Information Commissioner's Office

Update to automated decision making guidance – Draft Impact Assessment

March 2026

ico.
Information Commissioner's Office

Contents

Executive Summary 4
1. Introduction 7
1.1. Report structure 8
2. Problem definition 9
2.1. What is automated decision-making (ADM)? 9
2.2. Current data protection landscape 10
2.3. Prevalence of ADM in the UK 10
2.4. Applications of ADM 11
2.5. Market challenges – ensuring clarity 13
3. Rationale for intervention 15
3.1. Policy and legislative context 15
3.2. Market failures 16
3.3. Data protection harms and ADM 17
4. Options appraisal 19
4.1. Critical Success Factors (CSFs) for options appraisal 20
4.2. Assessment of options 21
5. Detail of proposed intervention 27
5.1. The guidance update 27
5.2. Scope of draft guidance update 30
5.3. Affected groups 30
6. Cost-benefit analysis 34
6.1. Identifying impacts 34
6.2. Counterfactual 35
6.3. Costs and benefits 36
6.4. Overall assessment 43
7. Monitoring and review 46
A.1 Familiarisation costs 47

Familiarisation costs per organisation 47

Executive Summary

This draft impact assessment (IA) accompanies the ICO's draft guidance update on automated decision-making (ADM), including profiling.

The guidance update clarifies key concepts introduced or refined through the Data (Use and Access) Act 2025 (DUAA), such as the definition of a solely automated decision, how to assess what lawful basis may be most appropriate for ADM, how these interact with the new special category data conditions for ADM, and what each of the four safeguards mean. The guidance therefore gives organisations regulatory certainty while strengthening protections for individuals. As well as uncertainty about scope and safeguards, there is evidence of inconsistent implementation of meaningful human involvement and transparency, alongside risks of data-protection harms. The IA assesses the potential impact of the guidance update, above and beyond the effects of the legislation itself.

This document sets out our initial IA of the draft guidance update. As this represents our early assessment, we are seeking feedback from stakeholders throughout the consultation period, including any additional evidence or information on potential impacts. This feedback will be used to inform our final policy decisions and ensure that the intervention remains proportionate to the issues identified and does not create undue burdens for those in scope. A revised and conclusive IA will be published alongside the final guidance update.

Problem definition

ADM systems have the potential to be used to make high impact decisions about individuals. Whilst these systems create opportunities for efficiencies in decision making, its use in certain contexts raises important questions about fairness, accountability, transparency and oversight.

Although only 1% of UK businesses reported using ADM in 2024, adoption is significantly higher among large organisations (10% of UK businesses in 2024) and throughout the public sector, where ADM already supports functions such as welfare eligibility checks and fraud detection. Organisations report an ongoing lack of regulatory certainty about how ADM requirements apply in practice and levels of human oversight vary widely. At the same time, public concern about automation is strong: 91% of UK adults have concerns that important decisions could be made by computers without human input. These factors create risks of inconsistent practice, unfair outcomes, and data-protection harms as ADM adoption grows.

The problem therefore extends beyond lack of regulatory certainty alone to include variable practice and weak safeguards, which heighten the risk of data protection harms and undermine public confidence.

Rationale for intervention

The ICO has a statutory role to interpret and clarify data-protection requirements. After DUAA reforms moved ADM to a safeguards-based regime, organisations need to have clear, practical expectations to apply the law consistently across sectors and use-cases. Without intervention, a lack of regulatory certainty around the processing that falls in scope, meaningful human involvement, and how to apply the safeguards is likely to persist, creating a barrier to responsible adoption and increasing the risk of data-protection harms and market failure as ADM scales.

Option appraisal

In the context of the identified problem and rationale for intervention, four options were considered. These options were assessed against a number of critical success factors and the preferred option of a consolidated guidance update across UK GDPR and Part 3 of the Data Protection Act was selected.

Details of proposed intervention

The guidance update provides practical direction on identifying ADM, determining meaningful human involvement, using the appropriate lawful basis, and applying safeguards. It aims to improve consistency across sectors, improve regulatory certainty, and help organisations build accountability into ADM systems. A theory of change outlines how clearer expectations are expected to lead to improved compliance, reduced data protection related harms, and increased trust.

Cost benefit analysis

This draft assessment has identified a number of impacts of the draft guidance update including the reduced potential for data protection related harms. The guidance update is expected to increase regulatory certainty for developers and adopters of ADM systems. Although there will be costs to organisations from reading, understanding, and implementing the guidance update, this is expected to be outweighed by the wider societal benefits of reduced data protection harms and a reduced need for external legal advice amongst those seeking to adopt ADM.

At this draft stage of guidance update, we expect the guidance to have a net positive impact on balance. However, we will seek to gather additional information on the potential costs and benefits of the guidance update

throughout consultation and development of our final guidance update and impact assessment.

Monitoring and review

When finalising the guidance update post consultation, we will consider the monitoring and review processes. This intervention sits within our wider AI and Biometrics Strategy. As such the outcomes and impacts of this intervention will feed into wider ex-post impact measurement carried out on the AI and Biometrics Strategy.

1. Introduction

This document sets out a draft IA of our proposed intervention to increase regulatory certainty around the compliant adoption of ADM technologies.

The purpose of an IA is to improve regulatory interventions and policymaking by:

- informing decision-makers about potential economic, social, and (where relevant) environmental ramifications;
- providing a mechanism to consider the impact of interventions on a range of stakeholders, including different groups of citizens and organisations;
- improving the transparency of regulation by explicitly setting out the intervention theory of change and the quality of underlying evidence; and
- increasing public participation to reflect a range of considerations, improving the legitimacy of policies.

IA is also a key mechanism that helps the ICO to meet its principal objective and wider duties under Section 120A and Section 120B of the Data Protection Act (DPA) 2018.

This document sets out our initial IA of the draft guidance update. As this represents our early assessment, we are seeking feedback from stakeholders throughout the consultation period, including any additional evidence or information on potential impacts. This feedback will be used to inform our final policy decisions and ensure that the intervention remains proportionate to the issues identified and does not create undue burdens for those in scope. A revised and conclusive IA will be published alongside the final guidance update.

We have assessed the potential impacts of the approach using cost benefit analysis. Our approach follows the principles set out in the ICO's Impact Assessment Framework,[1] which is in turn aligns with HM Treasury's Green Book.[2]

---

[1] ICO (2023) *The ICO's Impact Assessment Framework.* Available at: https://ico.org.uk/media2/about-the-ico/documents/4027020/ico-impact-assessment-framework.pdf (Accessed February 2026)
[2] HMT (2020) The Green Book. Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020 (Accessed February 2026)

1.1. Report structure

The remainder of this report is structured as follows:

- **Section 2: Problem definition** sets out the evidence base to support the identification of the problem that the intervention aims to address.
- **Section 3: Rationale for intervention** considers the rationale for intervention by exploring whether there is market failure and highlighting the legislative and policy context.
- **Section 4: Options appraisal** assesses potential options for intervention against critical success factors.
- **Section 5: Details of proposed intervention** provides an overview of the approach and sets out the key groups that are expected to be affected.
- **Section 6: Cost-benefit analysis** presents identified costs and benefits of the approach, across each of the affected groups.
- **Section 7: Monitoring and review** outlines future monitoring considerations to ensure the impact of the intervention, and any lessons learned are captured.
- **Annex: Familiarisation costs**

2. Problem definition

Problem definition

Where Automated decision-making (ADM), including profiling, is used, the processing will by default have a high impact on individuals. Whilst these systems create opportunities for efficiencies in decision making, their use in certain contexts raises important questions about fairness, accountability and human oversight.

While overall penetration of ADM remains modest (1% of UK businesses in 2024[3]), adoption is far higher among large organisations (10% of businesses) and is already embedded in the public sector (e.g., welfare eligibility checks and fraud detection). Organisations report an ongoing lack of clarity about how ADM requirements apply in practice, and oversight approaches vary widely. At the same time, public concern is strong: 91% of adults worry that important decisions could be made by computers without human involvement. Together, these factors increase the risk of inconsistent practice, unfair outcomes, and data-protection harms as ADM adoption grows.

In summary - alongside uncertainty, there is inconsistent oversight, unclear implementation of safeguards, and strong public concern about fairness, transparency and meaningful human involvement in automated decisions.

2.1. What is automated decision-making (ADM)?

ADM refers to decisions made about people where the outcome is based solely on automated processing (i.e. there is no meaningful human involvement), including profiling, and where the decision has a legal or similarly significant effect. Recent updates to the UK GDPR have revised the ADM framework, shifting away from a prohibition-based model to a requirement that organisations put in place rights-based safeguards whenever solely automated significant decisions are made. This change expands the circumstances in which organisations can use ADM, while creating a greater need for clarity about what counts as a "decision",

[3] DSIT (2024) *UK Business Data Survey 2024.* Available at: https://www.gov.uk/government/statistics/uk-business-data-survey-2024/uk-business-data-survey-2024 (Accessed March 2026).

when a decision is "solely automated", and how the safeguards should be applied in practice.

ADM systems are commonly used across contexts including recruitment, financial services, welfare administration and access to public services. Drivers of ADM adoption typically reflect organisational efficiency pressures, and expectations around its capacity to provide speed, scale, consistency and task delegation to decision making.

2.2. Current data protection landscape

Recent updates to Article 22 of UK GDPR have led to a new legal framework that provides organisations with greater flexibility to undertake ADM, provided certain safeguards are met. This marks a departure from the previous approach, which prohibited solely automated decisions with significant effects except under specific conditions.

2.3. Prevalence of ADM in the UK

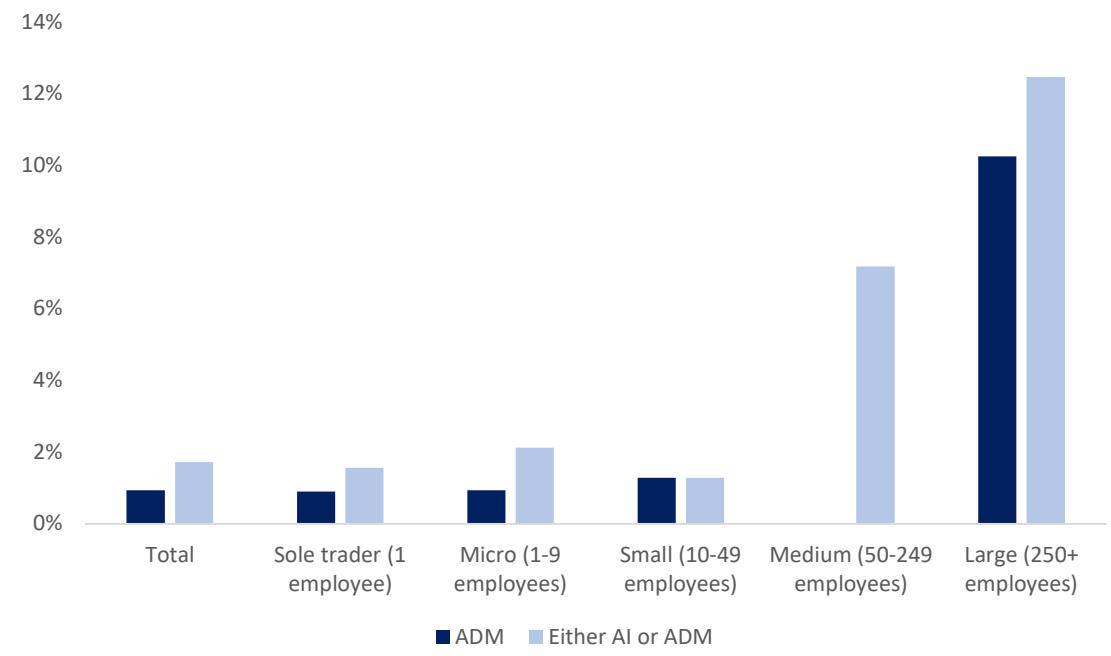
Overall adoption of ADM remains modest. In 2024, 1% of UK businesses handling digitised personal data reported using ADM technologies.[4] Usage typically varies by business size with adoption rates ranging from 1% amongst small businesses to 10% in larger firms.

These differences likely reflect disparities in data availability, technical capability, and digital maturity. Larger organisations typically hold richer datasets, operate at scale and have greater capacity to develop or procure ADM. For SMEs, lower adoption likely reflects resource constraints and more limited access to relevant skills.

That said, because ADM requires the absence of meaningful human involvement, many organisations classify their systems as "AI-enabled analytics" or "decision support" rather than ADM. This implies true ADM prevalence is low not because automation isn't used, but because many systems retain a level of human involvement.

[4] DSIT (2024) *UK Business Data Survey 2024.* Available at: https://www.gov.uk/government/collections/business-data-survey (Accessed Feb 2026).

Figure 1: Percentage of businesses using AI & Automated Decision Making in 2024



Source: DSIT, Business Data Survey 2024

2.4. Applications of ADM

ADM offers the potential for improved efficiency and consistency for society and the wider economy, with potential benefits including:

- faster processing times that support quicker decisions and outcomes for consumers;
- greater consistency in the application of rules and policies;
- enhanced fraud detection; and
- enhanced personalisation of services, 92% of businesses report using AI-driven personalisation techniques.[5]

However, the same operational advantages that make ADM attractive also increase the potential for negative impacts when errors, biases or misunderstandings occur, especially where decisions materially affect people's rights or access to essential services.

Public concern about ADM is high, with 91% of UK adults expressing concerns that important decisions about them will increasingly be made

[5] The State of Personalization Report 2024 | Twilio Segment.

by computers without human involvement.[6] This indicates widespread unease about reducing human judgement in consequential decision-making contexts.

2.4.1. Sector specific ADM use cases

Despite overall low adoption of ADM, its use is becoming increasingly common in sectors such as financial services and the public sector. Below, we outline illustrative use cases that demonstrate how ADM is being applied in practice.

Financial services

ADM is well established in financial services. In 2024:

- 75% of UK financial firms reported using AI; and
- 55% of these AI applications involved ADM.[7]

These systems support activities such as affordability assessments, anti-money laundering (AML), fraud detection, and cybersecurity. While the majority of ADM use cases in this sector are considered "low materiality" (62%), a notable subset of applications, such as automated credit scoring, have potential for high-impact outcomes. Only 2% of financial ADM use cases are fully autonomous. Reported benefits include improved productivity, cost efficiencies and more consistent risk management.

Government and public services

ADM is extensively used by public bodies to streamline routine decisions, undertake eligibility checks and identify fraud. Since 2024, when the Algorithmic Transparency Recording Standard[8] (ATRS) was introduced,

---

[6] DSIT (2024) *Public attitudes to data and AI: Tracker survey (Wave 4)*. Available at: https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey-wave-4/public-attitudes-to-data-and-ai-tracker-survey-wave-4-report (Accessed Feb 2026).
[7] Bank of England (2024). *Artificial intelligence in UK financial services.* Available at: https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024 (Accessed Feb 2026).
[8] Government Digital Service (2024) *Algorithmic Transparency Recording Standard*. Available at: https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub (Accessed Feb 2026).

central government departments and arm's-length bodies have been required to publish details of algorithmic tools that have a significant influence on decision-making processes with public effect, or that directly interact with the public. This includes ADM systems in use.

As of November 2025, more than 100 systems were listed on the ATRS register. This includes tools used in:

- welfare fraud detection;
- Universal Credit risk scoring;
- child maintenance compliance;
- tax investigation and prioritisation;
- environmental monitoring; and
- education assessment routing.

ADM deployment has the potential to lead to cost efficiencies in public service delivery. For example, the Department for Work and Pensions (DWP) estimates that the algorithmic systems used to detect Universal Credit fraud could generate savings of £1.6bn by 2030–31.[9]

2.5. Market challenges – ensuring clarity

While no single factor determines whether firms deploy new tools, regulation is a consistently strong influence on adoption decisions. In practice, uncertain or evolving regulatory expectations increase perceived risk and can delay or deter the deployment of AI and automated decision-making technologies.

- Among larger UK firms, regulatory compliance is cited as one of the top barriers to adoption (34%), underscoring the importance of clear rules and expectations.[10]

[9] Department for Work and Pensions (2023) *Fighting Fraud in the Welfare System: Going Further*. https://www.gov.uk/government/publications/fighting-fraud-in-the-welfare-system-going-further (Accessed Feb 2026).
[10] ANS (2025) *AI Readiness – How ready are UK businesses for AI?* Available at: https://www.ans.co.uk/data-ai/ai-readiness/ (Accessed Feb 2026).

- In addition, over one-third (37%) of UK businesses leaders have no plans to integrate AI into their workplaces, largely due to a lack of regulatory clarity.[11]

This indicates that a lack of clarity over what compliance looks like in practice remains a significant barrier to responsible adoption.

Oversight practices among AI adopters vary widely.[12] While most organisations report some form of human input, 84% say they check automated outputs and 67% report significant checking, only 2% report no oversight at all.[13] ICO-commissioned research on public perceptions of ADM in recruitment found that people place strong importance on fairness, transparency and meaningful human oversight, and express significant concern about fully automated decision-making in hiring contexts.[14] Participants also reported limited understanding of how ADM works and emphasised the need for clear information about when automated systems are used and how decisions are made.

This indicates that ambiguity about compliance is a significant barrier and that clearer expectations about effective human involvement, transparency and fairness checks are needed to support responsible adoption.

[11] TechRadar (2025) *Lack of clarity on AI regulation could be holding back businesses.* Available at: https://www.techradar.com/pro/lack-of-clarity-on-ai-regulation-could-be-holding-back-businesses (Accessed Feb 2026).
[12] Note that not all AI processing will include ADM.
[13] DSIT (2024) *AI Adoption Research Report.* Available at: https://assets.publishing.service.gov.uk/media/6960f3924343a0da370869ba/AI_Adoption_Research_Report.pdf (Accessed Feb 2026).
[14] ICO (2025) *"Understanding public perceptions towards automated decision-making in recruitment."* (Accessed March 2026).

3. Rationale for intervention

Uncertainty around ADM scope and safeguards, together with inconsistent oversight practices and the risk of data-protection harms, creates a need for regulatory intervention. The ICO is best placed to address these issues given its statutory role in interpreting and enforcing UK GDPR and DUAA provisions, its responsibility for setting expectations around fairness, transparency and meaningful human involvement. Regulatory intervention in this area could have the potential to improve compliance, strengthen safeguards and support responsible adoption.

This section sets out the rationale for intervention and why the ICO is best placed to solve the problems identified in Section 2. It considers the policy and legislative context, market failures this intervention seeks to address and data protection harms.

3.1. Policy and legislative context

It is important to consider the wider policy and legislative context, including DUAA reforms to the ADM regime and relevant GDPR provisions.

3.1.1. ICO policy

The ICO's Artificial Intelligence and Biometrics Strategy[15] identifies ADM as a priority area requiring clarifying guidance update and strengthened safeguards. The strategy commits the ICO to:

- Consulting on updated ADM and profiling guidance update to reflect reforms introduced through the Data (Use and Access) Act, with a public consultation planned before the statutory code of practice is produced;
- Promoting clear and practical expectations on transparency, explainability, bias mitigation and redress, to ensure organisations can deploy ADM responsibly;
- Setting clear expectations for the responsible use of automated decision-making in recruitment; and

[15] ICO (2025) *"AI and Biometrics Strategy"* Available at: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/artificial-intelligence-and-biometrics-strategy/ (Accessed March 2026).

- Securing assurance from central government departments that ADM systems are used fairly, with appropriate oversight and monitoring.

These actions are intended to give organisations certainty on how they can use AI and ADM responsibly under data protection law, while maintaining high standards of individual rights and trust.

3.1.2. Legislative context

ADM in the UK is governed by a combination of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The DUAA reforms the ADM regime by replacing the original Article 22 framework with Articles 22A–22D. These amendments reset the statutory thresholds for what counts as a "significant decision" (legal or similarly significant effects), clarify when a decision is "solely automated" (i.e., absent meaningful human involvement), and codify safeguards that controllers must apply.

3.2. Market failures

This section explains the main market failures that can arise from a lack of regulatory certainty around when organisations use ADM.

3.2.1. Information asymmetry

People often do not know when ADM is used, what data it uses, or how the decision was reached. Organisations can also be unsure about key concepts. For example, what counts as a "decision", when a decision is "solely automated", or what "meaningful human involvement" looks like. These information gaps could be reduced by enhanced regulatory clarity setting out what organisations must tell people, and how Article 22 safeguards should work in practice.

3.2.2. Negative externalities

When ADM goes wrong, the costs are often borne by individuals, such as delays, stress or unfair outcomes, rather than by the organisations that deploy the systems. Enhancing regularity clarity could help internalise these costs by clarifying expectations for explainability, audit trails, and timely human intervention, before a decision is applied.

3.2.3. Power imbalances and limited competition

In some public sector context, people may have little choice but to accept ADM (as individuals cannot easily switch providers). If processes are opaque, they can feel powerless to understand or challenge outcomes. Enhancing regularity clarity could strengthen practical routes to explanation and challenge, helping to rebalance these power dynamics.

3.3. Data protection harms and ADM

ADM systems can lead to individual and societal harms, especially where used to make decisions that have material outcomes – such as access to essential services or benefits.

Data protection harms[16] can arise where models are inaccurate, biased, or where human involvement is not meaningful enough to prevent errors before consequential actions are taken. This matters in high-stakes contexts, such as welfare eligibility and fraud detection, where false positives or biased flags can lead to financial harm, distress and unfair treatment for those affected.

ADM can also adversely affect individuals' wider rights and freedoms. Barriers to exercising legal rights, such as lack of clarity about when automated decisions are made, unclear routes to challenge, or insufficient explanation, can limit people's ability to challenge outcomes or secure meaningful human review. These barriers may undermine core data-protection rights around transparency, fairness and redress, particularly where automated tools operate at scale or where individuals have limited choice of provider.

At a societal level, systemic inaccuracies, biased outcomes, or opaque ADM deployments can contribute to an erosion of trust in institutions, services or public bodies that rely on automated tools.

3.3.1. Financial and psychological harm

ADM tools have the potential to cause financial harm. For example, in a welfare context benefit claimants may be flagged for erroneous investigations. False-positive rates within models could result in legitimate claimants being incorrectly flagged, subjected to extended review

[16] ICO (2022) *"Overview of Data Protection Harms and the ICO's Taxonomy."* Available at: https://ico.org.uk/media2/migrated/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf (Accessed March 2026).

procedures, and experiencing income disruption. Furthermore, if individuals are unable to comprehend or challenge decisions made by ADM systems, this may contribute to anxiety and psychological distress.

Outside of welfare, ADM poses financial risks across the private sector. Automated credit scoring, insurance pricing, fraud-detection, dynamic pricing, gig-economy work allocation and algorithmic recruitment all carry the potential to produce misclassifications that reduce people's access to employment, increase their cost of living, suspend access to funds, or trigger inappropriate enforcement actions.

Discrimination

Bias can enter ADM through training data and design choices. If models learn from historic patterns, they can entrench biases against specific groups and discriminate against individuals with certain characteristics—even when those characteristics are not lawful or relevant risk factors.

Example of ADM related harms: risks identified in ICO audits of AI in recruitment

ICO audits of AI-powered sourcing, screening and selection tools found concrete risks to people's information rights where recruitment systems are designed or configured without adequate safeguards. The audits identified features that could facilitate discriminatory outcomes (e.g. filters enabling recruiters to exclude candidates by protected characteristics), instances of inferring sensitive attributes (such as gender or ethnicity) from names or application text without an appropriate basis, gaps in accuracy and bias testing, and excessive collection/retention of personal data (including large pools of scraped data) with limited transparency to candidates. Collectively, these practices increase the risk of unfair or discriminatory treatment, opaque decision-making and loss of control over personal information in a high-stakes context.[17]

[17] ICO (2025) *"AI tools in recruitment."* Available at: https://ico.org.uk/media2/migrated/4031620/ai-in-recruitment-outcomes-report.pdf (Accessed March 2026).

4. Options appraisal

The following options were selected as part of the ICO's AI and Biometrics strategy:

- **Option 1:** Business as usual – minimal guidance updates
- **Option 2:** Do less – update only Part 2 of core GDPR guidance (excludes Part 3)
- **Option 3:** Preferred way forward - update guidance and provide regulatory clarity over key concepts
- **Option 4:** Do more – update guidance and commission landscape review

Following an appraisal against a number of Critical Success Factors, Option 3 - update guidance and provide regulatory clarity over key concepts - emerged as the preferred way forward.

This section provides an overview of the regulatory options considered in response to the problem definition.

The ICO is best placed to address the problems set out in Section 2 given its statutory role in interpreting and enforcing UK GDPR and DPA 2018 requirements, including the amended Articles 22A–22D introduced through the DUAA. In discharging this role, the ICO has access to a range of regulatory tools that can be deployed. These include:

- Guidance and regulatory expectations;
- Codes of practice;
- Supervisory engagement;
- Audits and upstream monitoring;
- Advice and sandbox functions and
- Enforcement powers where appropriate.

Identifying appropriate regulatory tools formed part of the ICO's AI and Biometrics Strategy, which committed the ICO to enhancing regularity certainty by updating 'our ADM and profiling guidance'. Thus, the remainder of this options appraisal section assesses the parameters and forms of guidance-based intervention that could be address the problem definition. The options considered are set out below.

Option 1: Business as usual – minimal guidance updates

Make minimal updates to existing guidance, focusing only on the most essential changes required by DUAA. Avoids broader clarification or consolidation of concepts like "decision" or "legal or similarly significant effects."

Option 2: Do less – update only Part 2 of core GDPR guidance (excludes Part 3)

This option involves updating the core guidance to reflect changes required by the DUAA, but only for Part 2 (UK GDPR). Part 3, covering law enforcement, would not be updated at this stage.

Option 3: Preferred way forward - update guidance and provide regulatory clarity over key concepts

Update suite of existing guidance covering UK GDPR and Part 3 of the DPA. Clarify and consolidate definitions and expectations around:

- What constitutes a "decision" in ADM.
- What is "meaningful human involvement" (MHI).
- What are "legal or similarly significant effects" (L/SSE).
- The safeguards required for ADM.

This option includes a public consultation of the UK GDPR guidance update, and a more limited targeted consultation of specific stakeholders for Part 3 of the DPA.

Option 4: Do more – update guidance and commission landscape review

Provide detailed guidance on the stages of automation, specifying the varying degrees of human involvement and offering clear direction on which stages constitute meaningful human involvement.

In addition to updating guidance, commission a comprehensive review of technical and organisational measures (including third-party services) that could support compliance.

4.1. Critical Success Factors (CSFs) for options appraisal

The following critical success factors (CSFs) were used to appraise intervention options.

1. Strategic fit

- How well does the option align with government and organisational objectives, such as promoting responsible innovation, supporting economic growth, protecting individual rights, and upholding public trust in data-driven decision-making?

2. Deliverability and feasibility

- Can the option be practically implemented by organisations and enforced by regulators, given current technical, legal, and organisational constraints?

3. Stakeholder confidence and trust

- To what extent does the option enhance confidence among individuals, regulated entities, and the wider public that ADM is used fairly, transparently, and lawfully?

4. Risk management

- How effectively does the option identify, assess, and mitigate risks associated with ADM, such as risks of non-compliance, legal challenge, reputational harm, algorithmic bias, or the undermining of individuals' rights due to lack of meaningful human involvement?

5. Impact

- What is the scale and significance of the option's expected benefits and risks, including its effect on individuals, organisations, and the wider public interest?

4.2. Assessment of options

This section evaluates the options against the CSFs outlined above, including strategic alignment with organisational objectives, practical deliverability and feasibility, stakeholder confidence and trust, risk management, and overall impact.

The preferred option, updating and consolidating guidance to provide regulatory clarity over key concepts in automated decision making (ADM), was selected following a structured appraisal against the critical success factors above. This assessment is summarised in Table 1, which uses a RAG (Red-Amber-Green) rating to compare each option's performance across strategic fit, deliverability and feasibility, stakeholder confidence and trust, risk management, and overall impact.

The preferred option emerged as the strongest candidate for several reasons:

- It received the highest number of green ratings across the CSFs, indicating strong alignment with organisational and legislative objectives, practical deliverability, and the ability to enhance stakeholder confidence and trust.
- It had the lowest number of red ratings, suggesting minimal significant risks or barriers to implementation compared to the alternatives.
- Relative to alternative options, it strikes a balance between providing regularity clarity for organisations and safeguards for individuals affected by ADM, while remaining proportionate and feasible for organisations to implement. It avoids the pitfalls of minimal intervention (which risks perpetuating a lack of clarity and inconsistency) and the potential complexity and resource demands of a more expansive review.
- This approach provides an effective interim solution that addresses immediate regulatory needs and expectations, while allowing for further refinement when the statutory code of practice is developed.

Table 1: Appraisal of policy development options relating to ADM guidance update

Option	Strategic Fit	Deliverability	Stakeholder Confidence	Risk	Impact
Business as Usual - Minimal updates to guidance; only essential DUAA changes addressed. No broader clarification of key ADM concepts.	**Red** Fails to address new legal requirements and stakeholder expectations post-DUAA. Does not clarify key concepts or provide necessary regularity certainty, risking misalignment with ICO objectives on responsible innovation, individual rights and public trust.	**Green** **Highly deliverable**: Minimal change, low resource requirement for both ICO and organisations. However, this is because it does not address new legal or technical complexities, not because it is effective.	**Red** **Low confidence and trust**: Fails to address new legal requirements or clarify key concepts. Stakeholders (public, regulated entities, civil society) are likely to perceive the ICO as passive, leading to confusion, inconsistent practice, and reduced trust in ADM safeguards.	**Red** **Poor risk management**: Fails to address new or emerging risks from DUAA changes. Leaves ambiguity in key concepts, increasing the risk of non-compliance, legal challenge, reputational harm, and algorithmic bias. Does not strengthen safeguards for individuals.	**Red** **Individuals:** Weak protection of rights, limited empowerment, continued confusion. **Organisations:** Lack of clarity, inconsistent compliance expectations, risk of legal/reputational harm. **Public Interest:** Erodes trust, risks negative societal and economic outcomes.
Do Less: Update guidance for	**Amber**	**Green**	**Amber**	**Amber**	**Amber**

UK GDPR only; exclude law enforcement. No public consultation; limited stakeholder engagement.	Limited alignment with ICO's strategic goals as it only partially addresses the need for clarity and consistency. Excludes Part 3, leaving gaps in protection and guidance, especially law enforcement services.	**Highly deliverable**: Focused update, limited in scope, easy to implement for most organisations. Avoids complex changes, but leaves gaps for sectors not covered (Part 3).	**Limited improvement**: Provides some clarity for GDPR-regulated entities but leaves significant gaps for the law enforcement sector. Stakeholder trust may improve slightly in covered areas but confusion and lack of confidence will persist elsewhere.	**Partial risk mitigation**: Some improvement for GDPR-regulated sectors, but leaves significant risks unaddressed in law enforcement contexts. Inconsistent guidance increases the risk of gaps in protection and compliance failures.	**Individuals:** Some improvement for those covered by GDPR, but many left unprotected (e.g., law enforcement). **Organisations:** Partial clarity for some, but persistent uncertainty and compliance risk for others; uneven playing field. **Public Interest:** Limited improvement in trust and outcomes; persistent gaps undermine overall impact.
Preferred way forward: Update and clarify guidance across UK GDPR and Part 3; consolidate key ADM	**Green** Strong alignment with ICO objectives. Clarifies and consolidates key concepts, covers all relevant legal regimes and includes public consultation. This supports responsible	**Amber** **Moderately deliverable**: Broader update across all regimes, requires more effort from ICO and regulated entities. Increases clarity but may challenge some organisations	**Green** **Strong confidence and trust**: Comprehensive clarification and consolidation of key concepts, public consultation (of UK GDPR update), and	**Green** **Strong risk management**: Comprehensive clarification and consolidation of key concepts and safeguards	**Green** **Individuals:** Stronger rights, clearer safeguards, greater empowerment. **Organisations:** Regulatory certainty, level playing field, clearer

concepts. Public consultation of UK GDPR and targeted consultation for Part 3; interim solution pending statutory code.	innovation, individual rights and public trust.	(especially smaller ones) to adapt to new definitions and expectations. Feasible, but with moderate resource and change management needs.	alignment across regimes. Stakeholders are likely to perceive the ICO as proactive, transparent, and committed to fairness and rights. Individuals will be better empowered to exercise their rights.	across all regimes. Reduces ambiguity, supports compliance, and addresses risks of bias, legal challenge, and reputational harm. Empowers individuals and organisations to manage risks proactively.	compliance pathways, reduced risk of legal challenge. **Public Interest:** Enhanced public trust, supports responsible innovation, positive societal and economic impacts.
Do More: Update guidance, clarify automation levels, and commission a landscape review.	**Green** Fully aligns with and ICO objectives. In addition to Option 3, it explores technical and organisational measures, supports innovation, and may set new standards for compliance and transparency.	**Red** **Challenging deliverability**: Adds a landscape review and potential new standards/tools. High resource requirement, longer timelines, and may be difficult for smaller organisations to implement technical recommendations. Risk	**Green** **Highest confidence and trust**: Builds on the preferred way forward by adding a landscape review and exploring technical/organisational solutions. Demonstrates leadership and	**Green** **Best practice risk management**: Builds on the preferred way forward by adding a landscape review of technical and organisational	**Green** **Individuals:** Maximised rights protection, transparency, and empowerment. **Organisations:** Access to best practice, technical/organisational solutions, and sector leadership; may require

		of overburdening both ICO and regulated entities.	ambition, further enhancing stakeholder trust and public confidence in ADM safeguards and ICO oversight.	measures. Identifies emerging risks and best practices, supports continuous improvement, and maximises the ICO's ability to anticipate and mitigate risks across the sector.	more resources but supports long-term compliance and innovation. **Public Interest:** Sets benchmark for fairness and trust, supports economic growth and societal benefit, future-proofs regulatory approach.

Source: ICO analysis.

5. Detail of proposed intervention

The draft guidance update aims to assist organisations in understanding and fulfilling their responsibilities when conducting ADM. It outlines updates to UK GDPR due to the Data (Use and Access) Act 2025 (DUAA), explains the pertinent provisions, and offers advice on recommended practices.

This guidance update is aimed at organisations currently deploying or planning to use ADM. This includes deploying ADM tools developed in-house or using solutions offered by external vendors. The draft guidance update seeks to:

- Provide clarity on the scope and application of ADM provisions post-DUAA, ensuring organisations understand when ADM is in scope and what safeguards are required.
- Protect individuals from potentially harmful or unfair automated decisions, especially where there is no meaningful human involvement.

This section provides an overview of the proposed intervention along with a theory of change for the intervention (i.e. the guidance update), which covers the change that the guidance update is expected to bring about. It concludes by providing an overview of the main groups expected to be impacted by the intervention.

The overall aim of this intervention is to provide regulatory certainty to adopters of ADM technologies that process personal information. In order to achieve this, the preferred option of updating the guidance to reflect the changes in Data (Use and Access) Act 2025 was selected.

5.1. The guidance update

The draft guidance update aims to assist organisations in understanding and fulfilling their responsibilities when conducting ADM. It outlines updates to UK GDPR due to the Data (Use and Access) Act 2025 (DUAA), explains the pertinent provisions, and offers advice on recommended practices.

It provides clarity regarding in the following areas.

- How to determine whether processing falls within the scope of the Article 22A of UK GDPR, including solely automated decisions with legal or similarly significant effects.
- What constitutes meaningful human involvement.
- How to identify and apply the appropriate lawful basis for ADM.
- The conditions required when processing special category data for ADM.
- How profiling interacts with ADM.
- The restrictions and conditions organisations must meet when using ADM.

5.1.1. Overarching objectives

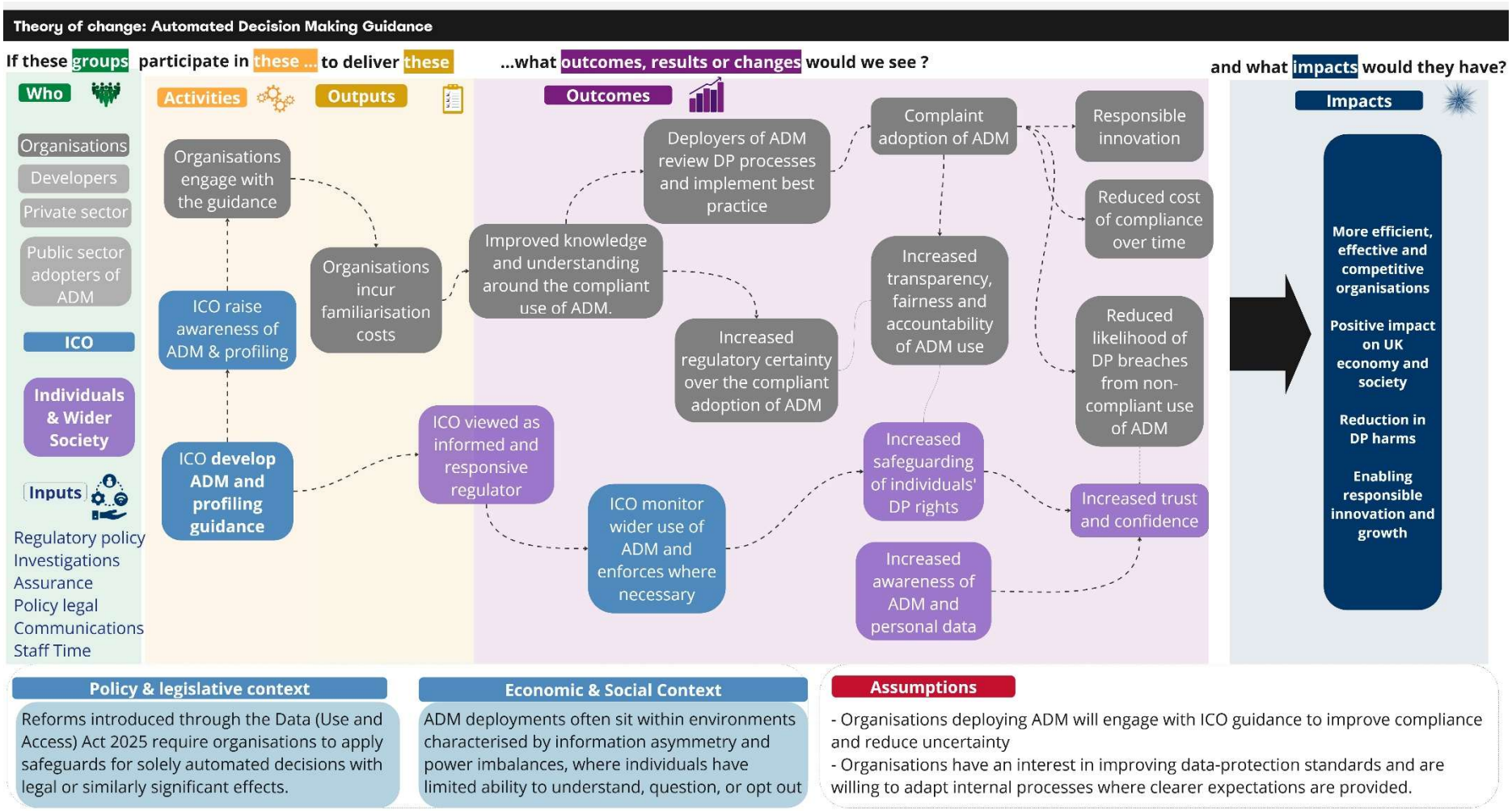
Given the problems identified, uncertainty and inconsistent practice around safeguards, transparency and effective human involvement, the draft guidance update seeks to:

- Provide clarity on the scope and application of ADM provisions post-DUAA, ensuring organisations understand when ADM is in scope and what safeguards are required.
- Protect individuals from potentially harmful or unfair automated decisions, especially where there is no meaningful human involvement.
- Ensure consistency across sectors and legal regimes (UK GDPR, DPA Part 3), reducing compliance burdens and risks of misinterpretation.
- Support innovation and meet our secondary duties by giving organisations clear, tech-neutral rules that can adapt to new ADM use cases.
- To meet legislative and public expectations for the ICO to interpret and clarify the law.

5.1.2. Theory of change

Our draft impact assessment is underpinned by an 'output to outcome to impact' methodology known as 'theory of change'. This shows how the guidance update links to chain of results that lead to intended impacts. It should be noted that impact is often the most challenging aspect to measure since it occurs over a longer timeframe and can be influenced by other external factors. Our theory of change is show in Figure 2 below.

Figure 2: Draft guidance update on Automated Decision Making – theory of change



Source: ICO analysis.

5.2. Scope of draft guidance update

This guidance update is aimed at organisations currently deploying or planning to use ADM. This includes deploying ADM tools developed in-house or using solutions offered by external vendors.

5.3. Affected groups

There are a number of challenges with quantifying the scale of affected groups, including a lack of robust data and evidence. As ADM is a process which is not limited to specific sectors, there are no industry SIC codes which can be used to identify market size, employment or turnover. The majority of evidence on the scale of affected groups is therefore derived from external research, surveys and reports which we have used to provide an indication of scale. We hope to refine these estimates with any further evidence received through the consultation process.

5.3.1. Developers and suppliers of ADM processes

Developers, suppliers and proprietors of ADM processes will need to:

- read and understand the guidance update and how it applies to them; and
- where appropriate, make changes to their internal processes and procedures to reflect the requirements of the guidance update. This may also include updating contracts with purchasers of relevant technologies where relevant and appropriate.

There are no comprehensive and reliable estimates of the number of organisations that develop systems that can be deployed for ADM. In the absence of a dedicated ADM market classification developer landscape, we have developed a proxy using AI capability tags reported within the UK Government's AI sectors study.[18]

The study identifies around 6,000 dedicated and diversified AI companies in the UK, of which 29% (1,684) report capabilities in "Autonomous and Agent Systems" – a category that is likely to include, but is not limited to, organisations developing technologies used for ADM.

[18] DSIT (2024) *Artificial Intelligence Sector Study 2024*. Available at: https://www.gov.uk/government/publications/artificial-intelligence-sector-study (Accessed Feb 2026).

The use of "autonomous and agent systems" as a proxy for systems that can be used for ADM is likely to provide a conservative lower bound estimate of the developer landscape. This is because:

- ADM is not synonymous with AI: many AI applications involve automation or prediction but do not constitute ADM under UK GDPR, and should not be classified as ADM.
- Conversely, some ADM systems do not fall within "autonomous and agent systems".
- Capability tags in the AI Sector Study are self-reported and may reflect marketing choices rather than strict technical definitions.

For these reasons, the proxy should be treated as an imperfect indicator, rather than a comprehensive estimate of the ADM developer population. It helps illustrate the potential scale of organisations that may be affected by guidance update. It does not seek to imply that all AI developers engage in ADM, nor that all ADM developers fall within this category.

There are around 6,000 dedicated and diversified AI companies operating in the UK, 29% (1,684) of these have capabilities in "Autonomous and Agent Systems", and are likely to include ADM based technologies.

5.3.2. Adopters of ADM

Private sector

Adopters of ADM processes will need to ensure they have read, understood and applied the guidance, which may involve making internal changes to data protection processes and procedures.

ADM tools were used by 1% of UK businesses in 2024.[19] Applying this to the UK business population estimates suggests there are a cohort of 44,000 UK businesses that actively use ADM tools.[20]

[19] DSIT (2024) *UK Business Data Survey 2024.* Available at: https://www.gov.uk/government/collections/business-data-survey (Accessed Feb 2026).
[20] DBT (2024) Business population estimates 2024. Available at: https://www.gov.uk/government/statistics/business-population-estimates-2024 (Accessed Feb 2026).

Public sector

ADM is widely applied in the public sector for eligibility checks (eg welfare, benefits etc), fraud detection, and streamlining routine processes. For example, the Department for Work and Pensions (DWP) deploys algorithmic models for detecting Universal Credit fraud, which they estimate could save the UK exchequer around £1.6bn by 2030–31.[21]

Central government departments and arm's-length bodies are required to publish information about how and why they are using algorithmic tools – this includes the use of ADM.

By one independent count there are at least 55[22] automated tools being used by public authorities in the UK (as of 27th November 2025) potentially affecting decisions about millions of people.[23] Ten of these make decisions that affect people's legal rights, entitlements or similarly significant decisions.

5.3.3. Individuals

ADM can process people's data across multiple high-impact contexts. This includes:

- **Welfare and public services:** eligibility and fraud-risk scoring of claimants;
- **Financial services and payments**: automated risk scoring, including open-banking transactions.

A single, reliable count of affected individuals is not currently available because:

- the legal and technical scope is broad;
- the Government's Algorithmic Transparency Recording Standard (ATRS) lists central-government ADM tools but typically does not report volumes processed; and

---

[21] Department for Work and Pensions (2023) *Fighting Fraud in the Welfare System: Going Further*. https://www.gov.uk/government/publications/fighting-fraud-in-the-welfare-system-going-further (Accessed Feb 2026).

[22] Public Law Project (2025) *Tracking Automated Government Register.* Available at: https://trackautomatedgovernment.shinyapps.io/register/ (Accessed Feb 2026).

[23] Public Law Project (2025) *Tracking Automated Government Register.* Available at: https://trackautomatedgovernment.shinyapps.io/register/ (Accessed Feb 2026).

- many ADM deployments, particularly those in local government, health, social care and other locally delivered public services, are not captured in routine public statistics.

Given the prevalence of ADM across the wider public sector, the number of individuals whose data is processed by ADM systems is likely to be in the millions. This is a conservative, order-of-magnitude statement reflecting the diffusion of ADM across large, population-serving systems rather than a point estimate.

5.3.4. ICO

The ICO will be affected, as the regulator of DP legislation and the producer of the guidance update.

5.3.5. Wider society

The guidance update also has the potential to impact other groups and may have indirect effects on wider society.

It is challenging to estimate who the guidance update would and wouldn't affect indirectly. As such we estimate the whole UK population (69 million individuals[24]) as an upper bound estimate.

[24] Office for National Statistics (2025) *Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2024* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates (Accessed Feb 2026).

6. Cost-benefit analysis

The initial draft assessment has identified a number of impacts of the draft guidance update including the reduced potential for data protection harms. The guidance update is expected to increase regulatory certainty for developers and adopters of ADM technologies. Although there will be costs to organisations from reading, understanding, and implementing the guidance, this is expected to be outweighed by the wider societal benefits of reduced data protection harms and a reduced need for external legal advice amongst those seeking to adopt ADM.

The guidance update advances the ICO's primary duties by clarifying safeguards that protect individuals affected by solely automated significant decisions, and supports secondary duties by enabling responsible innovation and avoiding unnecessary burdens on compliant organisations. The IA will continue to test this balance through consultation and monitoring.

In this section we look at the likely costs and benefits of the draft guidance update on ADM. We assess the potential impacts of the guidance update on affected groups and illustrate the potential impacts on wider society.

Our consideration of these impacts is a means of ensuring that we are securing an appropriate level of protection for personal data, having regard to the interests of different parties, and promoting public trust and confidence in the processing of personal data in line with our principal objective under Section 120A DPA 2018. Our wide consideration of impacts also ensures that we are meeting our broader duties under Section 120B DPA 2018. We will continue to test this balance through consultation on the IA.

6.1. Identifying impacts

In identifying the potential impacts of the draft guidance update it is important to distinguish between:

- Additional impacts that can be attributed to the guidance update – these are affected by how the ICO chooses to develop the guidance update.

- Impacts that are not attributable to the guidance update. These are impacts that arise from the legislative requirements that controllers are expected to comply with.

For the purposes of the impact assessment we are interested in impacts that are attributable to the draft guidance update, rather than those that would have occurred in the absence of regulatory intervention – a concept known as additionality.[25]

Impacts can also be direct or indirect:

- Direct impacts: these are 'first round' impacts that are generally immediate and unavoidable, with relatively few steps in the theory of change between the introduction of the measure and the impact taking place.
- Indirect impacts: these are 'second round' impacts that are often the result of changes in behaviour or reallocation of resources following the immediate impact of the introduction of the measure. These tend to occur at the latter stages of the theory of change.

While it is not always feasible to categorise impacts distinctly, we have identified those that are attributable to guidance update as far as possible. Our impact assessment draws on a mixture of quantitative and qualitative evidence where available, to substantiate and measure impacts. However, our analysis is limited by the lack of robust and specific evidence available.

6.2. Counterfactual

The counterfactual is a term used to describe the baseline or current level of activity. Measuring this baseline allows us to measure the additional of introducing the updated guidance.

Under the counterfactual, organisations must comply with legislative requirements without updated guidance. They experience continued uncertainty around key ADM concepts (definition of a 'decision', meaningful human involvement, legal/significant effect). In this scenario, legal advisory costs remain higher; inconsistent practice persists; and

[25] The Government's Data (Use and Access) Bill Impact Assessment estimates the legislation will generate around £4.7 million per year in savings for businesses from reduced legal advice relating to AI deployment. These savings arise from the legislative reforms themselves, not from ICO guidance.

individuals face weaker transparency and more variable exercise of safeguards

6.2.1. Monetising impact

Providing a quantification of the impacts of the proposed draft guidance update is challenging, given its wide-ranging scope and the limited evidence base. Our analysis therefore focuses primarily on non-monetised impacts. However, where possible, we have provided high-level quantitative analysis to indicate scale.

6.2.2. Uncertainty, risk and optimism bias

As set out in HM Treasury's Green Book, it is important to consider levels of uncertainty surrounding the assumptions used to estimate the potential impacts of the draft guidance update. Although optimism bias is typically considered in capital projects, there can also be a tendency to overestimate aspects within non-capital projects. This might include assumptions around the level of engagement with the ICO's guidance update. To account for this, we have conducted sensitivity analysis of key assumptions where impacts have been monetised.

6.3. Costs and benefits

The costs and benefits of the draft guidance update have been identified, as far as is possible and proportionate. These are summarised in Table 3, which provides an overview of what we consider to be the primary costs and benefits for each of the affected groups. This list should not be viewed as exhaustive or hierarchical.

Figure 3: Draft guidance update on automated decision making – table of impacts

Affected group	Scale of affected group	Benefits	Costs
Organisations	**Developers and suppliers of ADM** ~6,000 UK AI companies; ~1,700 with "Autonomous & Agent Systems" capabilities[26] (proxy for ADM tech)	• Improved clarity on data protection (DP) expectations on profiling/solely automated decisions. • Increased confidence in product compliance. • Reduced legal and compliance uncertainty for product design and go-to-market. • Potential long term reduction in compliance costs as common practices converge on guidance.	• Familiarisation costs of reading and understanding the updated guidance (£111 per organisation[27]) • Implementation costs (e.g. updating internal processes, contracts, documentation). • Operational costs from potential increased time responding to data subject rights requests.

[26] DSIT (2024) *Artificial Intelligence Sector Study 2024*. Available at: https://www.gov.uk/government/publications/artificial-intelligence-sector-study (Accessed Feb 2026).
[27] See Annex A – based on a single read assumption per organisation. We will refine this estimate using evidence gathered during consultation and will report an appropriate central estimate and range in the final IA.

Adopters of ADM *Private Sector* 1% of UK businesses handling digitised data use ADM[28]. This suggests a cohort of 44,000 UK businesses that use ADM.	• Greater certainty on legal requirement for ADM and profiling. In 2024, around half of ADM adopters note lack of regulatory clarity as a challenge[29]. • Reduced need for external legal advice on ADM adoption. This is estimated to lead to a 20% reduction in legal costs equating to a £4.7m/yr savings across businesses[30]. • Lower risks of non compliance and associated penalties. • Increased confidence in compliant adoption,	• Familiarisation costs of reading and understanding the updated guidance (£111 per organisation[31]) • One-off implementation costs (e.g. DPIAs, updating policies, contracts, systems). • Ongoing compliance costs: due diligence of ADM suppliers, fairness testing, record keeping,

[28] DSIT (2024) *UK Business Data Survey 2024.* Available at: https://www.gov.uk/government/collections/business-data-survey (Accessed Feb 2026).
[29] ICO (2025) *Data Controller Study.* Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/data-controller-study/data-controller-study-2025/ (Accessed February 2026).
[30] DSIT (2024) *Data (Use and Access) Bill Impact Assessment.* Available at: https://assets.publishing.service.gov.uk/media/673cc6b97524e1b17c494efe/Data_use_and_access_bill_impact_assessment.pdf (Accessed February 2026).
[31] See Annex A – based on a single read assumption per organisation. We will refine this estimate using evidence gathered during consultation and will report an appropriate central estimate and range in the final IA.

		supporting uptake and responsible innovation.	handling requests from data subjects.
	Public sector adopters >50 ADM systems currently in use across the UK public sector.	• Improved clarity on legal obligations. • More consistent, transparent ADM deployment. • Potential increase in responsible innovation, with potential for efficiency savings (e.g. DWP fraud detection savings)	• Familiarisation costs of reading and understanding the updated guidance (£111 per organisation[32]) • Potential cost of updating processes, documentation and transparency mechanisms. • Possible increased scrutiny or challenge from data subjects.
Individuals	Millions affected by ADM in public and private services; 91% of UK public have	• Reduced risk of DP breaches and harms (e.g. discrimination, bias)	• Potential time costs (engaging with new

[32] See Annex A – based on a single read assumption per organisation. We will refine this estimate using evidence gathered during consultation and will report an appropriate central estimate and range in the final IA.

	concern about computer-only decisions[33].	• Increased trust and confidence in ADM • Clearer routes to contest decisions and seek human intervention • Empowerment to exercise rights	rights, understanding guidance update)
ICO		• Fewer enquiries and complaints due to improved clarity • More resources to focus on proactive compliance • Potential reduction in supervision costs	• Resource costs of developing, maintaining, and updating guidance • Ongoing monitoring and evaluation requirements guidance.
Wider society	69 million individuals[34]	• Improved public trust in ADM and data-driven services • Reduced risk of data protection harms (e.g.	

[33] DSIT (2024) *Public attitudes to data and AI: Tracker survey (Wave 4*). Available at: https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey-wave-4/public-attitudes-to-data-and-ai-tracker-survey-wave-4-report (Accessed Feb 2026).
[34] Office for National Statistics (2025) *Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2024* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates (Accessed Feb 2026).

	discrimination, loss of control of personal data etc.)

Source: ICO analysis.

6.3.1. Costs

The additional costs attributable to publishing the ICO's ADM guidance update are expected to be modest and concentrated among organisations that use or supply ADM systems (especially large firms and public bodies). These costs primarily take the form of familiarisation and implementation/transition activities driven by clarification of expectations (e.g., "meaningful human involvement", information to individuals, documentation and audit trails). Ongoing costs are expected to be limited, with some offset by reduced uncertainty and fewer external advisory needs.

Administrative costs

Under the UK Standard Cost Model (SCM),[35] administrative costs are the costs to businesses of meeting information obligations arising from regulation (e.g., collecting, processing, storing and providing information to a public authority or to third parties when required by law). This category is narrow and excludes policy/compliance costs such as process redesign, training, system changes or capital outlays.

The ICO's guidance update does not itself create new legal information obligations; it clarifies how to comply with existing law. Consequently, we do not identify any additional administrative costs (as defined in the SCM) caused by the guidance update.

This treatment aligns with recent cross-government practice to distinguish administrative burdens (information obligations) from wider compliance costs, and with HM Treasury's current methodology for reporting administrative burdens at the aggregate level.[36]

6.3.2. Benefits

Publishing clear, practical ADM guidance is expected to deliver regulatory certainty, and a reduced need for external advisory costs on compliance. These benefits accrue most to organisations actively using ADM (large firms and public bodies), with wider social benefits via improved transparency and trust.

---

[35] Cabinet Office (2005) *Measuring Administrative Costs: UK Standard Cost Model.* Available at: https://regulatoryreform.com/wp-content/uploads/2015/02/UK-Standard-Cost-Model-handbook.pdf (Accessed Feb 2026).
[36] HMT (2025) *Technical Annex – 25% Target Methodology (Annex A).* Available at: https://regulation.org.uk/library/2025-HMT-admin_costs.pdf (Accessed Feb 2026).

6.4. Overall assessment

This initial draft assessment has identified a number of impacts of the draft guidance update including the reduced potential for data protection harms. The guidance update is expected to increase regulatory certainty for developers and adopters of ADM technologies. Although there will be costs to organisations from reading, understanding, and implementing the guidance, this is expected to be outweighed by the wider societal benefits of reduced data protection harms and a reduced need for external legal advice amongst those seeking to adopt ADM.

At this draft stage of guidance update, we expect the guidance to have a net positive impact on balance. However, we will seek to gather additional information on the potential costs and benefits of the guidance update throughout consultation and development of our final guidance and impact assessment. Table 2 presents a summary of the main impacts we expect to see from the guidance update and associated level of attribution.

Table 2 – Attribution of impacts to draft guidance update

Impact of guidance update		Attribution	Comment
Costs	Familiarisation costs of reading and understanding guidance	High	Fully attributable to the guidance. These are direct costs associated with organisations reading, interpreting, and disseminating the updated guidance.
	Ongoing compliance costs – due diligence, fairness testing, record keeping, handling requests from data subjects.	Low	These are legislative obligations under UK GDPR. The guidance does not introduce new rights or safeguards. Costs may arise where the guidance improves transparency about what good practice looks like, prompting organisations to amend their internal processes/procedures.
	Implementation costs (e.g. updating internal processes, DPIAs contracts, documentation)	Low	Most implementation costs derive from the legislation, not the guidance. However, costs may arise where guidance clarifies operational expectations.
Benefits	Improved regulatory certainty for developers and adopters of ADM technologies	High	Fully attributable to the guidance. The guidance clarifies key ADM concepts.

Improved public trust in ADM and reduction in data protection harms arising from ADM deployment	Low	The primary driver of trust is how organisations implement the law, not the guidance itself. However, improved clarity can indirectly support better practice, more consistent safeguards, and clearer information to individuals. 91% of public express concern about computer-only decisions, suggesting clearer guidance can support confidence however, this is not the main determinant of trust.
Reduced need for external legal advice on compliant ADM adoption	Medium	The clarification of ADM concepts is estimated reduces advisory costs. The guidance further amplifies this by providing operational detail.

Source: ICO analysis

7. Monitoring and review

Once the final guidance is published, monitoring and review activities will be carried out in line with the ICO's Ex-Post Impact Framework (EPIF). This will ensure proportionate, consistent measurement of outcomes and impacts. Monitoring for this intervention will also feed directly into the wider ex-post impact measurement of the ICO's AI and Biometrics Strategy.

A proportionate approach to monitoring and review is essential to understanding whether the guidance update achieves its intended outcomes.

Once consultation feedback has been incorporated and the final guidance is published, the ICO will apply the principles set out in its Ex-Post Impact Framework (EPIF) to design and implement appropriate monitoring activities.

This intervention also forms part of the ICO's AI and Biometrics Strategy, which sets out wider objectives for promoting responsible and compliant adoption of AI-driven technologies. As such, monitoring of this guidance will directly feed into the ex-post impact measurement of the Strategy, helping the ICO understand how regulatory guidance contributes to the strategy's broader aims.

A.1 Familiarisation costs

This annex explains how familiarisation costs for the guidance were estimated.

Familiarisation costs per organisation

We have estimated the total time for reading the guidance at **3 hours and 10 minutes**. This is based on a word count of around 14,184 words and a Flesich reading ease score of 45.

Table 3: Familiarisation costs

Document	Word Count	Fleisch reading ease score	Assumed words per minute	Estimated reading time (hr:mn)
Guidance	14,184	45	75	3:10

Source: ICO Economic Analysis

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings.

Making the conservative assumption that the relevant occupational groups is 'Managers, Directors, and Senior Officials', the 2024 median hourly earnings for this group is £29. This hourly cost is uprated for non-wage costs using the latest figures from the Regulatory Policy Committee guidance, resulting in an uplift of 22% and an hourly cost of £35. We therefore assume the cost of reading this guidance once to be approximately £111.

It is important to highlight that £111 is a conservative lower bound estimate of familiarisation cost per organisation based on a single read assumption. Stakeholder feedback and experience from previous consultations indicate this likely underestimates real world familiarisation cost for large organisations, where multiple teams will need to read and understand the guidance. We will therefore refine this estimate using evidence gathered during consultation and will report an appropriate central estimate and range in the final IA.