Title: Consultation Submission – Automated Decision-Making and Profiling Guidance (UK GDPR Article 22)

Respondent: Daramola Joseph Omoyele, Data Governance Practitioner, Economist and Data Analyst

Primary focus: Operational application of Article 22 UK GDPR within SME use of third-party business software.

Date: 17 February 2026

1. Executive Summary

This submission sets out how small and medium-sized enterprises (SMEs) encounter automated decision-making and profiling in everyday SaaS tools and where the current guidance is difficult to operationalise without legal or technical support.

SMEs routinely use payroll/HR platforms, payment services with fraud controls, applicant tracking systems, and accounting tools that can generate outcomes consistent with Article 22. In many cases, the automated element sits inside vendor products and is treated by SMEs as a standard "system output," not a regulated decision. The result is a practical compliance gap: many SMEs want to comply, but they need clearer indicators of scope, workable human-review steps, and stronger expectations on vendors to support transparency and rights in real deployments. These issues also engage the wider UK GDPR principles of fairness, transparency, and accuracy, which apply regardless of whether Article 22 is formally triggered.

2. SME Operational Context

2.1 How SMEs Actually Use Automation

SMEs across the UK rely on cloud-based software to manage routine business functions. These systems are selected for ease of use and cost-effectiveness, not for their compliance features. Typical examples include:

Payroll and HR systems that automatically flag staff attendance issues, calculate eligibility for benefits, generate warnings about performance metrics, and recommend disciplinary actions based on pre-set thresholds.

Fraud detection and payment processing tools that automatically block transactions, suspend accounts, or decline card payments based on algorithmic risk scores without human review.

Accounting and invoicing software that automatically applies credit terms, sets payment deadlines, or restricts access to services based on payment history and predictive scoring.

Recruitment and applicant tracking systems that automatically screen CVs, rank candidates, and filter applications based on keyword matching and scoring algorithms.

2.2 The Perception Gap

From an SME point of view, the outputs of these systems look like ordinary operational messages: warnings, flags, rankings, or suggested actions. A business owner who sees "Employee X flagged for attendance review" will usually treat this as an HR alert, not as a potentially significant, solely automated decision about an individual.

The automation is often opaque in practice. Decision rules, thresholds, and scoring logic sit inside vendor products and rarely appear in documentation in a form an SME can use to explain outcomes to staff, applicants, or customers. In many deployments, SMEs have limited configuration control, limited audit visibility, and limited ability to evidence how a decision was reached beyond "the system flagged it."

Most SMEs do not have in-house HR specialists, a legal team, or a Data Protection Officer. "Compliance" is often handled by an owner, office manager, or finance lead whose main exposure to UK GDPR is privacy notices and subject access requests. Concepts such as Article 22, DPIAs, and "meaningful information about the logic involved" do not match how their systems are bought, configured, or used in practice.

3. Where the Guidance Is Hard to Apply in SMEs

3.1 Definitions: Profiling and "Solely Automated"

The guidance defines profiling as automated processing used to evaluate personal aspects (UK GDPR Article 4(4)). SMEs often struggle to translate that definition into a practical test they can apply to common software features. For example, a payroll system that calculates overtime pay or a CRM that segments customers by purchase history may involve evaluation of personal aspects, but SMEs typically lack a clear operational threshold for when this becomes "profiling" for guidance purposes.

The guidance explains "solely automated" as a decision made without meaningful human influence (page 10) and clarifies that human involvement must be active rather than a token step. In SME settings, the boundary is often behavioural and procedural rather than technical. If a manager receives an automated attendance warning and issues it without checking the underlying records, exploring context, or exercising discretion, the "human step" may not be meaningful. SMEs often believe the presence of a person in the workflow is sufficient, which creates avoidable uncertainty and inconsistent practice.

3.2 Legal or Similarly Significant Effect

The guidance states that decisions with a "legal or similarly significant effect" include those that affect a person's circumstances, behaviour or choices (page 12). Examples given include automatic refusal of credit and e-recruiting without human intervention. However, the guidance also notes that decisions that might have little impact generally could have a significant effect on more vulnerable individuals, such as children.

For SMEs, this creates interpretive challenges. A decision to decline a £50 credit purchase might have little impact on one customer but a significant impact on another. A blocked payment might be inconvenient for one person but disastrous for someone in financial hardship. SMEs lack the expertise to make these contextual assessments and typically have no way to know the personal circumstances of affected individuals.

3.3 DPIA Requirements

The guidance makes clear that processing subject to Article 22 is high risk and therefore requires a Data Protection Impact Assessment (page 19). It states that DPIAs are "mandatory for processing that is likely to result in a high risk to individuals."

In practice, many SMEs either have never heard of DPIAs or are unsure how to complete one in a proportionate way. Even those that have often do not understand how to perform one, lack templates or tools, and find it difficult to identify which processing activities qualify as "high risk." The guidance assumes familiarity with risk assessment approaches that many small businesses have limited experience applying in day-to-day operations.

Even where Article 22 does not apply, controllers must still comply with the core UK GDPR principles of lawfulness, fairness, transparency, accuracy, and accountability. Automated tools used in everyday business operations still require oversight to ensure these principles are met. The guidance would benefit from SME-tested examples and templates that show proportionate ways to complete DPIAs where Article 22-style impacts are present.

3.4 Meaningful Information About the Logic

Articles 13 and 14 of the UK GDPR require controllers to provide "meaningful information about the logic involved" in automated decision-making (page 20). The guidance explains this does not require over-complex explanations of algorithms but should describe the type of information collected in creating profiles, why this information is relevant, and what the likely impact will be.

SMEs using third-party software often do not have access to this information. Vendors do not consistently disclose the specific algorithms, scoring models, or decision trees embedded in their products. When an SME customer asks their payroll provider how the system calculates a particular output, they typically receive generic answers or are directed to user manuals that describe features, not decision logic.

As controllers, SMEs are legally responsible for providing this information to data subjects. But they often struggle to provide information they do not possess. This creates a high-friction compliance position: SMEs remain responsible as controllers, but they often depend on vendors for the information needed to explain outcomes and support rights in practice.

SMEs should ensure their processor contracts require vendors to provide the information necessary to meet transparency obligations and support data subject rights. However, many SMEs lack bargaining power or expertise to negotiate these terms and therefore rely on vendor standard contracts.

3.5 Rights to Human Review and Appeal

The guidance states that individuals affected by solely automated decisions must have a right to obtain human intervention, express their point of view, and contest the decision (page 22). It recommends establishing a review process with someone who is suitably qualified and authorised to change the decision.

For a 15-person company, there may be no one suitably qualified to review an algorithmic decision about credit scoring, fraud detection, or HR risk assessment. The business owner may be the only person with authority to override a decision, but they typically lack the technical expertise to understand how the automated system reached its conclusion or whether the decision is justified.

4. Practical Examples from SME Operations

4.1 Example: Automated Payroll Flagging

A small retail business with 25 employees uses a cloud-based payroll and HR system. The system automatically monitors employee clock-in times and generates alerts when an employee is late on three occasions within a rolling four-week period. These alerts are sent directly to the store manager with a recommendation to issue a verbal warning.

The store manager, who has no HR training, receives the alert and issues the warning as instructed by the system. The employee is then placed on a performance improvement plan, also generated automatically by the software. Neither the manager nor the business owner understands that this process may constitute solely automated decision-making under Article 22. They believe they are simply using the system as designed.

From a regulatory perspective, this scenario may fall within Article 22(1), depending on how the process is configured in practice. The system generates the warning and recommended action automatically based on predefined rules, and the manager may rely on that output without independent review. If the manager issues the warning without reviewing attendance records, checking for data quality issues (e.g., clocking errors), considering mitigating factors, or exercising discretion, the review step may be treated as token rather than meaningful. The effect on the employee is significant: formal warnings, performance plans, and potential dismissal.

The SME finds it difficult to provide meaningful information about the logic because the vendor has not disclosed the specific thresholds, weighting factors, or decision rules. The SME has not conducted a DPIA because they did not recognise this as high-risk processing. The employee has no effective right to human review because no one in the business understands how to interrogate or override the system.

4.2 Example: Automated Transaction Blocking

A small e-commerce business uses a payment processing service that includes built-in fraud detection. A customer attempts to make a £200 purchase, but the transaction is automatically declined by the fraud detection algorithm. The customer receives a generic message stating, "Payment could not be processed." No explanation is provided.

The business owner is unaware the transaction was blocked. The payment processor's dashboard shows the declined transaction but provides no detail about why it was flagged as suspicious. When the customer contacts the business, the owner has no ability to review or override the decision. The customer is told to try a different payment method or contact their bank.

This may be a solely automated decision with a potentially significant effect, depending on how the arrangement between the SME and the payment provider is structured. For the customer, it may mean embarrassment, inconvenience, or inability to complete a necessary purchase. For a customer in financial hardship, being declined for a small transaction could have serious consequences. The SME, as controller, is responsible for ensuring the customer's rights under Article 22 are protected, but the vendor's system provides no mechanism for human intervention or transparency.

4.3 Example: Automated CV Screening

A small consultancy uses an applicant tracking system (ATS) to manage recruitment. The system automatically screens CVs against job descriptions using keyword matching and assigns each applicant a score. Applicants below a certain threshold are automatically rejected without any human review. The business owner believes this is an efficient way to handle high volumes of applications.

In regulatory terms, this may constitute solely automated decision-making that produces a significant effect: applicants may be excluded from employment opportunities based primarily on algorithmic scoring without meaningful human review. The system may inadvertently discriminate against candidates with non-standard career paths, older applicants, or those from certain educational backgrounds. The business has no visibility into how the scoring works and will struggle to explain to rejected applicants why their application was unsuccessful.

This scenario may constitute Article 22(1) processing depending on whether a suitably authorised person reviews applications in a meaningful way before rejection and can change the outcome. In practice, many SMEs treat ATS scoring as an administrative filter rather than a decision requiring human review safeguards, which increases the risk of opaque exclusion and discrimination.

4.4 Example: Good Practice Meaningful Human Review

A small professional services firm uses an ATS to rank applicants but does not auto-reject. The system flags “low match” profiles for review. A hiring manager reviews the CV, checks the ATS

reasons (missing keywords, role history gaps), considers alternative evidence (transferable skills, equivalent roles, non-standard career paths), and records a short justification for the final decision. The manager can override the system score and progress the candidate. This approach keeps efficiency benefits while supporting transparency, accountability, and meaningful human intervention where outcomes affect employment opportunities.

5. Recommendations to the ICO

5.1 Publish an SME-Specific Compliance Checklist

Problem: Many SMEs cannot confidently identify when a software feature produces an outcome that triggers Article 22 safeguards, because the decision point is embedded in vendor workflows and described as a “feature,” not as an automated decision.

Impact: SMEs that want to comply waste time guessing scope, miss high-impact use cases (employment, payments, access to services), and fail to put human-review mechanisms in place early enough.

Ask: Publish a one-page "SME Automated Decision-Making Checklist" with practical yes/no questions. For example:

Does your software automatically make decisions about people without you reviewing the information first?

Does the decision affect whether someone gets a job, a service, credit, or disciplinary action?

Can you explain how the software reached its decision?

Can you easily override the decision if you think it is wrong?

If an SME answers yes to the first two questions and no to the last two, they are likely performing Article 22 processing and need to take action. This simple tool would dramatically improve recognition and compliance.

5.2 Clarify Vendor Responsibilities

Problem: SME controllers rely on software vendors for automated decision-making functionality but receive inadequate information about how these systems work or how to configure them compliantly.

Impact: SMEs may struggle to fulfill their transparency obligations or provide meaningful human review. They are legally responsible as controllers but operationally constrained as users.

In many SME deployments, the vendor acts as a processor for payroll/HR/accounting, but the controller remains accountable for transparency and rights; guidance that sets clear minimum vendor support expectations would materially improve compliance outcomes.

Ask: The guidance should explicitly state that good-practice vendors offering automated decision-making features in business software should:

Provide plain-language summaries of decision logic in user-facing documentation

Offer configuration options to enable human review steps

Support controllers in responding to subject access requests and appeals

Clearly label features that may trigger Article 22 obligations

This would create market pressure for vendors to build compliance-friendly products and reduce the burden on SME controllers.

5.3 Provide Template Human Review Processes

Problem: The guidance expects meaningful human intervention, but SMEs do not know how to design a review process and often lack time and expertise.

Recommendation: Publish short template procedures for human review in common SME scenarios, for example:

payroll and attendance warnings

fraud and payment blocking

recruitment screening

Each template could set out:

what information the reviewer should see

what questions they should ask

when they can override the system

how to record the review and decision

Templates would give SMEs a practical starting point and improve the quality and consistency of human oversight.

5.4 Proportionate Compliance Guidance for Common SME Scenarios

Problem: The guidance correctly emphasises that Article 22 processing often involves high risk, but SMEs can interpret this as meaning a full DPIA is always required in every scenario, even where the processing is limited in scale, reversible, and subject to robust human review. This discourages engagement and pushes SMEs toward informal, undocumented practice.

Recommendation: Provide proportionate compliance routes for common scenarios, making clear that risk depends on impact on individuals (not organisation size), while offering scaled examples of what "good" documentation looks like at different impact levels.

Low: basic lead scoring used only to order marketing activity

Moderate: internal performance flags where a human always reviews before action

High: automated blocking of services, automated rejection of job applicants or automated account closure

Indicate when:

a full DPIA is mandatory

a shorter "DPIA-lite" or risk note is sufficient

a DPIA would not normally be required.

Expected benefit: A tiered model would help SMEs focus limited resources on genuinely high-impact scenarios while still managing lower-risk automation. It would make DPIA expectations more proportionate and increase the likelihood that SMEs use the ICO's tools rather than assuming they are "only for large organisations".

5.5 Improve Awareness of Individual Rights

Recommendation: Publish short, plain-language guidance for employees, job applicants, and consumers explaining when automated decisions may occur and how to request human review, provide additional information, and challenge an outcome. This would increase uptake of safeguards and create practical pressure for controllers and vendors to maintain workable review routes.

6. Conclusion

This submission reflects practitioner observations from working with administrative and operational business data processes rather than from a legal or vendor perspective. SMEs are controllers under the UK GDPR and are responsible for ensuring their automated decision-making processes comply with Article 22. However, the current guidance assumes a level of legal, technical, and organisational capability that most SMEs do not possess. Automated decision-making in SMEs is not happening in dedicated AI projects overseen by data science teams. It is happening silently, inside everyday business software, managed by people who do not recognise it as regulated activity.

Clear, operational guidance tailored to SME realities will improve compliance and better protect individuals. SMEs want to do the right thing, but they need practical tools: checklists, templates,

and vendor accountability frameworks. Without these, the gap between legal expectation and operational reality will persist, leaving both SMEs and data subjects at risk.

I appreciate the opportunity to contribute to this consultation and remain available to discuss these points further.