MAYER BROWN

WORKPLACE MONITORING How to Navigate the New ICO Guidance



The Information Commissioner's Office ("ICO") recently issued new guidance for employers on the monitoring of workers (see <u>here</u>). Data protection law does not prevent the monitoring of workers in the workplace, but it must be done in a way that is compliant with the law and fair. The guidance relates to employees as well as other people performing work for a company e.g. through the gig-economy.



1. What does 'monitor workers' mean?

Any form of monitoring of people who carry out work on behalf of a company. This includes:

- The systematic or occasional monitoring of workers
- Monitoring workers on work premises or elsewhere, such as when working from home or operating a company vehicle
- Monitoring workers during or outside of working hours
- Examples of monitoring include keystroke-logging, mouse-tracking software, location tracking of company assets and camera surveillance



According to the guidance, it is unlikely that organisations will be able to justify covert monitoring in most circumstances.

However, it may be permitted if, for example, it is necessary to prevent or detect suspected criminal activity or gross misconduct. Organisations should identify the circumstances in which it might take place in the relevant policy.

		-	
-		_	R
		.//	//
-	_	\boldsymbol{V}	

3. Is it necessary to notify workers of the monitoring?

4. Is it a legal requirement to have a policy in place?

No, it is not a legal requirement to have a policy in place. However, it is necessary to demonstrate compliance with data protection legislation.

Yes, workers have the right to be informed about the collection and use of their personal data.

As monitoring will involve both collecting and using personal data, it is necessary to tell workers about the monitoring in a way that is accessible and easy to understand. It is also necessary to notify workers if any changes to monitoring are introduced.

The guidance suggests that putting appropriate policies, procedures and measures in place may help demonstrate this. The policy should outline the nature, purpose and extent of the monitoring.

See the next page for steps you should now consider in light of the ICO guidance.

Checklist for Monitoring in the Workplace

Have a clear purpose for monitoring workers and ensure that there are no other reasonable and less intrusive ways to achieve that purpose. Companies should not monitor workers "just in case". Identify at least one of the <u>6 lawful bases</u> for monitoring workers under Article 6 UK GDPR, e.g. legal obligation or consent (which has strict requirements).

Where <u>special category data</u> (which includes biometric data such as facial images) is likely to be captured, identify one of the 10 conditions for processing the data.

Ensure that appropriate organisational and technical security measures are in place to protect personal information collected through monitoring. Ensure that any third party system or application is compliant with data protection legislation and that a contract is in place with the third party.

Detail why the monitoring is taking place and what you intend to do with the information you collect. Ensure that this information is readily accessible to workers so they are aware of any monitoring taking place. Keep this information updated. Assess whether a data protection impact assessment ("**DPIA**") is legally required or whether it would be beneficial to conduct one in any event. If the DPIA identifies that monitoring is high risk and that risk cannot be reduced, consult the ICO for further guidance.

Take reasonable steps to ensure that that any personal information collected is correct, kept updated and is not misleading. Correct any errors or erase incorrect information. Only collect as much information as is required to achieve your purpose. Erase any additional information and ensure that personal information is not kept for longer than necessary to achieve the purpose.

If you are considering making a <u>restricted transfer</u> of personal information outside of the UK, ensure that the transfer is covered by adequacy regulations, appropriate safeguards or an exception.

For further information about Mayer Brown's <u>data protection</u> or <u>employment & benefits</u> team in London, please contact your usual Mayer Brown contact or the individuals below.





Oliver Yaros

Partner, London







Mark Prinsley Partner, London Cybersecurity & Data Privacy E: mprinsley@mayerbrown.com T: +44 20 3130 3900



Miriam Bruce

Partner, London

Employment & Benefits

T: +44 20 3130 3695

E: mbruce@mayerbrown.com

Francesca Ingham Senior Associate, London Employment & Benefits E: fingham@mayerbrown.com T: +44 20 3130 3439

Cybersecurity & Data Privacy E: oyaros@mayerbrown.com T: +44 20 3130 3698

Please visit <u>mayerbrown.com</u> for comprehensive contact information for all Mayer Brown offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) and non-legal service providers, which provide consultancy services (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong & Nair LLC ("PKWN") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong & Nair Pte. Ltd. Details of the individual Mayer Brown Practices and PKWN can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2023 Mayer Brown. All rights reserved.

Americas | Asia | EMEA

mayerbrown.com