If the requester is unhappy with the response, they can complain to the Information Commissioner's Office (ICO). The ICO's aim is to resolve cases within 6 months of receipt⁶⁴. - Complaints may be resolved informally between the complainant and the public authority. If it cannot be resolved informally, the ICO will issue a decision notice setting out their	The ICO can take enforcement action for failures to comply with Article 15 UKGDPR. If the ICO is satisfied that a failure has occurred, it can issue an enforcement notice requiring the person to take or refrain from taking specified steps⁶⁷. The ICO has power to issue fines in the event of non-compliance⁶⁸. However, it applies a public sector approach whereby it will only consider issuing a fine to a public body in the most	Parties can apply to the court for: - An order for specific disclosure⁷¹, - An order compelling the other party to provide further information⁷². The above may bring risks of increased costs and delays⁷³. Additional consequences the Court could impose include: - Adverse costs orders, - Drawing adverse inferences⁷⁴,

⁶⁴ ICO, [How we deal with complaints](#)

⁶⁷ Section 149 DPA 18

⁶⁸ Section 155 DPA 2018

⁷¹ CPR 31.12(1)

⁷² CPR 18.1

⁷³ R (Good Law Project Ltd) v Secretary of State for Health and Social Care [2021] EWHC 2595 (TCC) [5]

⁷⁴ See for example Gardner v SSHSC [2021] EWHC 2422 (Admin)



	decision⁶⁵. If it finds that the public authority hasn't complied with the FOIA, it should specify the steps the authority should take to comply and in what period⁶⁶. • The ICO cannot issue fines or award compensation. If a public authority fails to comply with a decision notice the ICO can notify the courts who may treat it as a contempt of court. • If a complainant is dissatisfied with the ICO's decision, they can appeal to the First Tier Tribunal (Information Rights) (FTT) within 28 calendar days of the date of the decision notice. • A decision of the FTT can be appealed to the Upper Tribunal on a ground of law.	egregious cases, where it is appropriate and the infringements are especially serious⁶⁹. Requesters can also apply the court to: • Enforce their rights, and / or • Claim compensation for any damage caused if they have broken data protection law⁷⁰.	• Referral to professional regulator.⁷⁵
--	---	---	--

⁶⁵ section 50 FOIA

⁶⁶ section 50(4) FOIA

⁶⁹ ICO, [Public sector approach](#)

⁷⁰ sections 167 – 169 DPA 2018

⁷⁵ See for example, R (Sathivel) v SSHD [2018]4 WLR 89



Limitations	The right to information is limited to information held and does not extend to the creation of new information. Information can be withheld on the basis of exemptions. FOIA requests can be refused if they exceed a cost limit. In assessing whether the cost threshold is exceeded, public authorities can aggregate requests for the "same or similar information". This can lead the need to space out requests for information if there is a risk that they would be interpreted as "the same or similar". Phase 1 interviews reported delays in responses and the need for more than one round of requests to obtain information combined with lengthy complaints processes.	Only applies to information which constitutes personal data of the data subject. Additional information rights relating to decisions to which Article 22C UKGDPR limited to "solely" ADM systems. Information can be withheld on the basis of exemptions. Phase 1 interviews reported delays in responses and the need for more than one round of correspondence to obtain information combined with lengthy complaints processes. Phase 1 interviews referred to a perception of defendant compliance being hindered by practical or cultural challenges.	There is a lack of clarity and variation in approaches to: • The extent of the duty in the pre-permission stages, • The provision of underlying documents²³. Phase 1 interviews identified a "vicious circle" between application of a less extensive pre-permission duty of candour creating a barrier to progressing beyond the permission stage when the more extensive duty would be more clearly engaged. Phase 1 interviews also identified examples of late provision of documents within proceedings. Phase 1 interviews referred to a perception of defendant compliance being hindered by practical or cultural challenges.



	Even where information is provided in response to initial requests this may be too late in some contexts for complying with public body deadlines for submitting representations. Phase 1 interviews referred to a perception the public authorities' compliance could be hindered by practical or cultural challenges.		Redirection towards alternate sources of information could engage the limitations identified in the FOIA and SAR columns.
--	---	--	--

B. Proactive information provision (provision of information is not conditional on a claimant initiating action)

	ATRS	Right to be Informed (Arts 13 & 14 UKGDPR)	ADM Safeguards (Art 22C UKGDPR)
Information in scope	Information about 'algorithmic tools (a product, application or device that supports or solves a specific problem using complex algorithms) used by public sector organisations and that a) have a significant influence on a decision-making process with public	Articles 13 and 14 provide data subjects with a “right to be informed” about the collection and use of their personal data. They set out specific information that should be provided including:	Article 22C UKGDPR sets out safeguards that must be in place in relation to significant decisions based solely on automated processing without meaningful human involvement. Those safeguards must include measures which:



	effect, or b) directly interact with the general public⁷⁶. 'Algorithmic tool' is an intentionally broad term that covers different applications of Artificial Intelligence (AI), statistical modelling and complex algorithms. 'Significant influence' is defined as including where an algorithmic tool meaningfully assists, supplements or fully automates a decision-making process. 'Public effect' is defined as a decision-making process having an impact on members of the public where the latter are understood as any individual or groups of individuals, irrespective of their nationality or geographical location. The ATRS template is divided into 2 tiers.	• The purpose and legal basis for the processing • The existence of of the right to request access to, rectification or erasure of personal data and the right to object to the processing of data. In the case of automated decision making that falls within the definition of Article 22C (significant decisions based solely on automated processing without meaningful human involvement - see Article 15 above)that must include provision of information about: • The existence of automated decision-making, including profiling, • “at least in those cases” meaningful information about the logic involved	(a)provide the data subject with information about the decision; (b)enable the data subject to make representations about such decisions; (c)enable the data subject to obtain human intervention on the part of the controller in relation to such decisions; (d)enable the data subject to contest such decisions. The ICO consulted on guidance regarding Article 22C this year⁷⁹. This draft guidance provides that data controllers must explain all ADM to give people an understanding of how you reached the decision. It states that this is decision-specific information about the actual outcome, rather than simply repeating information set out in a privacy
--	--	--	--

⁷⁶ Section 4, Government Digital Service (GDS), [Algorithmic Transparency Recording Standard \(ATRS\) Mandatory Scope and Exemptions Policy](#)

⁷⁹ ICO, [ICO consultation on the draft guidance about automated decision-making, including profiling | ICO](#)



	• Tier 1 is aimed at the general public, and as such should be clear and simple in language. • Tier 2, whilst still accessible to the general public, is aimed at specialist audiences such as civil society, journalists, academic researchers and other public sector organisations wishing to learn from their peers. An ATRS template specifies the categories of information that should be provided about systems that are in scope⁷⁷. It is supplemented by guidance⁷⁸.	• The significance and envisaged consequences of such processing for the data subject. See above for the CJEU's interpretation of "meaningful information about the logic involved" in the context of Article 15 rights. In practice, the right to be informed is often discharged by way of a privacy notice on a data controller's website. This information is often high level and not specific to an ADM system. Article 12 provides that information provided under Articles 13 and 14 must be in a concise, transparent, intelligible and easily accessible form using clear and plain language.	notice (under the right to be informed, see previous column). It states that what information is required will depend on the context. However, data controller must ensure information is: • Clear and accessible, • Helps people understand the decision, • Explains how the decision was reached • Tells them what its actual impact is It should include aspects such as: • The factors that contributed to the decision, • Whether profiling was involved • Whether data from a third-party controller influenced the decision.
--	--	--	---

⁷⁷ GDS, [Algorithmic Transparency Recording Standard template](#)

⁷⁸ GDS, [Guidance for organisations using the Algorithmic Transparency Recording Standard](#)



Exemptions	The ATRS does not require the publication of information that would be subject to an exemption under FOIA or data protection legislation (see above). The exceptions to this are ss.12 (cost limits), 14 (vexatious or repeated requests), 21 (accessible by other means) and 22 (intended for future publication) which should not apply in relation to the ATRS. The ATRS guidance advises that claiming exemptions under s. 43 (commercial sensitivity) “should be exercised with care”. It also advises that where an exemption does apply, in most cases the response should be to reduce the level of information supplied for relevant fields rather than withholding it altogether⁸⁰.	Schedule 2 Data Protection Act 2018 provides a number of exemptions in relation to Articles 13 and 14. These include: Para 2 (prejudice to crime and taxation): personal data processed for the purposes of: (d) The prevention, investigation of detection of crime (e) The apprehension or prosecution of offenders, or (f) The assessment or collection of a tax or duty, To the extent that it would be likely to prejudice those matters Para 3 (crime and taxation: risk assessment): where access would disclose a person’s classification within a risk assessment system to the extent that it would prevent the system from operating effectively.	Where the decision relates to law enforcement processing, the requirement to apply those safeguards do not apply if exemption is required to: (a) avoid obstructing an official or legal inquiry, investigation or procedure, (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, (c) Protect national security, (d) Safeguard national security (e) Protect the rights and freedoms of others.
--------------------------	--	---	---

⁸⁰ Section 5, [ATRS Scope and Exemptions Policy](#).



		The risks assessment must be operated: (c) by a government department, a local authority or another authority administering housing benefit and, (d) for the purposes of: (i) the assessment or collection of a tax or duty or an imposition of a similar nature, or (ii) the prevention, investigation or detection of crime or apprehension or prosecution of offenders where the offence concerned involves the unlawful use of public money or an unlawful claim for payment out of public money. Para 4 (immigration): where access would prejudice (a) the maintenance of effective immigration control, or	
--	--	---	--



		(b) the investigation or detection of activities that would undermine the maintenance or effective immigration control. Additional exemptions apply in relation to data processed by competent authorities for criminal law enforcement processes. This allows the data controller to restrict access rights if necessary and proportionate to (a) avoid obstructing an official or legal inquiry, investigation or procedure, (b) avoid prejudicing the prevention, detection investigation or prosecution of criminal offences or the execution of criminal penalties, (c) protect public security, and (d) protect the rights and freedoms of others.	
When, where and how is the	Entries are published on an online register ⁸¹ .	When personal data is collected from the individual it relates to, they must	It is implicit in the requirements that information should be provided when the decision is communicated.

⁸¹ GDS, [Repository of ATRS records](#)



information provided?	The mandatory requirement to publish an ATRS record applies to tools that are in Beta/Pilot or Production phase. Teams are welcome to submit records for tools in earlier stages of the lifecycle, but it is not mandatory to do so. ATRS entries should be updated in the event of substantive changes.	be provided with privacy information at the time the data is collected. When the personal data has come from a source other than the individual it relates to, it must be provided within a reasonable period of obtaining the personal data and no later than one month. ICO guidance provides that this requirement can be met by putting information on a website, although the data controller must make individuals aware of it and give them an easy way to access it.	
Enforcement	There is no external mechanism for complaining or triggering enforcement of compliance with the ATRS. It is described as a mandatory requirement in guidance in relation to central government bodies. Compliance is underpinned by digital spend controls, which means that when budget is	The ICO can take enforcement action. If the ICO is satisfied that a failure has occurred, they can issue an enforcement notice requiring the person to take specified steps or refrain from taking steps¹¹.	The ICO can take enforcement action. If the ICO is satisfied that a failure has occurred, they can issue an enforcement notice requiring the person to take specified steps or refrain from taking steps¹¹.



	requested for a relevant tool, the team in question must commit to publishing an ATRS record before receiving the funds⁸².	The ICO has power to issue fines in the event of non-compliance. However, it applies a public sector approach whereby it will only consider issuing a fine to a public body in the most egregious cases, where it is appropriate and the infringements are especially serious¹². Requesters can also apply the court to: • Enforce their rights, and / or Claim compensation for any damage caused if they gave broken data protection law¹³.	The ICO has power to issue fines in the event of non-compliance. However it applies a public sector approach whereby it will only consider issuing a fine to a public body in the most egregious cases, where it is appropriate and the infringements are especially serious¹². Requesters can also apply the court to: • Enforce their rights, and / or • Claim compensation for any damage caused if they gave broken data protection law¹³.
--	--	--	--

C. Summary

⁸² [HL Deb \(16 December 2024\), vol 842, col 49GC](#)



	Proactive – "solely" automated decision making (ADM)	Proactive – automated assisted decision making (AADM)	Individual information - ADM	Individual information - AADM	Systemic information	Limitations
Algorithmic Transparency Recording Standard (ATRS)	Yes (if complied with)	Yes (if complied with)	No	No	Some	Does not provide notice or information about whether and how it has been applied in an individual decision Exemptions may apply Compliance is not enforceable - with high-risk systems reported as missing in practice Gaps in information provided in practice.
Art 22C UKGDPR - ADM safeguards	Yes	No	Some	No	No	Only applies to solely ADM Focussed on information about individual decisions rather than systemic information



Art 13 – 14 UKGDPR – right to be informed	Potentially	No	No	No	Some	Very limited information provided in practice ADM specific information limited to solely ADM Phase 1 findings included perception of poor compliance and enforcement Exemptions may apply
Article 15 UKGDPR	No	No	Potentially	No	No	Additional information rights only apply to "solely" ADM Exemptions may apply Phase 1 findings included perception of poor compliance and enforcement Phase 1 findings reported multiple rounds of requests and lengthy timelines



FOIA	No	No	No	No	Potentially	Only applies to information held in recorded form at the time of request. Exemptions may apply Phase 1 findings included perception of poor compliance and enforcement Phase 1 findings reported multiple rounds of FOIA requests and lengthy timelines
Duty of Candour	No	No	Potentially	Potentially	Potentially	Lack of clarity and variation in practice in relation to when and how it applies Application of less extensive duty before permission stage in judicial review Phase 1 findings reported multiple rounds of pre-action correspondence



Annex 3 – Litigation Mapping Exercise

As part of Phase 1 of the research project, an exercise was undertaken to identify instances of a) judicial review, and b) regulatory complaints to the ICO under data protection law, that related to ADM systems falling with the definition set out at B.1 of the main report.

This included cases where a judicial review challenge or data protection regulatory complaint had been:

1. Considered but not initiated (for example, no pre-action correspondence had been sent) (**category 1**),
2. Initiated (for example, through sending of initial pre-action correspondence) but dropped or settled without progressing to judgment or a final decision (**category 2**)
3. Was still under consideration or otherwise in progress (**category 3**)
4. Initiated and progressed to judgment or final decision (**category 4**)

Cases were identified by undertaking a search of legal research platforms and the ICO's database of enforcement action, supplemented by a further call out through our networks and a snowballing approach.

The partial results of this exercise are set out below. This only includes information on cases that are in the public domain. It does not include cases that were identified but which are not currently referred to publicly (either in official court reporting or otherwise). As a result the majority of entries refer to cases that progressed to judgment or final decision.

A. Judicial Reviews and Upper Tribunal appeals

	Case	Type (Judicial Review (JR), Upper	ADM system description	Grounds (if known)	Category
--	------	--	---------------------------	--------------------	----------



		Tribunal (UT))			
1.	R (Bridges) v CCSWP [2020] EWCA Civ 1058	JR (appeal)	Facial recognition/matching software deployed at large public events	1. Unlawful interference with Article 8 European Convention on Human Rights (ECHR) 2. Disproportionate interference with Article 8 ECHR 3. Data Protection Impact Assessment (DPIA) based on two material errors of law 4. No “appropriate policy document” for purposes of s. 42 Data Protection Act 2018 (DPA 2018) 5. Public Sector Equality Duty (PSED) Equality Impact Assessment (EIA) was inadequate	4
2.	<i>R (Bridges) v CCSWP [2019] EWHC 2341 (Admin)</i>	<i>JR (first instance decision of 1)</i>	<i>See above</i>	1. <i>Unlawful interference with Article 8 ECHR</i> 2. <i>Failure to comply with s.35 DPA 2018.</i> 3. <i>Failure to conduct DPIA per s.64(1) DPA 2018.</i> 4. <i>PSED EIA failed to have due regard to possibility of higher false positives for minority ethnic groups and women</i>	4
3.	R (Johnson) v SSWP [2020] EWCA Civ 778	JR (appeal)	Rules based algorithm to calculate amount of Universal Credit award (underpinned by regulations)	1. Secretary of State’s (SSWP) construction of relevant regulation was wrong 2. Construction was arbitrary, contrary to regulations aims and irrational. 3. Unlawful interference with Article 14 ECHR read with Article 1 Protocol 1 (A1P1)	4
4.	<i>R (Johnson) v SSWP [2019] EWHC 23 (Admin)</i>	<i>JR (first instance</i>	<i>See above</i>	1. <i>SSWP had wrongly construed the regulations</i> 2. <i>SSWP had not complied with the PSED</i>	4



		<i>decision of 3)</i>			
5.	R (Pantellerisco) v SSWP [2021] EWCA Civ 1454	JR	Rules based algorithm to calculate earnings-related threshold. HMRC data matching.	1. First-instance judge erred in finding calculation under the relevant regulations was irrational due to four-weekly payments	4
6.	<i>R (Pantellerisco) v SSWP [2020] EWHC 1944 (Admin)</i>	<i>JR (first instance decision of 5)</i>	<i>See above</i>	1. <i>Relevant regulations should be construed as saying that money earned but not paid during an assessment period was nonetheless 'income' from that assessment period. SSWP's construction was wrong.</i> 2. <i>Relevant regulations produced an unreasonable and irrational result</i> 3. <i>Breach of Art 14 ECHR read with A1P1</i>	4
7.	ADL v SSHD [2024] EWHC 994 (Admin)	JR	GPS tagging of people on immigration bail. GPS tagging includes use of algorithmic decision support tool, however this element was not directly at issue.	Full list of issues at [117] Automated element of system not directly at issue.	4



8.	R (Nelson) v SSHD (2024) JR-2023-001472	UT	GPS tagging of people on immigration bail. GPS tagging includes use of algorithmic decision support tool but not used in individual claimant's case [45]	1. Breach of Art 8 ECHR 2. Imposition irrational as based on factual errors and irrelevant factors 3. Collection of trail data for the purpose of immigration claim is ultra vires (Home Office did not access data) 4. Requiring claimant to wear a broken tag was ultra vires	4.
9.	R (S and AZ) v SSHD, SSD [2022] EWCA Civ 1092	JR (appeal)	Automated application processing system	1. Application for leave outside of the rules should have been considered even though it wasn't made using the online procedure - the online form required information that the applicants could not provide (irrational and procedurally unfair)	4
10.	R (S) v SSFCDA, SSHD [2022] EWHC 1402 (Admin)	JR	See above	See above	4
11.	Pre-action correspondence - Home Office sham marriage algorithm ⁸³	JR (PAP)	Algorithmic 'triage' tool relating to decisions on whether couples planning to get married should be subject to a sham	1. Indirect discrimination, 2. Failure to comply with PSED 3. Breach of UKGDPR transparency requirements 4. Limitations in human involvement inconsistent with published policy	2

⁸³ Public Law Project, [Legal action launched over sham marriage screening algorithm - Public Law Project.](#)



			marriage investigation.	5. Limitation in human involvement constitutes improper delegation	
12.	R (Blundell) v SSWP [2021] EWHC 608 (Admin)	JR	Fully automated deductions process [116] - issues arose from over-general rigid rule of deducting at a fixed rate	1. Fettering of discretion 2. Irrationality (unsuccessful) 3. Discrimination 4. PSED	4
13.	R (Phillip Freeman Mobile Welders Ltd) v Pensions Regulator [2024] UKFTT 91 (GRC)	UT	Automatic issuance of penalty notice	1. Determination of whether notice was received and delivered	4
14.	R (R) v [2013] EWHC 2864 (Admin)	JR	Risk scoring matrix for police forces to prioritise which homicide/sexual offences convicts to contact to take DNA samples.	1. Unlawful interference with Art 8 ECHR	4
15.	R (X) v Parole Board [2022] EWHC 2319 (Admin)	JR	Risk scoring matrix for parole decisions - not central to case	1. Failure to give adequate reasons 2. Ultra vires	4



16.	DWP Advances Fraud Machine Learning	JR	Machine learning model	1. Failure to follow policy 2. Breach of principle of transparency/duty to publish/systemic unfairness 3. Art 22 UKGDPR 4. EA2010 discrimination 5. Art 14 ECHR 6. Breach of withdrawal agreement 7. PSED	3
17.	Pre-action correspondence - A Level algorithm ⁸⁴	JR	A level algorithm	1. Discrimination 2. Insufficient inquiry 3. Relevant & irrelevant considerations	2 ⁸⁵
18.	Pre-action correspondence 2- A Level algorithm ⁸⁶	JR	A level algorithm	1. Systemic procedural unfairness 2. Ultra Vires 3. Discriminatory	2 ⁸⁷
19.	R (The Joint Council for the Welfare of Immigrants) v Secretary of State	JR	Rule-based algorithm	1. Direct discrimination (s. 29(6) EqA 2010) 2. Irrationality and / or irrelevant considerations 3. Failure to conduct a lawful DPIA 4. Breach of the PSED	3 ⁸⁸

⁸⁴ Cornerstone Barristers, [U-turn on A-level algorithm in wake of JR threats | Cornerstone Barristers](#), 17 August 2020

⁸⁵ n74

⁸⁶ Good Law Project, [Legal action over A-Level results fiasco | Good Law Project](#)

⁸⁷ Good Law Project, [Update: A-Level results fiasco | Good Law Project](#)

⁸⁸ Case settled: Electronic Immigration Network, [Home Office suspends use of digital streaming tool for visa applications after legal action by JCWI and Foxglove | Electronic Immigration Network](#)



	for the Home Department				
20.	R (Shaun Thompson and Silkie Carlo) v The Commissioner of Police of the Metropolis and The Equality and Human Rights Commission (Intervener) [2026] EWHC 915 (Admin)	JR	Facial recognition technology	1. Art 8 ECHR 2. Art 10 ECHR 3. Art 11 ECHR	4
21.	Pre-action correspondence - DWP fraud prediction tools ⁸⁹	JR	Data matching	1. Art 22 UKGDPR 2. Art 14 ECHR 3. PSED 4. DPIA insufficiency	3 ⁹⁰
22.	PAP – Met Police facial recognition	JR	Facial recognition technology	Not publicly available	3

⁸⁹ [DWP faces legal action over use of algorithm in decisions over fraud investigations; GMCDP & Foxglove Legal Challenge to the Department for Work and Pensions DWP Fraud Algorithm | Greater Manchester Coalition of Disabled People](#)

⁹⁰ [We forced the DWP to explain its benefits fraud algorithm: here's what we found - Foxglove](#)



	surveillance (2018) ⁹¹				
23.	Khan Properties Ltd v HMRC [2017] UKFTT 830 (TCC)	FTT	Automated issuing of penalty notice	1. Whether penalty was validly determined under s. 100(1) Taxes Management Act	4
24.	R (Ames) v Lord Chancellor [2018] EWHC 2250 (Admin)	JR	Automated calculator	1. Irrationality (failure to correct error) 2. Failure to publish policy	4
25.	R (Eisai Ltd) v National Institute for Health & Clinical Excellence [2008] EQCA Civ 438	JR	Economic model	1. Procedural unfairness	4
26.	R (Servier Laboratories Ltd v National Institute for Health & Clinical Excellence) [2009] EWHC 281 (Admin)	JR	Economic model	1. Procedural unfairness 2. Failure to take into account a relevant reason 3. Unlawful discrimination	4

⁹¹ [Legal challenge launched over "dangerously authoritarian" facial recognition cameras](#)



B. UKGDPR complaints

	Complaint / enforcement action	Type (Judicial Review (JR), Upper Tribunal (UT), Regulatory)	Tool description	Grounds	Outcome
1.	ICO Enforcement Notice 28.02.24 (Home Office pilot of GPS electronic monitoring)	Regulatory - ICO enforcement notice (satellite to 7 in JR mapping above)	Pilot of GPS electronic monitoring of migrants (satellite to row 7 Judicial Review mapping above)	1. DPIA of GPS tracking pilot inadequate 2. Failure to demonstrate compliance with Article 5(1) UKGDPR	Enforcement notice and warning issued
2.	ICO complaint 15.08.25 (Home Office use of automated recommendation tools in immigration operations) ⁹²	Regulatory - ICO complaint	Two automated recommendation tools – the Identify and Prioritise Immigration Cases (IPIC) tool and Electronic Monitoring Review (EMRT) tool	1. Art 22 - right and transparency 2. UKGDPR - no lawful basis for processing	Decision pending

⁹² <https://privacyinternational.org/legal-action/complaint-against-uks-automated-recommendation-tools-immigration-operations>



C. FOIA complaints, decision notices and appeals

	Litigation / complaint	Type (Judicial Review (JR), Upper Tribunal (UT), ICO decision notice)	Tool description	Subject of complaint
1.	Elsbury v Information Commissioner [2025] UKFTT 915 (GRC)	FTT (GRC) - appeal of 2	Large Language Model (LLM) used by HM Revenue & Customs (HMRC)	Reliance on section 31(1)(d) FOIA (prejudice to the assessment or collection of tax or duty).
2.	IC-298140-V1D6	ICO decision notice	LLM usage by HMRC	See above
3.	PLP v ICO [2024] UKUT 71 (AAC)	UT – appeal of 4	Sham marriage algorithm	Reliance on sections 31(1)(a)(prevention and detection of crime) to redact assessment criteria in an Equality Impact Assessment
4.	PLP v ICO [2023] UKFTT 102 (GRC)	FTT (GRC)(appeal 5)	Sham marriage algorithm	See above
5.	IC-130877-COS1	Regulatory - ICO decision notice (related to 17)	Sham marriage algorithm	See above
6.	ICO Decision Notice	ICO decision notice	Burglary ‘solvability model’	Reliance s.12(1) FOIA (cost limit)



	28.01.19 FS50798023			
7.	IC-64889-B9C2	ICO decision notice	None disclosed	Whether information was not held.
8.	IC-70514-H7K5	ICO decision notice	A-level algorithm	Reliance on section 36(2)(c) FOIA (prejudice to the effective conduct of public affairs)
9.	IC-160077-Z7M0	ICO decision notice	DWP Integrated Risk and Intelligence Service	Reliance on section 31(1)(a) ICO agreed (prejudice to the prevention and detection of crime)
10.	IC-170221-G9L8	ICO decision notice	Trial predictive policing algorithm	Reliance on sections 31(1)(a) (prejudice to the prevention and detection of crime) and 31(1)(b) (prejudice to the apprehension or prosecution of offenders)
11.	IC-169615-H7Z3	ICO decision notice	Advances fraud machine learning model	Reliance on section 31(1)(a) (prejudice to the prevention and detection of crime) - changed to reliance on section 12(1) (cost limit)
12.	IC-186305-M7N7	ICO decision notice	Transaction risking	Reliance on section 31(1)(a) (prejudice to the prevention and detection of crime)
13.	IC-193012-J8T2	ICO decision notice	Advances fraud machine learning model	Reliance on section 31(1)(a) (prejudice to prevention and detection of crime) changed to s.12(1) (cost limit)
14.	IC-282814-Z7W5	ICO decision notice	Universal Credit machine learning	Reliance on section 31(1)(a) (prejudice to prevention and detection of crime)
15.	IC-320077-T2C7	ICO decision notice	Automated Facial Recognition	Reliance on section 24(2) (required to safeguard national security)



Public
Law
Project