Elphinstone Research Group

Legal Research

Policy Report and Recommendations

Workplace Monitoring Technologies

UK Legal Research Branch | Publication 2

August 2026

Editor's Note

This second publication from the ERG UK Legal Research Branch brings together legal, workplace and policy research prepared alongside the Government's consultation on monitoring technologies.

Monitoring is not automatically wrong. It can protect people, premises, information and services. Problems arise when a tool is continuous, intrusive, inaccurate or hard to challenge, especially where it affects pay, shifts, discipline or dismissal.

Our conclusion is practical: a statutory workplace monitoring code, updatable guidance and a targeted duty to consult before higher-risk systems are introduced or materially changed.

Jadyn Pitt
Director, Legal Research Branch
Legal Director and Trustee

How the research was organised

Three research streams fed into one report. The leads coordinated the work in their area; the final argument and recommendations were then edited as a single publication.

POD 1	**Law, Privacy and Rights** Lead: Victoria Dimitrova	Mapped the legal framework, privacy rights and available routes of challenge.
POD 2	**Evidence and Workplace Reality** Lead: Eman Siddiqui	Examined how monitoring is used at work and what can go wrong in practice.
POD 3	**Policy and Recommendations** Lead: Dayaan Khokhar	Compared the reform options and developed the final recommendations.

SCOPE AND METHOD

This is a focused desk review, not a systematic literature review or a representative worker survey. It draws on the team's research map, scoping notes and policy-option analyses, checked against primary legal and regulatory sources. The report accompanies, but does not reproduce, ERG's question-by-question online response. The consultation applies to England, Scotland and Wales; employment and consultation arrangements are not identical in Northern Ireland. Law and guidance were checked to 29 August 2026.

Contents

ERG's position at a glance

The evidence points to a practical middle course: keep useful monitoring possible, but require earlier scrutiny where the intrusion or consequence is serious.

01 **WHAT THE EVIDENCE SHOWS**

Monitoring can protect safety, security and services. Risk rises where it is continuous, hidden, biometric, used in the home or tied to decisions about recruitment, work, pay, discipline or dismissal.

02 **WHERE THE PRESENT FRAMEWORK FALLS SHORT**

The law already provides meaningful protection, but it is spread across data protection, equality, employment and consultation rules. Too often it becomes useful only after a system is operating or a decision has been made.

03 **WHAT ERG RECOMMENDS**

No single option is enough. ERG supports a statutory code, practical guidance and a targeted duty to consult before higher-risk monitoring is procured, introduced or materially changed.

A clearer framework for responsible monitoring

ERG's recommendations to the UK Government consultation

Workplace monitoring technologies can support safety, security, compliance and effective management. They can also reveal where systems or workloads are failing. The same tools, however, can collect intimate data, reduce work to crude metrics and influence decisions that affect a person's livelihood. Risk is greatest where monitoring is continuous, biometric, hidden, used in the home or connected to recruitment, pay, shifts, discipline or dismissal. [1]

The law already provides meaningful protection. The UK GDPR and Data Protection Act 2018 require lawful, fair, transparent, necessary and proportionate processing. Equality law, employment rights, consultation arrangements and Article 8 privacy principles may also apply. These protections sit across different regimes, are not always understood together and often become useful only after harm has occurred. [2][3]

ERG's view is that no single option is enough. A statutory code should translate existing duties and the Government's eight principles into one workplace standard. Practical guidance should show how that standard applies to particular technologies and sectors. Employers should also consult workers or their representatives before introducing or materially changing higher-risk monitoring. That discussion must begin while alternatives remain open and end with a reasoned response, not the announcement of a finished decision.

Taken together, these measures would protect workers while supporting responsible adoption. They give employers clearer expectations, give workers an informed voice and direct attention to the uses capable of causing the greatest harm. They do not create a general worker veto or treat every routine security tool as higher risk.

The Government is still deciding how monitoring should be regulated

The Government opened its workplace monitoring technologies consultation on 8 July 2026. It asks how monitoring can be used fairly, transparently and responsibly, with particular attention to clarity, worker voice and industrial relations. No final policy has been chosen. The real question is which combination of law, guidance and workplace engagement can improve practice without blocking useful technology. [1]

The timing is significant. The consultation reports that monitoring has expanded across office, remote, industrial and platform work. It cites a 2025 survey in which one in three UK managers said they actively monitored workers' digital activity, compared with one in five in an ICO survey from 2023. These figures do not show that every use is harmful. They do show that monitoring is no longer confined to obvious cameras or clocking systems. It is increasingly built into software, devices and ordinary management processes. [2]

ERG's analysis starts with a practical question: what should an employer be required to do before a monitoring tool begins shaping daily work or consequential decisions? The answer must protect rights, but it also has to be usable. A framework that is too vague will change little. One that treats every software update as a major legal event will lose support and may direct attention away from the most serious cases.

What counts as workplace monitoring technology

Workplace monitoring technology is broader than surveillance in the ordinary sense. It includes systems that observe, collect, analyse or infer information about workers, their activities or their environment. Some tools are visible and familiar, such as CCTV, entry cards, vehicle tracking and clocking systems. Others sit inside software and produce scores, alerts or recommendations from data that workers may not realise is being combined. [2][3]

The relevant question is not only what a device records. It is also what the employer does with the information. A camera used to investigate theft raises a different set of concerns from the same camera being used to time customer interactions. Location data collected to protect a lone worker is different from continuous off-duty tracking. An access system that checks a card is different from facial or fingerprint recognition because biometric identifiers are difficult to replace if compromised and may amount to special category data when used for unique identification. [4][5]

Monitoring can also become part of algorithmic management. Software may allocate shifts, rank workers, identify supposed underperformance or recommend further investigation. Even where a final decision is formally made by a person, the system can frame what the decision maker sees and how a worker is judged. The report therefore uses WMT as a functional term. If technology observes work or converts worker data into a management judgment, it belongs within the discussion.

Employers can have legitimate reasons to monitor

A credible framework should begin by recognising why employers monitor. CCTV may protect staff and customers. Access controls can secure sensitive sites. Vehicle tracking can support routing and lone worker safety. Recorded calls may help meet regulatory requirements or resolve disputes. Employers may also need reliable information about attendance, quality and the operation of a service.

These purposes are not automatically displaced because a system also processes personal data. The central tests are whether the purpose is clear and legitimate, whether the monitoring is necessary to achieve it, and whether the intrusion is proportionate. Employers should be able to explain why a less intrusive method would not reasonably meet the same need. They should also be able to show that the information collected is relevant and not simply useful to have. [3]

The tone of reform matters. If regulation is framed as hostility to technology, responsible employers may disengage and workers may receive formal notices that change little in practice. A clearer standard can support adoption where a tool has a real purpose and suitable safeguards. It can also make refusal easier where the proposed use is excessive. Responsible adoption means choosing a proportionate system, limiting what it does and being prepared to stop or change it when evidence shows that the safeguards are not working.

The same tool can serve very different purposes

Technology should be assessed by function, context and consequence rather than by its name alone.

AI SCORING
Used to rank performance, allocate work or flag risk. Main concerns are context, bias, accuracy and the weight placed on the output.

BIOMETRICS
Used for access or attendance. Main concerns are necessity, special category data, false matches, security and the absence of a genuine alternative.

CCTV AND VIDEO ANALYTICS
Used for safety and security, but may shift into behaviour or performance monitoring. Analytics can create further inference and accuracy risks.

SCREENS, KEYSTROKES AND COMMUNICATIONS
Used for security, workflow or quality. Continuous capture can expose private material and mistake activity for performance.

GPS AND WEARABLES
Used for routing, safety or attendance. Risks increase when collection continues outside work or is used to intensify targets.

ACCESS CARDS AND LOGS
Often less intrusive than biometrics, but still capable of revealing attendance patterns, movements and associations.

AI scoring can turn a proxy into a verdict

AI scoring systems can combine attendance, output, response time, keyboard activity, communications or customer feedback into a single assessment. The apparent precision of a score is attractive. It can also conceal a weak assumption. Fast replies may be treated as better work. Uninterrupted activity may be treated as commitment. A low number may look objective even where it reflects disability-related breaks, caring responsibilities, flexible hours or work that is valuable but difficult to count.

The danger increases when a score moves directly into recruitment, shifts, pay, promotion, discipline or dismissal. A worker may not know which data mattered, how an error can be corrected or whether the person reviewing the case has enough authority to depart from the system. The ICO's work on automated recruitment has stressed transparency, consistent human involvement and monitoring for fairness and bias. [9][16]

Before relying on a score, an employer needs to know what it is actually measuring. Testing should cover accuracy, false positive and false negative rates, performance across relevant groups and the effect of reasonable adjustments. A human signature at the end is not enough. Review is meaningful only where the reviewer understands the limits of the output, can see the relevant information, has time to hear the worker's explanation and can change the result. [15]

Biometrics demand a higher standard of justification

Biometric systems identify or verify people through physical or behavioural characteristics. In workplaces this may include fingerprints, facial recognition, voice patterns or forms of behavioural recognition. Where biometric data is processed for the purpose of uniquely identifying a person, it is special category data and requires both a lawful basis and a separate Article 9 condition. [5][20]

The central issue is necessity. In February 2024 the ICO ordered Serco Leisure, Serco Jersey and seven associated trusts to stop using facial recognition and fingerprint scanning for attendance. More than 2,000 workers at 38 facilities were affected. The regulator concluded that less intrusive means, such as cards or fobs, could achieve the purpose and that staff had no genuine alternative. [6]

Biometric data creates a particular security problem because it cannot be changed in the same way as a password. False acceptance or rejection can also affect access to work and pay, and performance can vary across demographic groups. Employers should complete the required risk assessment before procurement, test the system on the population in which it will operate, provide a practical alternative and set strict rules for retention, access and deletion. Biometrics should not become a default merely because a supplier describes it as convenient or modern.

Cameras, screens and location data are context dependent

CCTV is often introduced for a clear security or safety reason. That does not give an employer an open-ended right to use the footage for every later purpose. A camera installed to deter theft may gradually become a tool for counting breaks, assessing appearance or timing customer service. This is function creep. It changes the effect on workers and may require a new lawful basis, fresh information and a renewed proportionality assessment. [3]

Screen capture, keystroke logging and communications analytics create a similar problem. They can assist with security or quality assurance, but continuous capture can record private messages, sensitive information or moments that say little about performance. Activity is not the same as productivity. A worker thinking, speaking to a colleague or using assistive technology may appear inactive to a crude metric.

Location monitoring may protect lone workers, verify delivery or support routing. It becomes substantially more intrusive where tracking extends into breaks, travel outside work or a worker's home. The same is true of monitoring on personal devices. Employers should separate work and private time, collect location only at the frequency required, provide a clear off switch where appropriate and avoid retaining a detailed movement history without a specific reason. Covert monitoring should remain exceptional, narrowly targeted and time-limited.

Privacy is about power as well as secrecy

Workplace privacy is sometimes described as a question of whether a worker has something to hide. That is too narrow. Monitoring changes the balance of power because one party can observe, record and interpret the other. A worker may know that monitoring exists and still have little practical ability to refuse it. The effect is stronger where the employer controls pay, hours, access to work or continued employment.

Privacy also has a spatial dimension. Remote work can bring monitoring into the home, where cameras, microphones or device data may capture family members and private surroundings. Notice alone cannot make unlimited home monitoring proportionate. The employer must still identify a legitimate purpose, consider less intrusive means and restrict the scope of collection. [3][14]

The European Court of Human Rights decision in Bărbulescu v Romania is useful because it treats proportionality as a real inquiry. Relevant considerations include prior notice, the nature and extent of monitoring, the reasons for it, whether less intrusive measures were available, the consequences for the worker and the safeguards against abuse. The Grand Chamber found that the domestic authorities had not adequately protected the employee's Article 8 interests. The case does not say that an employer can make intrusive monitoring lawful simply by placing it in a policy.

Persistent measurement can reshape the job itself

Monitoring does not merely observe work. It can alter how work is organised and experienced. When every pause, movement or response is measured, workers may adapt to the metric rather than the real purpose of the job. Targets can become more intense because the system makes faster comparison possible. Discretion may narrow, and workers may avoid reasonable breaks or helpful conversations because these appear as inactivity.

The Government's consultation identifies psychological harms, loss of autonomy, inaccurate performance assessment, reduced wellbeing and inability to challenge as potential consequences. The evidence does not justify claiming that every monitoring system causes these outcomes. It does justify requiring employers to consider them before deployment and during review. [2][18]

A wellbeing assessment should remain practical. Employers should ask what behaviour the tool is likely to reward, whether targets create unsafe pressure, how workers understand the system and whether complaints or absence patterns change after introduction. Worker testimony is relevant evidence, especially where a metric cannot capture the substance of the job. Periodic review should include the option of reducing monitoring or withdrawing a system. A process that only checks whether the technology is still functioning misses the central question, which is whether it remains justified and whether the workplace consequences are acceptable.

Accuracy and equality cannot be separated

A monitoring system may be statistically accurate overall and still produce unfair outcomes. Error rates can differ between groups, the data may underrepresent particular workers, and the chosen metric may disadvantage people because of disability, caring responsibilities or working patterns. The Equality Act analysis is therefore not replaced by a general statement that an algorithm treats everyone in the same way. A neutral rule can create indirect discrimination where it places people sharing a protected characteristic at a particular disadvantage and cannot be objectively justified. [10]

Accuracy also has two levels. The underlying information may be wrong, such as an incorrect location or a false biometric match. The inference may also be wrong, such as treating reduced keyboard activity as low productivity. Both can lead to consequential errors. The ICO advises organisations using AI to define acceptable performance, monitor for bias, investigate significant variation and stop using a system where limits are exceeded. [15][16]

Employers should test before and after deployment. Results should be broken down where lawful and appropriate, and workers should be able to correct relevant data. Reasonable adjustments must be incorporated into the design of assessment and review. Procurement contracts should give the employer enough information to test the system and investigate incidents. A vendor's assurance that a model is accurate is not a substitute for evidence from the actual workplace in which it is used.

Function creep, retention and security require continuing control

A system can be proportionate when introduced and become disproportionate later. New analytics may be added, data may be combined with another source, or information collected for security may begin to influence performance management. The purpose limitation principle requires employers to confront this change rather than treating the original notice as permanent permission. Significant repurposing should trigger fresh assessment and, under ERG's proposed framework, renewed worker consultation. [4]

Retention deserves the same attention. Detailed activity or location records become more intrusive as they accumulate. Employers should define what information is needed, how long it will be kept and who may access it. A generic preference to retain data in case it becomes useful is not enough. Security controls should reflect the sensitivity of the information, particularly where biometric, health or communications data is involved.

The revised Amazon France Logistique decision offers a useful comparative example, although it is not binding UK authority. In December 2025 the French Conseil d'État reduced the original penalty from 32 million euros to 15 million euros and rejected some findings concerning real-time indicators. It nevertheless upheld findings relating to data minimisation, information and security. [17] The case does not make every productivity metric unlawful. It shows why a monitoring programme must be examined claim by claim, purpose by purpose and safeguard by safeguard.

The law is fragmented, not absent

Any case for reform should begin by recognising that workers already have legal protections. Data protection law applies where monitoring involves personal data. Equality law may apply where a system or decision disadvantages protected groups. Contract, workplace policies, collective agreements and the implied duty of trust and confidence may be relevant. Existing information and consultation arrangements can also provide a route for worker voice. Article 8 privacy principles influence the legal assessment, particularly for public authorities and the wider balancing undertaken by courts. [3][10][12][14]

The problem is translation. An employer considering a new system may need to connect lawful basis, transparency, proportionality, accuracy, special category data, impact assessment, equality, consultation and human review. A worker may receive a privacy notice without understanding how a score affects shifts or how to contest an error. Rights are spread across regimes with different coverage, remedies and enforcement bodies.

This fragmentation can harm both sides. Workers may struggle to identify the correct route before a decision takes effect. Employers without specialist legal teams may either avoid useful technology or adopt it without recognising the full risk. A workplace-specific standard should organise existing duties, add a targeted process where the present law is weakest and retain enough flexibility to deal with new technologies.

Data protection law already sets demanding standards

The UK GDPR principles provide the core legal discipline for monitoring. Processing must be lawful, fair and transparent. Information must be collected for specified purposes, limited to what is necessary, kept accurate, retained no longer than needed and secured appropriately. Employers must also be able to demonstrate compliance. [7]

Fairness looks beyond formal permission. Monitoring should not be used in a way that workers would not reasonably expect or that produces unjustified adverse effects. Transparency requires more than naming the software. Workers should understand the purpose, categories of data, frequency, recipients, retention, consequences and relevant rights. Where analytics or automated decisions are involved, the explanation should be meaningful to the people affected.

Data minimisation is particularly important because modern tools can collect far more information than the immediate task requires. A system should not record continuous detail where an event-based or aggregated measure would meet the purpose. Accuracy requires employers to distinguish observed facts from statistical inferences and to correct errors that matter. Accountability ties the principles together. The employer should document the purpose, alternatives considered, tests performed, people consulted, safeguards selected and the decision to continue, change or stop the system.

Lawful basis, special category data and impact assessment

An employer needs a lawful basis under Article 6 for processing personal data. Consent will often be difficult in the employment relationship because the imbalance of power can prevent it from being freely given. Legitimate interests may be available in suitable cases, but ordinary reliance requires a purpose, necessity and balancing assessment. The new recognised legitimate interests basis is not a general shortcut for workplace monitoring. It is confined to specified purposes, and necessity still matters. [22]

Where monitoring uses special category data, such as biometric information for unique identification or certain health-related information, the employer must also identify an Article 9 condition and meet any additional statutory requirements. A commercial preference for a more convenient system does not create that condition. [5]

A Data Protection Impact Assessment is required where processing is likely to result in high risk to people's rights and freedoms. It is not automatically required for every monitoring tool, but biometric identification, facial recognition, systematic observation, innovative technology and consequential profiling may meet the statutory test depending on the circumstances. The assessment must be completed early enough to influence procurement and design. Where appropriate, organisations should seek the views of affected people or their representatives. A completed document is not a defence if the analysis is superficial or ignored when the system changes. [21]

Automated decisions after the Data (Use and Access) Act

The Data (Use and Access) Act 2025 changed the UK rules on significant automated decisions. Section 80 replaced the former Article 22 structure with Articles 22A to 22D. A decision is based solely on automated processing where there is no meaningful human involvement. It is significant where it produces legal effects or has a similarly significant effect on the person. [8][9]

For personal data that is not special category data, the new framework permits a wider range of significant automated decisions, provided the controller uses an appropriate lawful basis and applies the required safeguards. Those safeguards include giving information about the decision, enabling the person to make representations, allowing the decision to be contested and providing human intervention. Stronger restrictions continue where special category data is involved. [8]

This makes the quality of human involvement more important, not less. A reviewer who merely confirms the system's output is not providing meaningful intervention. The reviewer needs relevant information, competence, time and authority. They must consider the worker's case and be able to change the outcome. The ICO consulted on revised automated decision guidance in March 2026, and its wider worker monitoring guidance remains under review following the Act. ERG recommends checking the final guidance again immediately before any code or submission is settled. [3][9]

Equality and human rights add a different form of protection

Data protection fairness and equality law overlap, but they are not the same. The Equality Act 2010 prohibits direct discrimination and can apply where an apparently neutral provision, criterion or practice places people sharing a protected characteristic at a particular disadvantage. Disability-related discrimination and the duty to make reasonable adjustments may also be relevant where monitoring metrics or attendance systems fail to recognise individual circumstances. [10]

An employer should therefore test how a system affects relevant groups and how adjustments will be handled. It should not assume that excluding protected characteristics from the input removes discrimination. Other variables may act as proxies, and the chosen definition of performance may itself create disadvantage. Equality review should continue after deployment because the effect may only become visible in real decisions.

Article 8 of the European Convention protects private life and correspondence. Public authorities are directly bound through the Human Rights Act, while the Convention also shapes the positive obligations and balancing carried out by courts in disputes involving private employment. The final report should not claim that every private employer is directly bound in the same way as a government department. The more useful point is that notice, legitimate purpose, scope, alternatives, consequences and safeguards form a coherent privacy framework. [14]

Employment and consultation rights remain uneven

Monitoring may engage contractual terms, workplace policies, collective agreements and the implied duty of mutual trust and confidence. A disciplinary decision based on inaccurate or undisclosed monitoring may also raise procedural questions. The available claim depends on employment status and the facts. Employees generally have a wider range of tribunal rights than workers with other forms of status, while some people performing work may have limited access to employment remedies even though data protection law still applies. [2]

Existing consultation routes are also partial. A recognised trade union or collective agreement may require engagement. The Information and Consultation of Employees Regulations can create formal arrangements in undertakings with at least 50 employees. Under the current rules, a valid request generally requires support from 2 per cent of the employees in the undertaking, subject to a minimum of 15 and a maximum of 2,500. These rules do not create a universal duty to consult before WMT is introduced. [12][19]

Acas describes meaningful consultation as a genuine two-way discussion in which affected people receive information, can express views and can see that those views were considered before the decision is made. Consultation can improve decisions and working relationships, but its value depends on timing and openness. If software has already been purchased and management will not consider alternatives, the exercise is closer to communication than consultation. [11]

Protection often arrives after harm

The current framework can stop unlawful monitoring and provide remedies. The Serco enforcement action demonstrates that the ICO can intervene where biometric attendance systems are unnecessary and disproportionate. Equality and employment law can address discriminatory or unfair consequences. Workers can use data rights to seek information, correct data or object in appropriate circumstances. [3][6][10]

The weakness is that many protections depend on a worker recognising the problem and finding the correct route after a system is operating. A privacy notice may satisfy part of the information duty without creating any influence over whether the system should be adopted. A grievance may not prevent a score from affecting the next shift. An employment tribunal claim is rarely a realistic way to shape procurement before harm occurs.

ERG therefore rejects two extremes. It would be inaccurate to say that present law offers no protection. It would be equally unrealistic to say that general duties alone produce consistent responsible practice. Reform should make compliance easier to understand, move worker voice earlier and create clear standards for the uses most likely to affect dignity, equality, privacy or livelihood. The objective is prevention and better design, supported by remedies where prevention fails.

The Government's eight principles form a useful common language

ERG supports the eight principles in the consultation, provided they are converted into concrete workplace duties and review questions.

PURPOSE AND RATIONALE
The employer can state the problem, intended benefit and evidence that monitoring is needed.

TRANSPARENCY AND UNDERSTANDING
Workers receive clear information about data, operation, consequences, retention and rights.

WORKER ENGAGEMENT AND VOICE
Affected workers and representatives are involved before significant decisions are fixed.

FAIRNESS AND EQUALITY
The system is tested for unjustified disadvantage and reasonable adjustments are built in.

NECESSITY, PROPORTIONALITY AND PRIVACY
Less intrusive alternatives are considered and collection is limited to the stated purpose.

HUMAN OVERSIGHT AND ACCOUNTABILITY
People with competence and authority review consequential outputs and take responsibility.

DIGNITY AND WELLBEING
The employer considers pressure, autonomy, trust and the quality of working life.

ACCURACY, RELIABILITY AND REVIEW
Data and inferences are tested, errors are corrected and the system is reassessed over time.

Consultation must begin while choices are still open

Workers understand how a job is actually performed. Their operational insight can expose a poor measure, an overlooked adjustment or an intrusion into private time before a supplier and system are fixed.

1	2	3	4
ADVANCE INFORMATION	**CONSULTATION**	**REASONED RESPONSE**	**REVIEW IN USE**
Explain the purpose, data, frequency, logic, recipients, retention, likely consequences and routes to challenge in plain language.	Discuss whether the tool is needed, what alternatives exist, which safeguards are required and how different groups may be affected.	Record the material concerns, what changed as a result and why the employer intends to proceed where concerns remain.	Revisit the system after deployment, significant change, a serious complaint, evidence of bias or a material error.

Consultation does not give workers an automatic veto. Management may retain the final decision, particularly where a lawful system is needed for safety, security or compliance. The point is to create a structured channel before concerns harden into grievances, regulatory complaints or disputes. Emergency measures may justify an accelerated process, but they should be narrow, time-limited and reviewed afterwards.

A functional test should identify higher-risk monitoring

The trigger should focus on effect and intrusiveness, with an open category for comparable future systems.

CONSEQUENTIAL DECISIONS
The output influences recruitment, allocation of work, shifts, pay, promotion, discipline, dismissal or access to a workplace.

CONTINUOUS OR GRANULAR OBSERVATION
The system persistently records screens, keystrokes, audio, communications, movement or productivity.

BIOMETRIC OR SENSITIVE INFERENCE
The system uses unique identification, health information, emotion inference or other special category data.

HOME OR PERSONAL DEVICE INTRUSION
Monitoring reaches domestic space, private devices, breaks or time outside the worker's duties.

SCORING, RANKING OR PROFILING
Data is combined into a rating or risk label that may shape management attention or opportunity.

SIGNIFICANT CHANGE
A new purpose, broader data, stronger consequence, new recipient or material system update changes the original assessment.

A statutory code would bring scattered duties together

ERG supports a statutory code of practice as the foundation of reform. Its main value is not the creation of an entirely new body of law. It is the translation of existing data protection, equality, employment and consultation principles into one workplace process that employers, workers, representatives, regulators and tribunals can understand.

The code should state the minimum steps for purpose definition, transparency, alternatives assessment, lawful basis, equality and accuracy testing, human review, worker engagement, retention, security, procurement, complaints and reassessment. It should use the Government's eight principles and make clear that significant repurposing is a new decision, not a minor operational change.

The consultation proposes that the code could be drafted so that, where a worker succeeds in a relevant tribunal claim, an unreasonable failure to follow the code may lead to an adjustment of compensation of up to 25 per cent under section 207A of the Trade Union and Labour Relations (Consolidation) Act 1992. ERG supports that formal connection, subject to careful drafting of scope and qualifying claims. [2][13] A code does not create a standalone claim simply because it exists, and some workers have narrower tribunal rights. It must therefore sit alongside data protection enforcement, practical challenge routes and the targeted consultation duty proposed below.

Practical guidance should carry the detail that will change fastest

A statutory code should remain durable. It cannot sensibly specify every product, model or data field, and a highly prescriptive code may become outdated or encourage mechanical compliance. Non-statutory guidance is better suited to technology-specific detail and worked examples. It can be revised more quickly as systems and evidence change.

Guidance should explain how the code applies to AI scoring, biometrics, CCTV, location tracking, screenshots, keystroke tools, communications analytics and home monitoring. It should include model worker notices, DPIA prompts, equality and accuracy testing, procurement questions, human review standards, retention examples and simple consultation templates. Employers need examples of what good practice looks like, while workers and representatives need a clear route through the same material.

The audience should include suppliers. Employers remain responsible for their own use of personal data, but they cannot assess a closed product without information about training data, performance, update cycles, security, explainability and audit access. Guidance should describe the contractual information an employer should obtain and when a system should not be purchased. Small employers should receive concise checklists and model documents. Guidance alone would be too weak because it lacks the formal status and preventive consultation process needed for higher-risk uses. Alongside a code and consultation duty, however, it is essential.

A targeted consultation duty addresses the preventive gap

The clearest gap concerns timing. General law can require information, fairness and proportionality, but it does not create a universal right for workers to influence a WMT decision before procurement or deployment. A targeted duty would move engagement to the point where design choices remain open.

The duty should apply to the functional higher-risk triggers set out in this report and to significant changes in existing systems. Employers should consult the recognised union where one exists, or elected representatives and affected workers through a suitable process where it does not. The process should provide enough information and time for informed views, consider alternatives and adjustments, and end with a written employer response.

ERG does not recommend a duty to negotiate agreement for every tool or a general veto. Where consultation does not produce consensus, the employer should retain the ability to proceed after completing the process, addressing legal risks and explaining its decision. Existing Acas services and workplace dispute resolution may assist where relations break down, but mandatory external mediation in every case could create delay and capacity problems. Enforcement should focus on failure to consult, withholding material information or treating the process as a formality. Emergency exceptions should be narrow and should trigger prompt retrospective review.

No single option is enough

Each option answers a different weakness in the present system. Used together, they provide a common standard, practical detail and a route for worker voice before higher-risk decisions are fixed.

OPTION	WHAT IT SOLVES	LIMIT IF USED ALONE
Statutory code	Brings scattered legal duties into one shared workplace standard.	It may remain too abstract without worked examples and practical tools.
Practical guidance	Carries technology-specific detail and can be updated as products change.	On its own, it may be treated as optional and leave poor practice untouched.
Consultation duty	Gives workers a structured voice while procurement and design choices remain open.	Without a substantive standard, consultation can become an exchange of competing assertions.

The code and core guidance can be prepared first, followed by commencement of the targeted duty once model documents and examples are available. That sequence must not become an indefinite delay. The combined approach should then be reviewed against adoption, disputes, worker understanding, equality outcomes, regulatory complaints and the cost to smaller organisations.

Implementation should focus on higher-risk monitoring

The framework should cover employees, workers and other people who perform work where their data is monitored, while recognising that employment remedies differ by status. Duties should fall on the organisation deciding why and how monitoring is used. Suppliers should support compliance through transparency, testing information, security and audit access, but outsourcing should not allow an employer to outsource responsibility.

Proportionality should shape procedure. Routine security updates or low-impact aggregate analytics should not automatically trigger the full consultation process. Higher-risk uses should require fuller information, representative engagement and documented assessment. Small organisations may use shorter templates, but workers should not lose basic protection because an employer has fewer staff. Government guidance should provide practical examples and sector-specific routes rather than a broad exemption.

Enforcement must connect to existing institutions. The ICO should remain central for data protection. Employment tribunals should be able to take the statutory code into account through the mechanism settled by Parliament. Acas should provide guidance and support workplace resolution. Equality issues may engage the Equality and Human Rights Commission and tribunal routes. Workers need a clear internal contact and a prompt way to contest data or a consequential output. Finally, employers should review a system periodically and after material change, serious complaint, evidence of bias, security incident or significant error.

ERG's recommendations

On the evidence reviewed, ERG recommends the following package:

01 A statutory, principles-based workplace monitoring code that translates existing duties and the eight consultation principles into one practical standard.

02 Supplementary guidance for specific technologies, sectors, suppliers and smaller employers, updated as evidence and products change.

03 A targeted statutory duty to consult before higher-risk WMT is procured, introduced or materially changed.

04 A standard worker transparency notice covering purpose, data, frequency, logic, recipients, retention, consequences and rights.

05 Meaningful human review for consequential outputs, carried out by someone with competence, time, information and authority to change the result.

06 Testing for accuracy, bias, equality and reasonable adjustments before deployment and throughout use.

07 A written employer response to consultation and accessible routes to correct data, contest outcomes and raise concerns without retaliation.

08 Periodic and event-based review, including the ability to restrict or withdraw a system where the purpose, evidence or safeguards no longer justify it.

Good governance matters as much as the technology

Workplace monitoring is now part of ordinary management infrastructure. That makes it more important to distinguish legitimate observation from excessive control. The answer is not a blanket ban, and it is not a collection of privacy notices that leave the underlying decision untouched.

Existing law supplies demanding principles, but those principles are scattered and too often become visible only after a worker challenges an outcome or a regulator intervenes. A statutory code can make the standard clearer. Practical guidance can turn it into decisions that employers and workers understand. A targeted consultation duty can move worker voice to the point where it can improve the choice, design and operation of a system.

The final framework should be confident about both sides of the issue. Employers can use technology for safety, security, compliance and effective services. They should also be able to show why the system is needed, what it measures, how it has been tested, who was heard, how errors can be corrected and when the system will be reconsidered. That is the basis for innovation that earns trust rather than demanding it.

Sources and Authorities

Primary legal and regulatory material is used wherever possible. All online sources were last checked on 29 August 2026.

[1] Department for Business and Trade, Make Work Pay: workplace monitoring technologies
Consultation page, published 8 July 2026.

[2] Department for Business and Trade, Consultation on workplace monitoring technologies
Official consultation document, July 2026.

[3] Information Commissioner's Office, Employment practices and data protection: monitoring workers
Regulatory guidance; marked by the ICO as under review following the DUAA.

[4] Information Commissioner's Office, Data protection and monitoring workers
Detailed guidance on lawful and fair monitoring.

[5] Information Commissioner's Office, Biometrics for time, access control and monitoring
Workplace biometric-data guidance.

[6] Information Commissioner's Office, Serco Leisure and associated trusts
Enforcement action concerning biometric attendance systems, February 2024.

[7] Information Commissioner's Office, Guide to the data protection principles
UK GDPR principles and accountability guidance.

Sources and Authorities continued

[8] Data (Use and Access) Act 2025, section 80
Automated decision-making amendments and explanatory notes.

[9] Information Commissioner's Office, What the DUAA means for organisations
Data-protection changes and draft automated-decision guidance, 2026.

[10] Equality Act 2010
Including sections 19, 20 and 39.

[11] Acas, Consulting employees
Guidance on genuine and meaningful consultation.

[12] Information and Consultation of Employees Regulations 2004
Current consolidated regulations, as amended.

[13] Trade Union and Labour Relations (Consolidation) Act 1992
Sections 203, 207 and 207A.

[14] European Court of Human Rights, Bărbulescu v Romania [GC]
Application no. 61496/08, judgment of 5 September 2017.

Sources and Authorities continued

[15] Centre for Data Ethics and Innovation, Review into bias in algorithmic decision making
Independent review, 2020.

[16] Information Commissioner's Office, Guidance on AI and data protection
Fairness, bias, discrimination and statistical accuracy.

[17] Conseil d'État, Amazon France Logistique
Decision no. 492830, 23 December 2025; comparative, non-binding UK material.

[18] CIPD, Employee monitoring
Workplace-practice overview and worker-impact discussion.

[19] Department for Business and Trade, The Information and Consultation Regulations
Official guidance confirming the 2 per cent request threshold, subject to a minimum of 15 and maximum of 2,500.

[20] Information Commissioner's Office, Biometric recognition guidance
Legal and technical guidance on biometric recognition.

[21] Information Commissioner's Office, Data Protection Impact Assessments
When and how organisations should assess high-risk processing.

[22] Information Commissioner's Office, Recognised legitimate interests
Scope and limits of the new lawful basis.

Contributor Credits

FINAL EDITOR AND ASSEMBLY
Jadyn Pitt

LAW AND PRIVACY RESEARCH
Victoria Dimitrova, Pod 1 Lead; Freya Irvine; Jhanvi Thakur; Stafos Galabov

TECHNOLOGY AND WORKPLACE EVIDENCE
Eman Siddiqui, Pod 2 Lead; Annagayle Mosemann; Filipe Ventura

POLICY OPTION ANALYSIS
Dayaan Khokhar, Pod 3 Lead; Viktoriia Volkova; Hridaya Marghade

PUBLICATION DETAILS
Published alongside ERG's response to the UK Government consultation. Law and guidance checked to 29 August 2026. Suggested citation: Elphinstone Research Group, Workplace Monitoring Technologies: Policy Report and Recommendations (2026).

IMPORTANT NOTICE
This is an independent educational contribution to a public consultation. It does not support or oppose any political party or candidate and does not constitute legal advice.