Published on *The National Law Review* https://natlawreview.com

Employment Practices and Data Protection: Monitoring Workers 101

Article By:

Sophie F. Levitt

Claude-Étienne Armingaud

The Information Commissioner's Office (ICO) has recently published guidance for employers on monitoring workers lawfully, transparently and fairly. The guidance aims to protect workers' data protection rights and help employers to build trust with workers, customers and service users. With Artificial Intelligence (AI) on the rise, the temptation may be strong for employers to leverage those emerging technologies in that space. This alert summarizes some specific steps employers should prioritise in light of the ICO guidance.

BASIC DATA PROTECTION CONSIDERATIONS

Any worker monitoring process will likely entail the processing of personal data and, as a consequence, will require employers to duly assess the most relevant (and sole possible) legal basis for the processing operation, among the six allowed under the UK GDPR. These are:

- That the monitoring is necessary for:
    - The performance of a contract;
    - Compliance with a legal obligation;
    - Preserving the vital interests of an individual;
    - Carrying out a public task; or
    - Pursuing a legitimate interest (which will need to be balanced against the rights of the data subjects); and
- Consent, albeit consent is always a questionable legal basis in the employment realm, especially when it comes to monitoring, due to the perceived inequality in negotiating power between employer and employee.

Furthermore, should the monitoring involve special categories of data as set out in Article 9 UK GDPR, alternative legal bases may need to be assessed and these are most likely to create conflict with the workforce. This will notably be the case when monitoring employees' behaviour through biometrics (e.g. fingerprints, iris scanning, facial or voice recognition) used for the purpose of uniquely identifying an individual. In these circumstances, employers should document their reasons for relying on biometric data, including any consideration of other less intrusive means and why they

think they are inadequate. Employers should be clear about their purpose and why using biometric data is necessary. If a reasonable alternative option to using biometric data is possible, they should be able to justify why this method was not chosen. This must all be documented in a data protection impact assessment (DPIA).

In addition, prior to the implementation of any new monitoring process, employers will need to inform their staff, either through direct information or by updating any employee privacy notice already in place.

Below is a list of some of the key takeaways from the new ICO guidance.

USING MONITORING TOOLS THAT USE SOLELY AUTOMATED PROCESSES

Where monitoring would rely exclusively on automated decision-making, and considering the outcome of such monitoring would lead to a legal or similarly significant effects on individuals, employers will need to keep in mind that Article 22 UK GDPR provides for additional safeguards, namely the right for the individuals to opt out from that processing, and in order to effectively opt out, be informed of such automated decision-making.

VARIOUS MONITORING METHODS

Remote Working

The rise in remote/home working in a post-COVID society has led to an increase in monitoring workers remotely. Workers' expectations of privacy are likely to be higher at home than in the workplace, especially when using personal IT infrastructure to connect to the company's network. Employers should factor in the risks of inadvertently capturing family and private life information when implementing monitoring systems for remote workers. Employers should do this as part of a DPIA as well as in their legitimate interest assessment (LIA) when legitimate interest would be the chosen legal basis for the processing operation. LIA focuses on assessing legitimate interests i.e whether the processing is necessary to achieve its purpose and whether such interest is overridden by data subjects' rights, whereas a DPIA assesses both impacts and risks of a processing operation and ways to mitigate them.

Monitoring Phone Calls

According to the ICO, it is not usually proportionate to monitor the content of calls. Business calls could be monitored if it is necessary to provide evidence of business transactions, or for training or quality control purposes.

If an organisation changed the way they monitored calls as a result of information gathered during call monitoring, they should revisit their DPIA and carefully consider the implications of increased levels of monitoring.

Employers must inform workers of any call monitoring in their privacy information document, as well as informing the other individuals involved in the phone conversation, as required by Article 13 UK GDPR.

Monitoring Emails and Messages

The purpose of monitoring emails and messages must be clear i.e employers should make sure they

have a legitimate reason to monitor their employees (such as assessing performance and productivity in order to improve it) and any monitoring must be necessary and proportionate to the purpose. Workers must be informed of the purpose of any monitoring.

If employers are considering monitoring emails and messages, the ICO mandates that a DPIA be completed, taking into account the disproportionate risks to the rights and freedom of the individuals, as well as the risk of capturing special categories of personal data in the process (e.g. correspondence with trade union representatives or healthcare providers).

FINAL CONSIDERATIONS

Before deploying any worker monitoring technologies, employers must take steps to properly (i) assess the contemplated technology and its proportionality for the purpose for which it is being used, and (ii) inform their personnel of the nature and extent of, as well as the reasons for, such monitoring.

National Law Review, Volume XIV, Number 85