Increase in workplace monitoring – how can employers ensure that it is legally compliant?

According to a recent TUC survey, the use of workplace surveillance significantly increased during the pandemic when staff were working remotely. In this article, we look at the results of this survey (as well as one of our own) and consider what employers should do to ensure that they comply with the law when undertaking workplace surveillance.

What is workplace monitoring?

Workplace surveillance is a wider concept than you may think – it can include email or document monitoring, use of webcams, tracking what an employee is doing (or not doing) on their computer (for example keystroke logging), systems surveillance and location monitoring (e.g. GPS trackers in cars).

There are a number of legitimate business reasons that employers may want to put workplace monitoring in place, for example monitoring/increasing productivity, improving security, tracking network permissions and ensuring compliance with IT/security policies. There may also be regulatory reasons, for example telephone monitoring may be required in regulated sectors to ensure that no unlawful acts are carried out.

What does the survey say?

A recent survey by the Trades Union Congress (the "TUC", a UK body which represents the majority of trade unions) reports that 60% of workers believe they have been subject to some form of surveillance and monitoring at their current or most recent workplace and 28% of workers believe that this has increased since the pandemic. According to the survey, the financial services sector has the highest proportion of workers reporting surveillance (74%), closely followed by wholesale and retail (73%).

This mirrors the results of the Littler European Employer Survey, which found that nearly 60% of employers were either already using (17%), planning to use (23%) or potentially interested in (19%) software tools that track or monitor remote employees' productivity. Of those surveyed, 11% were unsure, and 30% said that they would not use this technology.

How can employers ensure that they comply with the law?

If employers are considering the use of employee monitoring, they should consider the legal implications of doing so. There is no one area of law which applies to employee monitoring in the UK, which makes this a tricky area and employers will therefore need to ensure that they comply with UK GDPR, the UK's electronic interception laws, the European right to privacy as well as the employment law implications.

The things that an employer should consider before implementing workplace monitoring are:

- **Is the monitoring justifiable?** The UK data privacy regulator, the ICO, says that "in an employment context, any surveillance of an employee needs to be necessary, justified and proportionate". It will therefore be for each employer to decide, based on the specific context of their business, whether surveillance is appropriate and whether there is a legal reason that can be relied upon.
- **Telling staff what you are doing.** Employee monitoring will not always be obvious, so employers should inform staff what they are doing, why they are doing it and what use will be made of the data. This may involve updating privacy notices or putting a separate employee monitoring policy in place or any other policies which set out the rules relating to the use of electronic systems.
- **What data will you collect?** Depending on the method of data collection, an employer may have some choice over what they collect. For example, is it possible to limit data collection to only specific types of websites? Could employers exclude websites for personal use, such as personal banking or personal medical websites or limit data collection only to working hours? Some software permits anonymous data collection, which will only be re-identified in specific circumstances only to individuals with authorisation.
- **What are you doing to do with the data you collect?** What use will be made of the data the employer collects and who will it be shared with, if at all? As best practice, employers should limit the circumstances in which the data will be accessed and the individuals who have access to it. It is also preferable for those individuals to be subject to confidentiality obligations and have received appropriate training. Another question to consider is how long the data will be retained after collection.
- **Conducting a risk assessment.** Where processing is particularly high risk (which is likely to be the case for employee monitoring) the employer will need to undertake a Data Privacy Impact Assessment (DPIA). This will involve setting out the purpose of the monitoring, the intrusion/adverse impact on staff and considering whether there is a less intrusive way to achieve the same objective.

Failure to be transparent about employee monitoring can damage employee trust and in extreme cases could lead to employees resigning and claiming that they have been constructively dismissed. From a data privacy perspective, non-compliance with the obligations can result in high fines from the ICO as well as negative publicity.

As the surveys demonstrate, employee monitoring is a growing area and employers are well advised to consider the risks and their compliance before implementing any such surveillance. We are also expecting more guidance from the ICO, so this is something to look out for!

If you have any questions about workplace monitoring or data privacy more generally, please contact Deborah Margolis or Darren Isaacs.

