NEW GUIDANCE FOR UK ORGANISATIONS THAT MONITOR THEIR WORKERS

DECEMBER 2023

Weil

BITESIZE:

- Conduct a Data Protection Impact Assessment before monitoring and identify a legal basis for the monitoring.
- Do not rely on generic consent in agreements as a basis for processing personal data collected as a result worker monitoring. Consent should be specific.
- Inform workers about monitoring in a manner that is accessible and easy to understand.

Following developments in monitoring technology and the rise of home working, the Information Commissioner's Office ("**ICO**") published new guidance on employee/worker monitoring at the beginning of October.

The guidance applies whenever an individual performs work for the organisation including employees, contractors and workers. The guidance does not apply to processing of personal data that is carried out for law enforcement purposes e.g. suspected criminal activity; a separate regime applies to such processing. The term monitoring is widely construed and includes CCTV, audio recording, technologies for monitoring timekeeping or access control, keystroke monitoring, productivity tools and tracking internet activity.

We recommend that where organisations conduct, or plan to conduct, any kind of worker monitoring, internal policies are reviewed (e.g., work from home, acceptable use, BYOD, privacy and data protection, IT usage etc.) to determine whether amendments need to be made in light of the ICO guidance.

Below we set out eight key takeaways:

1. MONITORING IS PERMISSIBLE BUT MUST BE CONDUCTED IN COMPLIANCE WITH DATA PROTECTION LEGISLATION

- The ICO recognises that certain monitoring may be reasonable to achieve various aims, e.g., to protect health and safety, to meet regulatory requirements, and for security purposes; but some types of monitoring and/or excessive monitoring (e.g. video surveillance in bathrooms) are likely to intrude into employees' private lives and undermine their privacy and well-being and are incompatible with data protection legislation.
- Monitoring must comply with the principles laid out in data protection legislation including data minimisation, accuracy and security.
- There may be other legal implications under other legislation. Monitoring must be lawful in a general sense.
- Make use of the ICO's screening checklists (see here) before monitoring.

2. ONLY MONITOR WORKERS IN WAYS THAT THEY WOULD REASONABLY EXPECT AND NOT IN WAYS THAT CAUSE AN UNJUSTIFIED ADVERSE EFFECT ON THEM

- Remember that a worker's expectation of privacy is likely to be higher at home than when in the office.
- Be aware of the risk of capturing information about a worker's spouse or children, e.g., if workers use personal devices for work.

3. BE CLEAR ABOUT THE PURPOSE OF THE MONITORING AND IDENTIFY A LEGAL BASIS FOR IT

- Just because a form of monitoring is available does not mean that it is the best way to achieve your aims. You must be clear about your purpose ('just in case' is not sufficient) and select the least intrusive means to achieve it. You should be clear about what you intend to do with the information collected.
- You must identify one of the legal bases for the processing of the personal data you collect. Consent is not usually appropriate in an employment context, unless the worker has genuine choice and control. Generic consent in an employment agreement, or to a privacy policy, will not suffice.
- It is unlikely that worker monitoring is necessary to enable you to perform your obligations under the contract you have with the worker, so relying on 'contract' as your legal basis is unlikely to be appropriate.
- Legitimate interests is likely to be the most appropriate legal basis for worker monitoring, but the legitimate interest of the business in doing so needs to be weighed up against the risk of the worker's rights being overridden. Worker's rights are likely to be overridden if you are monitoring in ways a worker will not understand or will not reasonably expect or it is likely some workers would object. A legitimate interest assessment will help you to navigate the appropriateness and applicability of this legal basis.
- If the monitoring is likely to involve capturing more sensitive data i.e. 'special category data'[1] (even if you do not intend to), (e.g. CCTV) you will need a special category legal basis to process this data.

4. CONDUCT A DATA PROTECTION IMPACT ASSESSMENT ("DPIA") PRIOR TO ANY MONITORING

- If your monitoring will result in processing of personal data that is likely to result in a high risk to the worker, you must conduct a DPIA. High risk examples highlighted in the guidance include monitoring of email/message and keystroke monitoring, monitoring that involves processing of biometric data or which results in financial loss such as performance management. If your DPIA identifies a high risk that you cannot reduce, you must consult with the ICO before going ahead with the monitoring.

- The ICO strongly recommends that a DPIA is conducted before any worker monitoring, even if it is not mandatory to do so under the UK GDPR. If you decide not to conduct a DPIA when it is not mandatory, you should document your decision not to.

5. BE TRANSPARENT WITH YOUR WORKERS ABOUT MONITORING

- You must tell them about it in a manner that is accessible and easy to understand, apart from in very limited circumstances where covert monitoring may be justified.
- If you think that there may be circumstances where you may need to undertake covert monitoring (e.g., to detect suspected criminal activity or gross misconduct), you should outline in your worker policies the types of behaviour that are unacceptable and that may be subject to covert monitoring. Covert monitoring should always involve members of senior management and the completion of a DPIA. You must be satisfied that there are grounds for such monitoring and it should be subject to tight controls, and its scope should be strictly limited.
- Seek and document workers' views (e.g. by way of a Q&A session or seeking written feedback from workers) on monitoring prior to conducting it unless there is a good reason not to. If you choose not to, you should document this decision.

6. MONITORING THAT INVOLVES SOLELY AUTOMATED DECISION-MAKING

- Monitoring that involves solely automated decision making (i.e. decisions made by automated means without any meaningful human intervention) that has a legal or similarly significant effects on workers (e.g., decreasing a worker's pay based on their performance at work) is prohibited unless the decision (a) is necessary for the entry into or performance of a contract with that worker; (b) is authorised by law that applies to you (e.g., you have a statutory obligation to do something and automated decision making is the most appropriate way to achieve your purpose); or (c) based on the worker's explicit consent (i.e. to this specific processing – not a general consent).
- You must provide the worker with meaningful information about the logic involved in the automated processing, and the significance and the envisaged consequences of the processing for them.

7. MONITORING THAT INVOLVES PROCESSING OF BIOMETRIC DATA

- You should consider whether there are alternatives to using biometric data to achieve your desired objectives and provide an alternative for workers that wish to opt-out of the use of their biometric data. If there is an alternative and you decide not to use it, you should justify and document the decision in the DPIA.
- The nature of biometric data is that is it closely identified with a specific person, which increases the risk of harm to the worker in the event of a security breach. You must consider whether you need additional security measures when collecting, storing and using biometric data.

8. REMEMBER SUBJECT ACCESS REQUESTS ("SARS")

- Workers are entitled to make a SAR, which will extend to personal data collected and processed as part of any worker monitoring.
- The more personal data you collect and process as part of your worker monitoring, the more work you will need to conduct should a worker make a SAR, so consider the administrative burden involved with the SAR process when making decisions about worker monitoring.

1. 'Special Category data' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health, a person's sex life and a person's sexual orientation.

FOR MORE INFORMATION

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

BRIONY POLLARD

+44 20 7903 1372
briony.pollard@weil.com

MARK TAYLOR

+44 20 7903 1213
mark.taylor@weil.com

WEIL.COM

#97864250

Weil