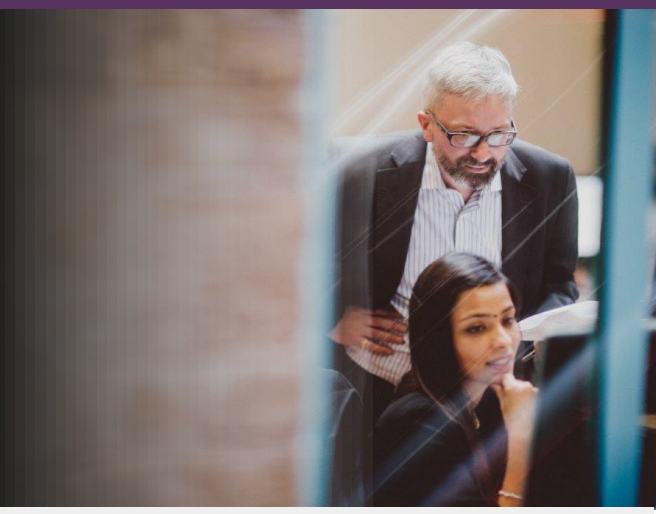
RIAA Barker Gillette

Overzealous monitoring may overstep data protection boundaries



November 2023

Employers who use software to help manage productivity and other employee activity may inadvertently violate data protection regulations.

Can employers monitor employees?

You can monitor employees if you do it in a way which is consistent with data protection law.

Data protection law does not prevent employers from monitoring employees. Instead, it requires employers to do so in compliance with existing data protection laws. Equally important is the Human Rights Act 1998 (HRA), which concerns a person's right to respect for private and family life. With the rise of homeworking, together with increased employer monitoring, this right is becoming increasingly important and relevant. An employee's expectation of privacy is likely to be significantly higher when working at home. Yet, the risk of recording private information increases the more employees work from home. Employers must balance employee's rights and freedoms against their business interests.

Impact of remote/hybrid working

Electronic monitoring of employees has risen in tandem with the rise in home working triggered by the Covid-19 pandemic. While the number working from home has dropped from its peak of 49% during the 2020 lockdowns, most recent figures from the Office of National Statistics show that around 40% of working adults still work from home at least some of the time.

Before the pandemic, the figure was around 12.5%, and the dramatic shift has driven businesses and organisations into uncharted territory to manage their workforce. Many have addressed the challenge through an increasing use of electronic monitoring to tackle any loosening of control.

New research from the Information Commissioner's Office (ICO), which oversees and regulates data protection and freedom of information in the UK, found that 19% of those surveyed believe an employer has monitored them.

Asked how they felt about being monitored, 70% of those surveyed by the ICO said it was intrusive. Only 19% were comfortable taking a new job where an employer would monitor their activity.

This discomfort echoes findings by the Trades Union Congress in 2022, which found significant and growing support amongst workers for stronger regulation of AI and tech-driven workplace surveillance, with more than 70% saying they believed technology-informed decision-making could increase unfair treatment. The TUC research found some sectors reporting very high levels of surveillance, for instance, more than 70% across the financial industry and the wholesale and retail sectors.

"Developments in software have made a range of options available to employers, making it all too easy to implement a form of monitoring, whether to check if people start work on time or to monitor activity – such as through the number of keystrokes made. However, employers should not take that ease of monitoring for granted. Any monitoring has to comply with data protection law," explains employment solicitor Patrick Simpson.

"There's also the potential breakdown in trust and reputational damage that may come through implementing what employees may consider to be a surveillance culture."

Patrick added: "Any surveillance needs to measure up against at least one of these criteria. However, in some situations, it may be tricky because of the imbalance in an employer/employee relationship. In some circumstances, employees may feel they are putting their jobs at risk if they dispute a planned form of monitoring.

"The best approach is to ensure not just that any action is legal, but also to be sure that employees know what is happening and have a sense of trust. It's too easy for surveillance to feel like an invasion of privacy, whether or not it passes the legal test. Policies also need to be reviewed and updated regularly to keep in line with any advancement in technology."

Six situations where monitoring is allowed

1. **Consent**
2. **Contract**
3. **Legal obligation**
4. **Vital interests**
5. **Public tasks**
6. **Legitimate interests.**

To support organisations in ensuring that any employee monitoring is lawful, transparent and fair, the ICO has issued guidance for employers, which highlights some of the key considerations:

- Making employees aware of the nature, extent and reasons for monitoring.
- Having a clearly defined purpose and using the least intrusive means to achieve it.
- Having a lawful basis for processing employees' data – such as consent or legal obligation.
- Telling employees about any monitoring in a way that is easy to understand.
- Only keeping the information which is relevant to its purpose.
- Carrying out a Data Protection Impact Assessment (DPIA) for any monitoring likely to result in a high risk to the rights of employees.
- Making the personal information collected through monitoring available to employees if they make a Subject Access Request (SAR).

The privacy watchdog has also warned employers, saying they will take action against employers if they threaten people's privacy.

What is a Data Protection Impact Assessment (DPIA)?

DPIAs are a formal procedure through which an organisation can assess the impact of data processing activities and protect personal data. Under the Data Protection Act 2018, you must carry out a DPIA when processing personal data is "likely to result in a high risk to the rights and freedoms of natural persons."

Even if not legally required, completing a DPIA helps you to identify and minimise the risks of any monitoring activity you might plan. The DPIA process includes a step to discuss your plans to introduce monitoring with employees. This step will help to shape your plans and build trust with your employees.

Speak to employment solicitor Patrick Simpson today for practical guidance on this complicated area of law. He can help to ensure your business is compliant with data protection obligations and to minimise the risk of claims from disgruntled employees.

Patrick Simpson
020 7299 7001
patrick.simpson@riaabg.com
www.riaabarkergillette.com