Employment practices guidance: Monitoring at work
Impact scoping document

Purpose of this document

Draft guidance on monitoring at work is now out for public consultation. This document is a high-level outline of some of the context and potential impacts of the draft guidance which we have considered so far. It is important to note that we do not intend for this document to provide an exhaustive assessment of impacts. It is just an initial overview of considerations. We are developing this work further into a more detailed impact assessment as we move towards publication of the guidance. The assessment follows best practice including, but not limited to, HM Treasury's Green Book.

We are seeking feedback on this document as well as any other insights stakeholders can provide on impacts through our call for supporting evidence.

Background

Problem under consideration

We published our current employment practices code in 2011. Since then, the world of work has changed considerably. Technology, employment relationships, data protection law and the COVID-19 pandemic have all impacted on working practices.

Workplace monitoring and analytics have increased over the last decade. We expect this trend to continue. A 2019 workplace survey of 239 large corporations showed that the number of large corporations using non-traditional[1] employee tracking technologies has increased from 30% to 50%.[2] A 2021 survey of employees suggested that 60% of them believe

[1] Non-traditional in this case means - analysing the text of emails and social-media messages, scrutinising who's meeting with whom, gathering biometric data and understanding how employees are utilising their workspace
[2] Gartner (2019) The Future Of Employee Monitoring

they have experienced some form of surveillance and monitoring at their current job, compared to 53% in 2020.[3]

During the pandemic, there was a large shift from office working to working from home. As a result, employers used more monitoring software, with global demand increasing by 108% in April 2020 and 70% in May 2020.[4, 5] A 2020 survey commissioned by YouGov suggests that 12% of all firms (16% of larger firms) that have employees working remotely have implemented online software to track employees and monitor productivity. One in ten of those that have not yet implemented such software plan to implement it in the future.[6]

The guidance

The guidance replaces the "Monitoring at work" chapter of the DPA98 employment practices code.[7] It has up-to-date guidance that is relevant to today's workplace.

We are aiming to create an online hub on our website, which would include separate pieces of guidance covering aspects of data protection and employment. This would update and replace the existing code of practice. We're intending for this new online resource to be more user-friendly and include topic-specific resources. It aims to address the changes in data protection law and reflect the changes in the way employers use technology and interact with staff.

Overarching objective

The overarching objective of the guidance is to provide relevant guidance, clarity and practical advice. This aims to help employers who are monitoring workers comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Legal and policy context

We have developed the guidance with consideration to relevant policies, the most relevant of which are set out below:

---

[3] The employee surveillance that fuels worker distrust - BBC Worklife
[4] Employee surveillance software demand increased as workers transitioned to home working | ZDNET
[5] Electronic monitoring and surveillance in the workplace - Publications Office of the EU (europa.eu)
[6] Remote-working Compliance YouGov Survey (skillcast.com)
[7] The employment practices code (ico.org.uk)

Legislation

We developed the guidance in accordance with relevant legislation on data protection and employment law, in particular the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). These laws control how organisations, businesses or the government use personal information.

The National Data Strategy

There are also specific areas of policy that the government is pursuing. Of most relevance to the use of data is the National Data Strategy.[8] This looks at how to use the UK's existing strengths to boost the better use of data across businesses, government, civil society and people.

The strategy has five main missions which set out the priority areas. These are:

- unlocking the value of data across the economy;
- securing a pro–growth and trusted data regime;
- transforming government's use of data to drive efficiency and improve public services;
- ensuring the security and resilience of the infrastructure on which data relies; and
- championing the international flow of data.

The fact that our guidance aims to assist organisations in complying with data protection legislation aligns well with the second mission, through improving trust in the data regime to enable growth.

UK Digital Strategy

Another important policy consideration is the UK Digital Strategy[9], which sits alongside the National Data Strategy with the following objectives:

- Unlocking the power of data.
- A secure digital environment.
- Enhancing the UK's place in the world.

Providing clarity and practical advice should help organisations to feel more confident about their use of personal data. This could help them to unlock the power of data securely.

---

[8] National Data Strategy - GOV.UK (www.gov.uk)
[9] UK Digital Strategy - GOV.UK (www.gov.uk)

Affected groups

The updated guidance could affect various groups. This is not an exhaustive list, but we tried to identify those which the guidance is potentially most likely to affect.

These include:

- UK employers;
- workers;
- the ICO; and
- wider society.

We have outlined below the scale of these affected groups.

Employers

As a key target audience, this guidance is likely to affect employers implementing or considering implementing monitoring. At this stage, we could not robustly estimate the number of employers who monitor workers or who are likely to do it in the future. Therefore, we have scoped in all employers to provide an upper end estimate. Using data from the ONS Business Population Estimates (BPEs), we estimate there are around 1.5 million UK organisations with workers.[10]

Table one: UK employers by public, private, and non-profit categories

Sector	Number
Private	1,447,900
Public	7,425
Non-profit	54,715
Total	**1,510,040**

Source: Business population estimates 2022 - GOV.UK (www.gov.uk)

Workers

As the subjects of the monitoring activity, the guidance has the potential to affect workers. This includes anyone likely to be monitored while working, for example:

- employees;
- self-employed contractors; or

[10] Business population estimates 2022 - GOV.UK (www.gov.uk)

- volunteers.

Using ONS data on UK population levels and employment levels, we estimate that there are 27.1 million[11] workers in the UK and 3.8 million self-employed people. For those that are self-employed, it is not possible to identify who is likely to be monitored. Therefore this is an upper end estimate. This also does not account for those who are volunteers, as it is not possible to identify those who are not already included in the workers figure to avoid double counting.

The Information Commissioner's Office (ICO)

As the UK's data protection regulator, the ICO is affected by this guidance.

Wider society

This guidance is likely to impact more than just UK employers and workers. It may have an indirect impact on wider society, with the potential to affect groups such as:

- trade unions;
- civil society groups; and
- the wider population.

It is difficult to estimate who the guidance would and wouldn't affect indirectly. As such, we estimate the whole population as a conservative, upper-end estimate. According to latest estimates, there are around 66,980,300 people in the UK.[12] There may also be businesses that have no workers that are indirectly affected through their connection to employers or wider societal impacts. This currently totals 4.1 million businesses.[13]

[11] This figure comes from the APS Nomis - Official Census and Labour Market Statistics - Nomis - Official Census and Labour Market Statistics (nomisweb.co.uk) This source only provides figures for those aged 16-64. Note that this excludes workers 65 and over and therefore is likely to be an underestimate of employment.
[12] Using census data from E&W and NI, with Mid Year estimates for Scotland 2021
[13] Business population estimates 2022 - GOV.UK (www.gov.uk)

Impact scoping

The table below outlines some of the potential impacts (benefits and costs) we have considered on each of the affected groups. This is not an exhaustive list, and it does not imply any hierarchy of impacts considered. We have not yet considered the likelihood or magnitude of any of these impacts. Many of them may not materialise or may only impact small subsets of the affected groups.

Table two: Potential impacts

Employers	Workers	ICO	Wider society
Benefits			
• Greater degree of regulatory certainty. • Reduced potential to face regulatory action from the ICO if the guidance is followed. • Higher workplace morale resulting in higher employee retention with associated productivity benefits. • Improved DP compliance could lead to increased trust from consumers.	• Reduced risk of data protection harm to workers. • Higher morale amongst workers.	• Gives a better position to assess compliance and take appropriate regulatory action where required. • Providing guidance may help mitigate the burden of regulatory action later. • Less likelihood of complaints from members of the public.	• Reduction in harms could improve overall societal welfare. • Benefits to business could lead to knock-on benefits to wider society.
Costs			
• Costs of familiarisation with the guidance. • Compliance costs could increase for employers that are not already compliant. • Sunk costs for organisations which have invested in monitoring software that they now realise is non-compliant.	• Reduced workplace monitoring using personal data could lead to increases in other forms of monitoring (eg micromanagement).	• Reputational risk if ICO is perceived to have overreached.	• Disbenefits to business could lead to knock-on disbenefits to wider society (eg suppliers of monitoring software).