ICO PUBLISHES GUIDANCE ON MONITORING WORKERS

On 3 October 2023, the UK's Information Commissioner's Office (ICO) published guidance for employers across both the public and private sectors on how to monitor workers in accordance with data protection law. Against the backdrop of technological developments and a rise in remote working, the guidance aims to provide *"greater regulatory certainty; protect workers' data protection rights; and help employers to build trust with workers, customers and service users"*.[1]

1 *ICO. Employment practices and data protection – Monitoring workers.* Available at: Employment practices and data protection – Monitoring workers | ICO

The range of technologies employers can use to monitor their workers' activities is ever increasing. Keystroke and screen monitoring, body worn cameras and location devices, and time tracking tools are all favoured by employers as a means of managing performance and ultimately boosting productivity and profits.

However, as these increasingly sophisticated monitoring technologies have become more prevalent, so has the concern that their excessive use may infringe the data protection and privacy rights of workers, lead to discriminatory practices, and damage workers' wellbeing.

The latest guidance from the ICO on this issue is therefore welcomed and will help employers to ensure that they are able to manage their workforce effectively using the tools available, whilst protecting the rights of their workers (and therefore minimising the risk of successful complaints and claims).

This briefing will: outline how employers can lawfully monitor workers; consider a worker's right to object to monitoring; identify the pitfalls for employers when using monitoring tools; and set out specific data protection considerations for different types of monitoring.

The ICO's definition of 'monitoring workers'

The ICO defines 'monitoring workers' as *"any form of monitoring of people who carry out work on your behalf"*.[2] The definition includes monitoring on work premises or elsewhere, such as workers' homes, and monitoring during or outside work hours. The definition also encompasses systematic monitoring, *"where an employer monitors all workers or groups of workers as a matter of course", and occasional monitoring, "where an employer introduces monitoring as a short-term response to a specific need"*.[3]

Workers have always had the work they do for their employer monitored, and would expect their hours, productivity and work quality to be scrutinized.

However, it is the use of technological monitoring tools that collect vast amounts of data (including personal data) which is the focus of the ICO's guidance.

The ICO gives some examples of monitoring technologies and their purposes, including:

- keystroke monitoring to track, capture and log keyboard activity;
- camera surveillance including wearable cameras;
- body worn devices that record the location of workers;
- audio recordings;
- productivity tools which log how workers spend their time; and
- technologies for monitoring timekeeping or access control.

How can employers lawfully monitor workers?

The ICO's guidance sets out how employers can comply with data protection law, including the seven key principles of the UK GDPR, when monitoring workers.[4]

It is important that employers comply with data protection law because, in addition to potentially heavy fines for non-compliance, excessive monitoring can have an adverse impact on workers' data protection rights and mental wellbeing, as well as on the trust and confidence between employees and employers, which is integral to any employment relationship and the fundamental breach of which can give rise to constructive dismissal claims, for those employees with more than two years' continuous employment. Research commissioned by the ICO revealed that 70% of those surveyed *"would find monitoring in the workplace intrusive"*.[5]

Indeed, excessive and overbearing monitoring of workers which has a detrimental impact on the worker's wellbeing (which in the extreme could result in mental health problems) would be counter-productive to the aim of boosting productivity and could ultimately result in work-related stress and personal injury claims against the employer.

Employers should take the following steps when monitoring workers:

1. Consider and be clear about the purpose of monitoring workers. Monitoring must be necessary for the purpose identified and be conducted in the least intrusive way possible.
2. Identify a lawful basis for the monitoring. There are six lawful bases including consent, contract, legal obligation, vital interests, public task and legitimate interests.
3. If processing special category data, the employer must identify a special category processing condition. Special category data includes personal information revealing or concerning, for example, racial or ethnic origin, political opinions, religious beliefs, or genetic data.
4. Document the personal information being processed when monitoring workers.
5. Only keep the information which is relevant to the purpose for monitoring. Employers should regularly review the information which they collect and destroy what is not necessary.
6. Inform workers about the nature and extent of and the rationale for monitoring in an accessible and easily understandable way. Such information should be set out in the organisation's privacy information.
7. Conduct a Data Protection Impact Assessment (**DPIA**) before undertaking any processing that is likely to cause high risk to workers' interests, for example, if the employer intends to monitor emails and messages. If the employer decides not to complete a DPIA, it should document its reasons for not doing so. When considering

2 ICO. *Data protection and monitoring workers.* Available at: Data protection and monitoring workers | ICO

3 Ibid

4 The seven key principles are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability. For more information, please see: A guide to the data protection principles | ICO

5 ICO. ICO *publishes guidance to ensure lawful monitoring in the workplace.* Available at: ICO publishes guidance to ensure lawful monitoring in the workplace | ICO

> **"The ICO's guidance sets out specific data protection considerations for different methods of monitoring workers. These considerations are in addition to the steps that employers need to take in order to monitor workers lawfully."**

whether to undertake a DPIA, the employer should consider seeking the views of workers and representatives.

8. Make the personal information collected through monitoring available to a worker if the worker makes a Subject Access Request.
9. If using a third-party provider or application to carry out monitoring, ensure that the system or application is compliant with data protection law. There must also be a contract in place with the provider.
10. If transferring personal information of workers outside the UK and outside the company or organisation, consider the rules for international transfers. If the transfer is restricted, it must be covered by adequacy regulations, appropriate safeguards or an exception.[6]

Can workers object to being monitored?

Workers can object to being monitored by employers where the employer is relying on the lawful bases of public interest task or legitimate interests.

The worker must provide specific reasons for their objection. Employers can refuse to comply with an objection if it is manifestly unfounded or excessive. Employers can also refuse to comply if:

1. the employer can demonstrate compelling legitimate interests for the processing, which override the interests, rights and freedoms of the worker; or
2. the processing is for the establishment, exercise or defence of legal claims.[7]

If the employer is satisfied that it does not need to comply with the request, it must inform the worker, and should document and explain its decision. The employer must also inform the worker of their right to make a complaint to the ICO and/or enforce their rights through a judicial remedy.

Data protection considerations for specific types of monitoring

The ICO's guidance sets out specific data protection considerations for different methods of monitoring workers.[8] These considerations are in addition to the steps that employers need to take in order to monitor workers lawfully.

Using monitoring tools that use solely automated processes

Employers may use personal information from monitoring workers for automated decision-making. Solely automated decision-making is *"a decision made by automated means without any meaningful human involvement"* and may also involve profiling.[9]

Article 22 of the UK (and EU) GDPR states that a data subject has *"the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".*[10]

Pursuant to Article 22(1), an employer can only make decisions based on automated processing where:

- it is necessary for entering into, or performance of, a contract between the worker and the employer;
- it is required or authorised by law that applies to the employer; or
- the worker explicitly consents.

The ICO advises that employers must inform workers if they are processing their information for solely automated decision-making. The employer should offer alternatives to workers who ask for human intervention in decision making, and should not disadvantage such workers. Employers should also conduct regular checks to ensure that the system works as intended.

Automated decision making is also known to result in discriminatory outcomes, which, if left unchecked, could lead to a worker bringing

6 For more information, please see the section titled "What do we need to consider if we transfer personal information of workers outside the UK?" Data protection and monitoring workers | ICO

7 ICO. *Data protection and monitoring workers: Can workers object to being monitored?* Available at: Data protection and monitoring workers | ICO

8 ICO. *Specific data protection considerations for different ways or methods of monitoring workers.* Available at: Specific data protection considerations for different ways or methods of monitoring workers | ICO

9 ICO. *What do we need to do if we use monitoring tools that use solely automated processes?* Available at: What do we need to do if we use monitoring tools that use solely automated processes? | ICO

10 Article 22 GDPR

a claim for discrimination under the Equality Act 2010 (where the compensation available is unlimited).

Applications that track mouse and screen movements to produce a "productivity score" are becoming increasingly common. However, a worker may suffer from a disability that requires them to take frequent breaks away from the screen, adversely affecting their score. If the employer then subjected this worker to a disciplinary or performance management process on the basis of their score, compared to workers who do not suffer from a disability, this would amount to disability discrimination.

There is a lack of transparency in the algorithms underlying automated decision making. How the data fed into the technology is analysed to produce a score may also be a mystery to the employer if it is relying on a third-party application. Therefore, what appears to be a neutral, data-based outcome or decision, may be inherently biased and discriminatory. If an employer is sued for discrimination, they will need to be able to justify to an Employment Tribunal the reasons behind why they reached the decision that they did. Ignorance is not a defence.

Using commercially available tools for monitoring

Employers may use tools or services to assist them in monitoring workers. When using such tools, the employer will often be the controller for the processing activity, because the employer will decide the means and purposes of the processing. The third party will often be the processor. As a controller, the employer will have specific data protection responsibilities, such as ensuring that the provider gives sufficient information about their tool through a written contract or service agreement.

Using biometric data to monitor workers

Employers may use biometric data to monitor access and time recording. The UK GDPR defines 'biometric data' as *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person"*.[11] Biometric data includes fingerprints, voice recognition and iris scanning.[12]

If using biometric data to monitor workers, employers must:[13]

- Conduct a DPIA. Processing biometric data is high risk.
- Identify a condition for processing as biometric data is special category data requiring additional grounds.
- Consider whether additional security measures are required when collecting, using and storing biometric data.
- Inform workers that biometric data is being processed.
- If using biometric data for automated decision-making, assess and mitigate any bias in the system.
- Ensure that manual reviews are available if an automatic process has resulted in a possible access denial and provide workers with the option to request a review.

Monitoring workers remotely

Employers increasingly monitor workers remotely given the rise in remote and home working. Employers should recognise that workers are likely to have a higher expectation of privacy when working at home. Employers may inadvertently capture information regarding workers' family and private lives, which interferes with a worker's right to a private and family life under the Human Rights Act 1998.

Therefore, employers should factor this risk into intended monitoring of remote workers, for example, as part of a DPIA. For example, automatically recording and accessing webcam images to monitor whether a worker is at their desk is likely to interfere with a worker's right to a private and family life, and their data protection rights, because there are less intrusive methods an employer could use to monitor the worker's activity (such as checking the time the worker logs on to the work system).

Monitoring telephone calls

The ICO advises that *"it is not usually proportionate to monitor or record the content of [workers'] calls in all cases"*[14]. However, employers may monitor business calls to evidence business transactions, or for training or quality control purposes. If an employer does monitor calls, it must: (1) inform workers of such monitoring in its privacy information; and (2) inform those making or receiving calls from the organisation.

Monitoring emails and instant messages

Employers must inform workers of the purpose of any monitoring of emails and instant messages, and such monitoring must be necessary and proportionate for the purpose. The employer must also complete a DPIA. The ICO advises that it would be difficult for an employer to justify monitoring emails and instant messages if it could instead meet its purpose by monitoring network data traffic.

Monitoring device activity

Employers may monitor devices to:

- track workers' activity and productivity;
- ensure that policies and procedures are followed; and
- track visits to applications and websites.[15]

11 Article 4(14) GDPR

12 For more information on biometric data, please see our September 2023 briefing titled "ICO publishes draft guidance on biometric data". Available at: 005255-HFW-ICO-publishes-draft-guidance-on-biometric-data.pdf

13 ICO. *Can we use biometric data for time and attendance control and monitoring?* Available at: Can we use biometric data for time and attendance control and monitoring? | ICO

14 ICO. *Specific data protection considerations for different ways or methods of monitoring workers: Can we monitor telephone calls?* Available at: Specific data protection considerations for different ways or methods of monitoring workers | ICO

15 ICO. *Specific data protection considerations for different ways or method of monitoring workers: Can we monitor device activity?* Available at: Specific data protection considerations for different ways or methods of monitoring workers | ICO

> **"Before implementing any monitoring of workers, employers must ensure that such monitoring is lawful. Employers should put in place a compliant monitoring policy if they have not already done so."**

Device activity monitoring may include capturing emails and messages, keystroke monitoring, documents and web browsing. It also includes screen captures and webcam captures.

Employers must be careful when monitoring devices because it is likely to capture excessive amounts of workers' personal information, particularly if workers are allowed to use devices for both work and personal purposes. It is likely that the employer will need to carry out a DPIA.

Video or audio surveillance

Employers may use CCTV to monitor workers. CCTV systems can capture video and audio, and may use facial recognition. Additionally, some CCTV systems may interact with AI to assess workers' productivity. Furthermore, use of CCTV may result in employers inadvertently capturing special category data.

Employers must carry out a DPIA if it is likely that CCTV monitoring will capture special category data, for example, if the CCTV will use facial recognition.

The ICO advises that *"continuous audio and video recording can be highly intrusive and you are unlikely to be able to justify it in most circumstances"*.[16]

An employer must inform workers and anyone caught by the monitoring, including customers, of the operation of CCTV and should have in place an appropriate policy and an appropriate contract with any outsourced provider.

Additional methods of monitoring

The ICO's guidance also considers:

- monitoring work vehicles and using dashcams to monitor workers;
- requests by a customer for an employer to monitor its workers;
- monitoring time and restricting access; and
- monitoring to prevent data loss or detect malicious traffic.

Next Steps

Before implementing any monitoring of workers, employers must ensure that such monitoring is lawful. Employers should put in place a compliant monitoring policy if they have not already done so. Conducting a DPIA will allow employers to assess the risks of any existing or proposed monitoring. The ICO recommends that a DPIA should be carried out regardless of whether the monitoring is likely to cause high risk to workers' interests.

For further information, please contact:

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

MICHELLE CHANCE
Employment Partner, London
T +44 (0)20 7264 8384
E michelle.chance@hfw.com

Ruth Stillabower, Trainee Solicitor, and Lydia Cammiade, Employment Associate assisted in the preparation of this briefing.

16 ICO. *Specific data protection considerations for different ways or methods of monitoring workers: Can we use video or audio surveillance to monitor workers?* Available at: Specific data protection considerations for different ways or methods of monitoring workers | ICO

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our Data Protection and employment capabilities, please visit hfw.com/Data-Protection, or hfw.com/Employment

Americas | Europe | Middle East | Asia Pacific