STEPHENSON HARWOOD

October 2020

Employment – 20:20 vision

Providing clarity and insight on employment law matters

Risks of remote working: How much can you monitor your employees?

Considering the Covid-19 pandemic, a shift to working from home has become the new normal for many employers. Whilst employees may work just as effectively from home as in the office, some employers are taking steps to monitor exactly what their employees are doing. Added to this are concerns that employees can more easily collate their employer's confidential information or plan to move to a competitor.

So how can employers use technology to protect their business? Is monitoring employees lawful?

In this e-alert we consider the benefits and risks of workplace monitoring and offer practical guidance for employers who are planning to implement monitoring systems.

What is workplace monitoring?

Workplace monitoring is any form of surveillance of employees. In a remote context, this can range from random spot checks of emails and internet use to installing more invasive software that records laptop screens and calls, tracks keyboard use or even uses facial recognition technology to monitor employee absences from their computer screens.

Employers commonly monitor their employees to analyse their performance at work, reliability, behaviour and location. Guidance from the Information Commissioner's Office makes a distinction between **occasional monitoring**, where an employer uses monitoring as a short-term measure in response to a particular need, and **systematic monitoring**, where employers monitor all workers or particular groups of workers as a matter of routine.

Are employers allowed to monitor their employees?

Employers have, for some time, included the right to monitor employees as a term in their contracts of employment or in their IT and communications policies. However, even if employers have the right to monitor their employees, they must consider the way they do so.

Employers should be mindful of the implied duty of trust and confidence, which exists in every employment relationship. If an employer excessively monitors employees, they could be in breach of this duty ultimately leading to employees resigning and claiming constructive dismissal.

Furthermore, excessive monitoring could constitute a breach of Article 8 of the European Convention on Human Rights ("ECHR") – the right to respect for private and family life. The concept of private life extends to the workplace and this right is engaged whenever there is a reasonable expectation of privacy. Whilst the Human Rights Act 1998 (which incorporates Article 8 of the ECHR into UK law) is only expressly applicable to public authorities, it is still relevant to all employers (including in the private sector) as courts and tribunals must try to interpret all legislation consistently with ECHR rights. To comply with the Human Rights Act 1998, employers must demonstrate that any monitoring is proportionate and necessary.

If an employer reasonably suspects that an employee is preparing to compete with the business or is collating confidential information to use against it, monitoring the employee's use of company computer systems is likely to be lawful.

What about data protection law?

Where employers are planning to monitor the activities of their employees, which in turn generates information relating to identifiable individuals, they must ensure that they are processing that personal data in compliance with the rules and principles set out in the General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA).

Key principles

Under the GDPR and DPA, any processing of personal data must have a **specific, explicit and legitimate purpose**. A legitimate purpose for monitoring employees may be, for example, to safeguard the security of personal data while employees are working remotely, to ensure compliance with legal obligations or to ensure an employee is performing their obligations under an employment contract. Once a legitimate purpose has been identified, the employer must ensure that any personal data collected for this purpose is only processed as necessary for that specific purpose, in accordance with the GDPR's purpose limitation principle. Key to this will be to establish whether the proposed monitoring will be within employees' reasonable expectations.

Another important consideration for employers monitoring employees is the principle of **data minimisation**. Personal data may only be collected if necessary to achieve a specific purpose. To establish this, employers will need to assess whether the collection of employees' personal data is proportionate to the purpose. For example, is it proportionate to record laptop screens to monitor the security of the organisation's data? Is it proportionate to collect data on the duration and frequency of employees' breaks to monitor performance and working hours? Is there another less intrusive way in which the same ends could be achieved? There may be adjustments that can be made to the proposed monitoring that could make it less intrusive and more likely to be lawful – for example, certain data may be analysed on an aggregated or pseudonymised basis in order to minimise personal data processing and risks.

Employers must also assess and document on which **legal grounds** they may collect and process the personal data of their employees when undertaking monitoring. It is generally not possible for employers to rely on consent as the legal ground on which to process the personal data of their employees, due to the imbalance of power in the relationship between employer and employee which makes it difficult to prove consent has been freely given. The appropriate legal ground will ultimately depend on the specific situation, but potentially relevant legal grounds include that the processing of personal data through monitoring is necessary for the performance of the employment contract, is necessary for compliance with a legal obligation to which the employer is subject, or is necessary for the purposes of legitimate interests pursed by the employer (where this is not overridden by the employees' rights and freedoms).

Documents

If an employer relies on the legitimate interest ground, it is prudent to carry out and document a **legitimate interest assessment (LIA)**, to ensure that the legitimate interest does in fact apply and that an audit trail is provided for the justification of that decision. Employees must be informed of any monitoring, in accordance with their right to be informed under the GDPR and DPA. Employers should review and update their **employee privacy policies** to ensure that they set out all the necessary details of the monitoring, where required. A privacy policy directed at employees should include details such as the purpose of the processing, the legal grounds on which the data are being processed, the recipients of the data and the period for which such data is being retained. If significant changes are made to any existing privacy policy, these must be brought to the attention of employees.

In order to consider, document and mitigate some of the risks of potential employee monitoring, it would normally be sensible to carry out a **data protection impact assessment (DPIA)**. It may even be mandatory to carry out a DPIA, which will be the case where the processing is *"likely to result in a high risk for the rights and freedoms"* of employees. Monitoring of employees is likely to satisfy this threshold especially where systematic monitoring is taking place, new technologies are being used, or evaluation or scoring is taking place based on that monitoring.

Employers considering undertaking evaluations of individuals based on monitoring should also note that the GDPR and DPA set out restrictions on

profiling employees and on making automated decisions in relation to them.

Practical steps to consider

- Employers should ensure their IT policies include the right to monitor. The policy should make clear who is authorised to monitor IT systems, which systems are monitored, who the information is shared with and the sanctions for computer misuse.
- Employers should also consider including references to monitoring in their working from home policies, especially if they plan to increase monitoring in light of the pandemic.
- The usual tell-tale signs that an employee is preparing to compete or is collating confidential information still bear out in a remote working context. Employers should have systems in place which can alert them when employees are working unusually late, printing excessively, downloading large amounts of company data or sending it to their personal email addresses or competing companies. For more information on this topic see our recent podcast.
- Employers must ensure they have identified a legitimate and specific purpose for which they process employee personal data through monitoring. In addition, employers must consider the following: is there an applicable legal ground that the employer can rely on for the processing of personal data? Is the processing of personal data actually necessary to achieve the purpose identified?
- Employers should review and update all employee privacy policies if they intend to conduct employee monitoring to ensure all necessary information has been incorporated in line with the GDPR and DPA. In the event significant changes are made to existing privacy policies, employers must ensure all employees are notified of the change.
- Employers should carry out a DPIA to identify and minimise the data protection risks of employee monitoring.

If you would like to discuss any of the issues covered in this e-alert please get in touch with any of the contacts listed below or your usual Stephenson Harwood contact.

Contact us

Paul Reeves
Head of employment, partner
T: +44 20 7809 2916
Email: Paul

Michèle Aubertin
Associate, employment
T: +44 20 7809 2264
Email: Michèle

Elspeth Hunt
Associate, employment
T: +44 20 7809 2903
Email: Elspeth

Katie Hewson
Associate, data protection
T: +44 20 7809 2374
Email: Katie

Kate Ackland
Associate, data protection
T: +44 20 7081 4174
Email: Kate