Browne Jacobson

Monitoring workers – ICO guidance

04 October 2023

The ICO has published guidance aimed at employers on how monitoring workers may impact on data protection obligations.

The ICO had previously included guidance on monitoring at work within the Employment Practices Code, published in 2011. However, it recently consulted on new guidance, in large part due to the increase in homeworking/hybrid working following the pandemic and the greater privacy implications that can follow from monitoring in such circumstances. Whilst the guidance refers to "workers" throughout, it is intended to apply more widely to cover any relationship between an organisation and an individual where the individual carries out work for the organisation, regardless of the terminology used for this relationship.

Monitoring workers legally can only be carried out where there is a lawful basis for doing so. The guidance highlights the six lawful bases which may apply: consent; contract; legal obligation; vital interests; public tasks; and legitimate interests. However, it also identifies the potential limitations of these bases – for example, it may be considerably harder to demonstrate genuine consent within an employment relationship, due to the imbalance of power between employers and workers.

Where monitoring may capture special category data (such as biometric data or trade union membership), then in addition to a lawful basis for processing, there must also be a special category condition that applies. Where any processing is likely to cause high risk to workers' and other people's interests, a data protection impact assessment (DPIA) is required; examples given in the guidance of high-risk processing include the use of biometric data of workers, keystroke monitoring and any monitoring that may result in financial loss (such as performance management).

The guidance highlights the need for transparency (save in very few cases where covert monitoring may be permissible), accountability, a clear purpose, data minimisation (to avoid function creep where data collected for one purpose is used for another), accuracy and retention. There are also specific considerations included where employers wish to monitor workers who work remotely. The guidance refers to the fact that workers are likely to have to a higher expectation of privacy in their home than they would in an external workplace, and that there are increased risks of capturing family and private life information. A DPIA is suggested in these circumstances so that these risks may be properly assessed. Further guidance is given on specific types of monitoring – such as monitoring telephone calls or emails – as well as on the use of biometric data within the workplace.

This guidance provides a helpful summary of some of the points employers should consider in respect of any monitoring of employees. Given the pace with which working practices have changed and developed over the last few years, as well as advances in technology as a result, even employers who are confident in this area may find the updated guidance helpful in navigating some of the complexities and challenges that arise.

A copy of the guidance can be found here. If you would like to discuss the implications of this on your workforce, please feel free to contact us.

Key contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000