BCLP. Client Intelligent

Insights

WATCHING EMPLOYERS WATCHING THEIR WORKERS: UK DATA PROTECTION AUTHORITY ISSUES UPDATED WORKPLACE MONITORING GUIDANCE FOR CONSULTATION

Nov 03, 2022

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[1]. 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 In its draft guidance on monitoring at work ("**Draft Guidance**"), the ICO is aiming to provide up-to-date, practical guidance on monitoring workers in a data protection-compliant way. Once finalised, the guidance will replace 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 The content of the Draft Guidance, by reference to data protection and employment law;

2. The background to the Draft Guidance;

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

4. Next steps for employers.

CONTENT

The 54 page long document is split into two parts – the first part explains the data protection obligations employers have in relation to monitoring workers. The second part considers these obligations with reference to specific types of workplace monitoring, e.g. using biometric data and device data.

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The key themes of the Draft Guidance emphasise the need to take a balanced and proportionate approach to employee monitoring, and the importance of transparency and purpose limitation.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 Draft Guidance makes clear that consent is unlikely to be an appropriate lawful basis or special data category condition in an employment context, due to the imbalance of power between an employer and its workers. The Draft 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 must 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 Draft Guidance states that employers must have "*an alternative for those who have not consented which does not involve the processing of their biometric data, such as a separate access*". 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 Draft Guidance states that employers should identify a special category data condition even where the planned monitoring may only capture special category data incidentally. This will be of relevance to any employers considering using biometric data for time and attendance control and monitoring or device sign on. Notably, the Draft 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.

- **Transparency**. The Draft 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 Draft Guidance acknowledges that there are a few, very exceptional circumstances where covert monitoring is 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 Draft 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. 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 Draft 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**. Here, the Draft 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 Draft 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; related to a clear legal provision allowing the processing in the public interest; clearly in the worker's interest; or related to activity that no employer could reasonably ignore. The Draft Guidance states that "*the types of activity an employer could not reasonably ignore might include criminal activity at work, gross misconduct and health and safety breaches which jeopardise workers*." This will be helpful clarification for employers wishing to use CCTV footage collected for security purposes in connection with an investigation into suspected criminal activity or gross misconduct. Taking this example one step further if, while reviewing the footage in connection with the investigation, the employer also discovered lesser infringements being made by another worker, e.g. a worker taking unauthorised breaks, it seems unlikely that the employer could use this information for disciplinary purposes in relation to that employee. However, the confirmation that acts which may amount to gross misconduct are considered sufficiently serious to override the purpose limitation principle will be welcome to employers.

- **Workers' expectations of privacy**. On this point, the Draft Guidance makes clear that workers' expectations of privacy need to be considered by employers. For example, it states that workers' expectations of privacy will be significantly higher at home or outside of the office, and that this needs to be factored into employers' DPIAs, where relevant. The Draft 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 Draft Guidance makes clear that employers will also be infringing the UK GDPR principle of fairness. The Draft Guidance emphasises that there is a particular risk of discrimination where AI and/or biometric recognition technologies are used. For example, multiple published studies have shown 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 they plan to use it on. Facial recognition is clearly a key area of focus for the ICO. On 26 October, 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 makes clear that the ICO will be investigating 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 Draft Guidance serving to highlight the potential unfairness of relying on data which may be inherently biased.

BACKGROUND

The process so far…

The ICO is in the process of producing topic-specific guidance on employment practices and data protection. Drafts of the different topic areas are being released for public consultation in stages. The Draft Guidance is the first, and was released on 12 October 2022. Before drafting the guidance, the ICO issued a call for views, which sought input from relevant stakeholders and the public on what its existing employment practices guidance (the 2011 Code, supplementary guidance and quick guide) should be replaced with. The ICO's summary of responses, sets out the key themes

that emerged from the call for views and how the ICO intends to use them to inform the production of the new guidance.

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.

We expect to see further enforcement action in this area, with the French supervisory authority (the CNIL) announcing that the investigation of telework monitoring is one of the three priority topics it has selected for investigation this year[2]. 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?

The summary of responses states that the ICO has no intention of issuing a new code of practice to replace the existing one "*primarily because having guidance known as a code, that is neither a[n] ICO statutory code of practice nor an Article 40 code of conduct, would risk confusion amongst stakeholders*." It seems clear from this that the guidance, once issued, will be just that – guidance that does not impose additional legal obligations. Of course, it will still be 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.

Are there likely to be significant changes made to the Draft Guidance before it is finalised?

Although the Draft Guidance is open to consultation until January 2023, the ICO has specified the questions in relation to which it invites feedback. While the questions do include an opportunity to provide general comment, they tend to focus on high-level issues, such as the clarity of the Draft Guidance and how easy it is to navigate. This may suggest that the ICO only envisages making limited changes to the Draft Guidance following the consultation period (of course, that may change depending on the actual feedback received).

FURTHER RELEVANT CONSIDERATIONS: DISCRIMINATION AND CONSTRUCTIVE UNFAIR DISMISSAL CLAIMS

Following the principles and best practice guidelines set out in the Draft 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 Draft 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 Draft 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 Draft 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.

Public consultation on the Draft Guidance remains open until 11 January 2023. If you are considering submitting a response and would like to discuss it with us, or if you would like us to include your views in a response, we would be pleased to hear from you.

[1] https://www.zdnet.com/article/employee-surveillance-software-demand-increased-as-workers-transitioned-to-home-working/.

[2] https://www.cnil.fr/en/priority-topics-investigations-2022-commercial-prospecting-cloud-and-telework-monitoring

RELATED PRACTICE AREAS

- Data Privacy & Security
- Employment & Labor

MEET THE TEAM

David von Hagen

London

david.vonhagen@bclplaw.com
+44 (0) 20 3400 3576