BCLP. Client Intelligent

Insights

WATCHING EMPLOYERS WATCHING THEIR WORKERS

UK DATA PROTECTION AUTHORITY ISSUES UPDATED WORKPLACE MONITORING GUIDANCE

Dec 05, 2023

Over the past few years there has been significant growth in the use of technology for monitoring workers, especially following the onset of the COVID-19 pandemic. Global demand (based on the number of internet searches carried out) for worker monitoring software increased by 108% in April 2020 compared with the same month of the preceding year. With remote and hybrid working set to remain a feature of the way we work – not to mention the role played by the "gig economy" – the uptake of such technologies is likely to continue.

In the UK, the ICO has recognised the need to update its existing guidance on monitoring workers to take into account the significant developments, both in terms of data protection law and technological capabilities, and to address new working practices. In its guidance on monitoring workers ("**Guidance**"), which was published on 3 October, the ICO is aiming to provide up-to-date, practical guidance on monitoring workers in a data protection-compliant way. The Guidance replaces the "Monitoring at work" chapter of the ICO's 2011 employment practices code ("**2011 Code**").

This briefing is centred upon guidance from the UK; however, the themes and recommendations covered are likely to be of wider relevance.

This briefing explores:

1. The content of the Guidance, by reference to data protection and employment law;

2. The background to the Guidance;

3. Further relevant considerations: discrimination and constructive unfair dismissal claims; and

4. Next steps for employers.

CONTENT

The Guidance applies both to systematic monitoring – where an employer monitors all workers or groups of workers as a matter of course, e.g. using software to monitor productivity – and occasional monitoring – where an employer introduces monitoring as a short-term response to a specific need, e.g. installing a camera to detect suspected theft.

The key themes of the Guidance emphasise the need to take a balanced and proportionate approach to employee monitoring, and the importance of transparency and purpose limitation. Employers may benefit from reviewing their current policies and practices in light of the following:

CONSENT

The Guidance makes clear that consent is unlikely to be an appropriate lawful basis or special category data condition in an employment context, due to the imbalance of power between an employer and its workers. The Guidance does acknowledge, however, that there are certain situations where consent may be the only gateway to a specific form of monitoring. For example, the use of biometric data for access control. In order to rely on consent in such scenarios, employers should ensure workers have free choice by offering an alternative to workers who do not wish to give consent. Employers relying on facial recognition or fingerprints for workspace access should note that the Guidance states that employers must have "*an alternative for those who do not do not want to use biometric access controls, such as swipe cards or pin numbers*". Further, the alternative "*should not disadvantage workers.*" This would be the case, for example, if workers who opted to use the alternative access option were required to walk further.

SPECIAL CATEGORY DATA CONDITIONS

The Guidance states that employers must identify a special category data condition even where the planned monitoring may only capture special category data incidentally. Notably, the Guidance gives an express example of a situation where an employer is considering monitoring emails and messages which may identify emails between a worker and a healthcare provider or trade union representative. This is relatively likely to be the case, particularly if the worker is known to have health issues, so it is important for employers to consider this requirement and ensure they comply with it **before** the monitoring is undertaken. This will also be of relevance to any employers considering using biometric data for time and attendance control and monitoring or device sign on.

TRANSPARENCY

The Guidance emphasises that workers must be informed in advance about any monitoring. Workers need to be made aware of the nature, extent and reasons for the monitoring in a way that is accessible and easy to understand. While the Guidance acknowledges that there are a few, very exceptional circumstances where covert monitoring may be justified (in which case the requirement to inform will not apply), it nevertheless suggests that employers should outline in their

organisational policies the types of behaviours which are not acceptable and the circumstances in which covert monitoring might take place, so that in this sense there is general, prior notice.

DATA PROTECTION IMPACT ASSESSMENTS ("DPIAS")

The Guidance states that it is good practice to conduct DPIAs before introducing any monitoring, even where there is no legal requirement under the UK GDPR to do so; and that any decision not to carry out a DPIA in such circumstances should be documented. DPIAs should consider the extent of an employee's privacy expectations, and the impact of monitoring on people generally, other than employees, such as household members if an employee is working from home. Current ICO DPIA guidance confirms that a DPIA will be required if the intended monitoring is covert and/or includes the processing of biometric data to uniquely identify individuals (e.g., electronic fingerprint scanning systems for time and access control or facial recognition sign on for devices) or the use of any monitoring tool which uses analytics to make inferences, predictions, or decisions. The Guidance also points out that the DPIA process should include consulting impacted individuals unless there is a good reason not to, and this remains the case with respect to a worker monitoring scenario. Other than in the case of covert monitoring, employers should therefore consider whether to consult on any new monitoring and, to the extent they decide not to seek the views of the workforce, this decision should be documented. In practice, following this step may require careful thought, as introducing monitoring measures - particularly those with a biometric element - tend to be unpopular with the workforce and may trigger whistle blowing complaints.

PURPOSE LIMITATION

The Guidance states that employers must be clear about the purpose of monitoring. Employers should document why they are monitoring workers and what they intend to do with the information they collect. The Guidance is clear that there are only limited circumstances under which an employer can change its purpose for monitoring. These are where: the new purpose is compatible with its original purpose; the employer obtains consent; or the employer has a clear obligation or function set out in law. The Data Protection and Digital Information Bill is set to clarify the rules on where further processing is to be treated as compatible with the original purpose, including processing that is necessary for preventing and detecting crime, but these changes are not part of UK data protection law at present.

WORKERS' EXPECTATIONS OF PRIVACY

The Guidance makes clear that workers' expectations of privacy need to be considered by employers. For example, it states that workers' expectations of privacy are likely to be higher at home than in the office, and that this needs to be factored into employers' DPIAs, where relevant. The Guidance also notes that employers "*should consider that workers base their expectations of privacy on practice as well as policy*." Employers should therefore be careful of trying to rely on a policy that is not strictly enforced to justify carrying out monitoring. For example, if an employer has

a policy which imposes a ban on personal calls but, in practice, a limited number of personal calls are overlooked, the employer cannot rely on the policy to justify carrying out monitoring of phone usage.

RISK OF BIAS AND DISCRIMINATION

Where monitoring results in processing which causes bias or discrimination, the Guidance makes clear that employers are likely to breach the UK GDPR principle of fairness. The Guidance emphasises that there is a risk of discrimination where biometric recognition technologies are used. For example, there is a risk that facial recognition works less reliability for some demographic groups. Employers wishing to use such systems must assess and mitigate the bias in the system, for example checking that the facial recognition system that they intend to use is suitable for the groups of individuals whose information it will capture. Biometric technologies seem to be a key area of focus for the ICO. On 26 October 2022, the regulator issued a warning to organisations about the potential for systematic bias and discrimination in the use of “immature” emotion analysis technologies, citing, as an example, the monitoring of the physical health of workers via wearable screening tools. Emotion analysis technologies process data such as gaze tracking, sentiment analysis, facial movements, gait analysis, heartbeats facial expression and skin moisture. The warning stated that the ICO will investigate organisations that do not act responsibly when using such technologies. Further, the use of data gathered in this way as the basis for disciplinary or other action against employees also risks employment related claims, for example, unfair dismissal or claims under the Equality Act 2010, with the Guidance serving to highlight the potential unfairness of relying on data which may be inherently biased.

SOLELY AUTOMATED DECISION-MAKING

The Guidance clarifies that monitoring workers will fall within the restrictions on automated decision-making under Article 22 UK GDPR if the decision making is solely automated and has legal or similarly significant effects. For example, paying workers based entirely on automated monitoring of their productivity would fall within Article 22.

BACKGROUND

THE PROCESS SO FAR...

The final Guidance follows a consultation launched in October 2022 on the ICO’s draft guidance (see our briefing, "Watching employers watching their workers: UK data protection authority issues updated workplace monitoring guidance for consultation"). The final Guidance substantially follows the draft guidance, with some additional examples and indications on what employers “must”, “should” and “could” do to comply.

The Guidance forms part of a package of new guidance being issued by the ICO on employment practices and data protection. The ICO also released guidance on workers' health data on 31 August 2023.

WHY SHOULD EMPLOYERS TAKE NOTE?

While it is clear that there are legitimate business interests in conducting workplace monitoring, some of its aspects are more intrusive and open to misuse. One of the top five largest fines (€35.3m) levied for data protection breaches, was issued by the Hamburg supervisory authority (HmbBfDI) against retailer H&M in 2020 in connection with its employee surveillance practices. In addition, there has been a spate of recent enforcement action by European supervisory authorities in relation to workplace monitoring. Last year saw the Italian supervisory authority (the Garante) issue a fine of €84,000 against the Municipality of Bolzano in connection with its use of a system to control and filter employees' internet browsing, as well as a number of supervisory authorities issuing fines in relation to the use of CCTV within the workplace. In most of these cases, the applicable supervisory authority found that the monitoring involved went beyond what was necessary for the purpose, e.g. the use of CCTV for security purposes capturing footage of workspaces and recreational areas, and had been conducted without sufficient notice.

There has been a recent spate of enforcement action in this area, with the French supervisory authority (the CNIL) issuing fines to 10 organisations for failing to respect the principle of data minimisation when deploying geolocation and continuous video surveillance of employees. The CNIL reaffirmed its position that the continuous recording of geolocation data, with no possibility for employees to stop or suspend the system during break times, is, unless there is special justification, an excessive infringement of employees' freedom to come and go and right to privacy. Similarly, the implementation of continuous video surveillance of workstations is, with a few exceptions, disproportionate to the aims pursued.

Even where a supervisory authority decides not to take enforcement action (as was the case with the ICO's reported 2020 investigation of a financial institution's use of Sapience software to track employees' computer use), organisations should be alive to ramifications such as (i) the impact negative press coverage can have, (ii) the impact for employee relations of the workforce perceiving monitoring as intrusive, and (iii) the potential for the issue to impact on litigation (whether by triggering claims or by impacting on the evidential weight placed on any data gathered in a manner which breaches either data protection rights or the wider right to privacy under Article 8 of the Human Rights Act 1998).

WHAT IS THE STATUS OF THE NEW GUIDANCE?

While the Guidance does not impose additional legal obligations, it is still important for employers to consider the views of the ICO, as expressed in the Guidance, from a risk management perspective, as the views of the ICO are likely to inform its enforcement activity.

FURTHER RELEVANT CONSIDERATIONS: DISCRIMINATION AND CONSTRUCTIVE UNFAIR DISMISSAL CLAIMS

Following the principles and best practice guidelines set out in the Guidance plays an important role in mitigating the risk of statutory or contractual employment claims arising from the manner in which monitoring is carried out, or the use of the data obtained. For example, Tribunals may be reluctant to place weight on evidence obtained from monitoring carried out in breach of these principles. There is also frequently an overlap between monitoring of employees and discrimination claims; for example, the monitoring of an employee's absence or work performance may well give rise to disability discrimination issues. In this context, carrying out monitoring in a way which breaches an employee's privacy and data rights can in itself amount to an act of disability discrimination with the resultant risk of significant compensation awards.

Further, as noted above, the Guidance has been prepared in response to the changed working environment post-COVID-19 and, in particular, the increase in home-working. It makes it clear that excessive monitoring may be more of a risk where a worker is working from home. As employers continue to grapple with the impact of hybrid working, it is important that any steps taken to monitor the productivity of home-workers are taken in line with these guidelines to minimise the risk of constructive unfair dismissal and discrimination claims.

NEXT STEPS FOR EMPLOYERS

As always, the introduction of new guidance serves as a useful prompt for employers to review their existing practices to ensure that they remain appropriate, both in light of the ICO's updated expectations and also the changing nature of the workplace and the technology available to support monitoring. This could sensibly include a review, both of the written policies in place and the practical implementation of worker monitoring. Below we have distilled some focus areas:

POLICIES AND NOTICES

Data protection documentation, such as the employee privacy notice, IT systems usage policy and (possibly) signage, should be reviewed to ensure they remain compliant and consistent with good practice. Where routine monitoring is carried out, ensure that policies and notices accurately describe the monitoring taking place and explain the purposes.

THE ROLE OF DPIAS

Carry out a DPIA prior to conducting monitoring, or refresh an existing DPIA. This should be done prior to any new or changed monitoring – it should not just be a box ticking exercise. The ICO may want to see that the DPIA process has had an impact on the final form of the monitoring carried out (where appropriate) and in particular that the adopted method is the least intrusive way of achieving proportionate, justified objectives.

POLICY COMPLIANCE MONITORING

If the purpose of monitoring is to ensure compliance with internal policies (for example, data security or internet usage) the Guidance makes it clear that an employee's expectations of privacy will be based on what happens in practice, not just the written policy. Monitoring to uphold a written policy which is not adhered to in practice is likely to be excessive and therefore unlawful.

CONSULTING WITH WORKERS

Consider whether it is appropriate to consult with employees and/or representative bodies prior to introducing new monitoring. Where consultation does not take place, keep a record of the decision.

INVESTIGATIONS

If the proposed monitoring is for the purposes of specific investigations, rather than business as usual activities, the Guidance is still relevant and should be consulted.

COVERT MONITORING

Explain in your organisational policies the types of behaviours which are not acceptable and the circumstances in which covert monitoring might take place. Covert monitoring remains a measure which should only be taken in exceptional circumstances, for example where it is necessary to prevent or detect criminal activity or gross misconduct.

BIOMETRIC DATA

Pay particularly careful attention to the guidance before introducing any new monitoring measures which result in the processing of biometric data. The Guidance contains specific guidance on this issue and it is important to make sure that there is a joined up approach to the introduction of any new technology.

VENDORS

When making use of third-party tools or services to monitor workers, it is likely for UK GDPR purposes that the employer will be the controller for such processing activity and the third-party will be a processor. As part of the procurement process, you should make sure that the vendor provides you with sufficient information about their tool (e.g. default settings) or service (e.g. any international data transfers involved) to enable you to comply with your data protection responsibilities. A UK GDPR compliant processing contract will also need to be put in place.

RETENTION

Consider retention policies and ensure that data obtained through monitoring is deleted once it is no longer necessary for it to be retained.

If you would like to discuss anything raised in this briefing, please contact Geraldine Scali or your usual BCLP contact.

RELATED CAPABILITIES

- Data Privacy & Security
- ESG Governance, Compliance and Reporting

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483