May 4, 2020

Employee monitoring during the COVID 19 lockdown GDPR considerations revisited

Attorneys
Robert Lister

The COVID-19 pandemic has forced organisations to reconsider their working arrangements and how employees interact with both internal and external clients and stakeholders. In the pursuit of maintaining a "business as usual" approach, many UK employers have questioned whether they can continue to effectively monitor their non-furloughed employees' performance when all but those in essential roles are working remotely.

While monitoring of employees both inside and outside the workplace is nothing new, and advances in technology in recent years have increasingly caused the boundaries between work and home to become blurred, the COVID-19 lockdown has brought these issues back to the fore. Employers may understandably have legitimate concerns around employee productivity – some employees may not have adapted to working as efficiently out of the office (particularly when juggling home schooling, family needs and work requirements), while others may take advantage of the lack of face time for their own personal benefit. However, does this mean that UK employers are justified in monitoring their employees in the privacy of their homes?

Technology providers have been quick to proffer potential solutions, offering tools that range in functionality from allowing organisations to continue to monitor remote usage of their information and communication technology (**ICT**) systems to capturing key strokes and data from work device webcams intermittently to check that employees are actually working. These monitoring technologies present significant GDPR compliance risks to organisations if left unchecked. If quick decisions are made regarding their implementation without due consideration of the relevant issues, organisations risk breaching their employees' fundamental rights to privacy and exposing themselves unnecessarily to potential enforcement actions by the Information Commissioner's Office (**ICO**).

It is therefore an opportune moment to remind ourselves of some of the existing principles regarding employee monitoring outlined by the ICO and the European Data Protection Board's predecessor, the Article 29 Working Party (**WP29**). This article highlights some of the key data protection-related issues for UK employers to consider when contemplating putting in place new tools or technologies to monitor their employees outside the workplace.

Background

The COVID-19 pandemic has not changed the UK legal landscape regarding employee monitoring. Various laws impact on its implementation and usage, including:

- Article 8 of the European Convention on Human Rights (implemented in the UK by the Human Rights Act 1998), which provides individuals with the non-absolute right to respect for private and family life and correspondence; and
- The GDPR and the Data Protection Act 2018 (given that almost all forms of employee monitoring will involve the processing of employees' personal data).

In addition, while not covered in this article, employers should also be aware of and consider potential UK employment law issues in the context of employee monitoring, particularly where disciplinary action may be taken as a result of such monitoring.

The key obligations arising under the GDPR regarding the processing of personal data collected from employee monitoring include that personal data must be demonstrably:

a. processed lawfully, fairly and transparently;

b. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; and

c. adequate, relevant and limited to what is necessary for those purposes.

The ICO has confirmed that it will take the compelling public interest in respect of the COVID-19 pandemic into account when assessing organisations' compliance with the GDPR. As such, if an organisation's practices fall short of its typical data protection standards, the ICO may not take regulatory action, understanding the need to prioritise other areas. This does not mean, however, that the ICO will refrain from pursuing serious breaches of the GDPR.

Guidance

Other than key GDPR security considerations relevant to remote working during the COVID-19 lockdown, the ICO has not yet issued any specific guidelines in relation to employee monitoring in this context. However, the ICO and WP29 have issued guidance directly covering the privacy implications of remote employee monitoring generally. Although this guidance was issued before the GDPR came into force, the principles remain relevant and the ICO is likely to take into account non-compliance with relevant recommendations when determining the extent of any enforcement action to be taken.

Key principles outlined by the ICO and WP29 include:

1. **Expectation of Privacy**: employee monitoring is typically intrusive and employees have an expectation of privacy in the workplace. When working from home, employees' expectations of privacy are significantly greater.
2. **DPIAs**: it will almost always be necessary to conduct a formal data protection impact assessment (**DPIA**), before implementing any form of employee monitoring.
3. **Legal Basis and Proportionality**: organisations may be able to rely on their legitimate interests as a legal basis to process personal data obtained through monitoring (e.g., to improve employee productivity or to ensure compliance with organisational policies). However, such interests must be balanced against employees' rights and reasonable privacy expectations, and the monitoring must satisfy a proportionality test (as documented in the DPIA), requiring organisations to:

    - identify why the monitoring is necessary and the tangible benefits that this will provide;

- identify any potential detriment to employees because of the monitoring, including the risk of harm, damage or distress, as well as mitigating factors;
- ensure that the purposes of monitoring are sufficiently important to justify limiting employees' rights to privacy;
- ensure that no more personal data than is necessary is collected; and
- ensure that there are no less privacy-intrusive alternatives available.

4. **Fair Processing Information**: employees must be provided with detailed information regarding the intended monitoring, including about:

   - why the monitoring will be carried out (and, if the monitoring relates to enforcing the employer's policies, employees must be clear what those policies are);
   - what the monitoring will involve and when and how it will take place;
   - how information obtained through monitoring will be used and to whom it will be disclosed; and
   - the safeguards implemented to protect employees and to mitigate against any risks to their personal data.

Covert monitoring can only very rarely be justified (such as when there are grounds for suspecting criminal activity or equivalent malpractice and where informing suspected employees would prejudice investigations).

5. **Safeguards**: safeguards should be implemented, including to ensure that personal data obtained through monitoring is:

   - only used in a manner consistent with the purposes originally communicated to employees. Only if the monitoring uncovers criminal activity (or equivalent activity that no employer could reasonably be expected to ignore) should the data be used for other purposes; and
   - subject to strict access controls – only a limited number of trained staff who are subject to confidentiality and security requirements should have access to the data.

Specific Use Cases

While typical monitoring by organisations of their ICT equipment usage when their employees are working remotely is unlikely to fall foul of the GDPR's requirements (if the recommendations above are followed), there are various forms of monitoring that, in the WP29's opinion, are unlikely to be lawful due to their disproportionate and excessive nature. These include:

1. intrusive ICT monitoring, including monitoring employee keystrokes and mouse movements/clicks, capturing images of employee screens and tracking application usage. Audio and video monitoring (e.g. through laptop webcams and microphones) should generally never be conducted in areas which employees would reasonably expect to be private (such as in their homes).

2. mobile device management software enabling organisations to locate or track ICT equipment remotely, if used as part of a wider programme enabling the ongoing monitoring of employees. Tracking systems must only be used for specified purposes, such as recovering property in the event of loss or theft.
3. where employees are permitted to use their personal devices for work purposes (e.g., under a Bring Your Own Device policy), the use of security scanning software allowing the organisation to access the employees' personal files in the absence of appropriate measures to prevent such access.
4. general employee monitoring through social media.

Conclusion

The COVID-19 lockdown presents opportunities for organisations to change their working practices, but careful consideration needs to be given before implementing remote monitoring tools. While employers' legitimate interests can be a valid legal basis for processing employee personal data collected from monitoring, this will only be permissible if the processing is strictly necessary for legitimate purposes that bring tangible and justifiable benefits and complies with the principles of proportionality and subsidiarity and the other rules set out above. Unless there are exceptional circumstances, particularly intrusive forms of monitoring should also be avoided entirely.

It is also clear that employers must, before using any monitoring tool, consider whether the processing outweighs the general privacy rights that employees have at home and what measures can be taken to ensure that any encroachment on their right to a private life is limited to the minimum necessary. In addition, just because you can, doesn't necessarily mean you should – particularly if there are any less privacy-intrusive alternatives available. Wherever possible, organisations should follow the ICO's and WP29's guidelines and recommendations and continue to monitor new recommendations made in the context of COVID-19. Organisations should also keep in mind that, even if the ICO may be temporarily relaxing enforcement activities due to the COVID-19 pandemic in certain limited circumstances, this does not mean that it will ignore serious breaches of the GDPR.