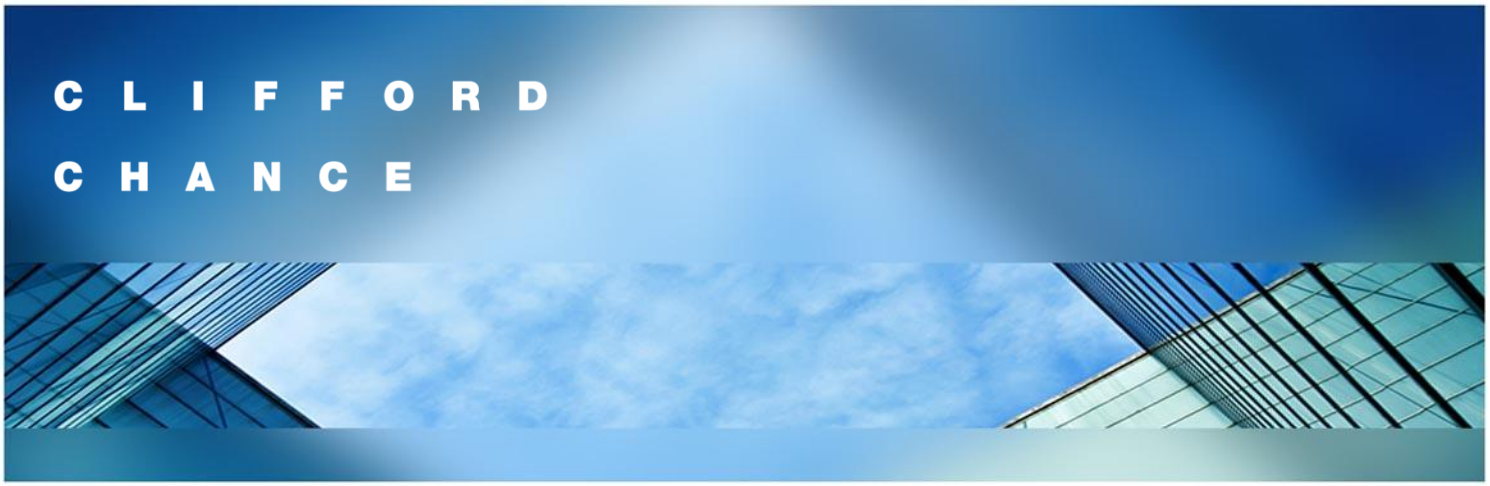

MONITORING IN THE WORKPLACE: DIRECTION OF TRAVEL

Monitoring employees in the workplace is not new but the methods by which this is achieved, the workplace itself and relevant regulatory regimes are continually evolving. The UK's Information Commissioner's Office (ICO) has published for consultation draft Guidance on Monitoring at Work. Coincidentally, in the same week the international press reported a Dutch case in which the courts awarded an employee in the region of €75,000 after being dismissed for refusing an instruction to keep his webcam on for the entire duration he was logged on to his work PC.

Key issues

- Monitoring: what, why, how?
- ICO Employment Practices: monitoring at work draft guidance
- Draft Monitoring Guidance: Key Points
- Data Protection Impact Assessments
- Consulting the workforce
- Objections to monitoring
- Covert monitoring
- Automated decision making
- Video monitoring emails, instant messaging and phone calls
- Personal devices and personal communications on work devices
- Policies, procedures and day to day working practices
- Timeline and action points
- Webcams: Global survey

This Briefing examines the issues that can arise in the context of workplace monitoring, in particular examining the ICO's draft guidance and taking a high-level look at whether employees may be required to keep their webcams on during the working day in various jurisdictions.

MONITORING: WHAT, WHY, HOW?

Post pandemic, the world of work has evolved quite considerably. Hybrid working is, for many, now a permanent feature of that world. Rapidly evolving technology has facilitated this shift and equipped employers with the means by which employees can be monitored.

Monitoring may take many different forms including the use of heat and motion sensors to assess desk occupancy; software programmes that monitor breaks, keystrokes, computer, app and instant messaging usage, email activity and overall individual productivity. Some software can send automated push notices in relation to such monitoring.

A 2020 YouGov survey suggested that 12% of all firms (16% of larger firms) that have employees working remotely have implemented online software to track employees and monitor productivity. More recently, new research from the CIPD and HiBob shows that 55% of bosses agree with collecting information on regular home workers, including the amount of time spent on laptops each day and email sending behaviours to identify risk of burnout.

Monitoring may be driven by a variety of legitimate (and competing) concerns: employee wellbeing, improving productivity and space planning/building efficiency. This mix makes getting the right balance difficult. Employers are legally obliged to maintain a safe place of work; this includes an employee's home workplace when hybrid working arrangements are in place. Physical

and mental health are in scope of this duty and technology can be an effective tool to meet this obligation. It is also legitimate to use office space usage monitoring tools to manage and reduce workplace costs as well as to optimise hybrid working arrangements.

The use of monitoring tools can also create significant issues, adversely impacting employer relations with employees and trade unions, harming physical and mental wellbeing and giving rise to potential discrimination and other employment claims and data protection breaches if not handled appropriately. Employees may feel personally targeted - there is anecdotal evidence that some have felt unable to take breaks which is important for eye and musculoskeletal health and required by some medical conditions (which may qualify as disabilities under the Equality Act 2010). A working environment that inhibits this could place an employer in breach of its health and safety obligations and could lead to constructive dismissal and/or discrimination claims.

ICO EMPLOYMENT PRACTICES: MONITORING AT WORK DRAFT GUIDANCE

Having regard to the potential for employee monitoring to give rise to breaches of data protection laws, the ICO's draft guidance on monitoring at work (Monitoring Guidance) is timely. It is part and parcel of the ICO's programme to produce updated data protection and employment practices guidance given that the current Employment Practices Code dates back to 2011 and in some respects may be considered obsolescent.

Once finalised, the Monitoring Guidance will feature on the ICO's proposed online hub, which will include separate pieces of guidance covering aspects of data protection and employment aimed at helping employers comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (together '**Data Protection Legislation'**).

The suspension and review of the recently introduced Data Protection and Digital Information Bill (DPDI Bill), together with comments made by government ministers about reviewing the UK's current data protection regime create uncertainty as to the continued relevance of ICO guidance that is based on the current regime, including the ICO Employment Practices Guidance. However, the approach taken under the DPDI Bill, and the desire to retain EU adequacy for the UK, would suggest that we might expect a regime that is based on the existing framework and, therefore, that much of the existing and prospective guidance would remain relevant.

DRAFT MONITORING GUIDANCE: KEY POINTS

The Data Protection Legislation does not, as such, prevent employee monitoring; however, where it involves the processing of personal data, it sets out the legal framework within which it must occur. Key points to note:

- **Type of monitoring**: the draft guidance addresses both systematic and occasional monitoring by employers.
- **Homeworking:** the draft guidance clarifies that monitoring in the context of homeworking does not constitute personal or household

processing (in relation to which there are exemptions from the Data Processing Legislation), and so is also covered by the draft guidance.

- **Minimum intrusion**: employers should use the least intrusive means of monitoring to achieve their aim.

- **Privacy Notices**: employers must make workers aware of the nature, extent and reasons for the monitoring unless exceptional circumstances mean that covert monitoring is necessary.

- **Purpose of monitoring**: in most circumstances employers must not use the information collected for a new purpose unless it is compatible with the original purpose.

- **Lawful processing**: an employer must identify the lawful basis for the processing (e.g. maintaining a safe place of work, compliance with law, legitimate business interest) and, if special category data will be processed, a legal basis for processing special category personal data under the Data Protection Legislation.

- **Data protection impact assessment (DPIA):** a DPIA should be carried out for any monitoring that is likely to result in a high risk to the rights of workers and other people captured by the monitoring. Where a DPIA is not mandatory, employers should consider completing one anyway as good practice.

- **Assumptions:** employers should not assume that monitoring data is accurate or that commercial monitoring tools have the appropriate level of security protection built in.

- **Regular review**: employers should carry our regular reviews of the nature, impact and purpose of any monitoring.

DPIA

The draft Monitoring Guidance provides that an employer must carry out a DPIA before undertaking any processing likely to cause high risk to workers' and other people's interests. What does 'high risk' mean in practice?

In the section addressing specific types of monitoring, the draft Monitoring Guidance states that if an employer is considering monitoring emails and instant messages, a DPIA should be completed as this poses a high risk to workers' data protection rights and freedoms and is likely to capture special category data. The DPIA could be completed even if it is not required as a matter of good practice and to assess any risks involved.

It is worth noting that the European Data Protection Board (**EDPB**) is also of the opinion that the workplace monitoring requires DPIA to be performed under article 35 of the EU GDPR.

The draft Monitoring Guidance goes on to say that employers will find it difficult to justify the monitoring of emails and messages where monitoring network data would meet the employer's purpose. This does not preclude monitoring which involves access to the content of emails and messages – which some employers use, for example, in relation to checking for breaches

of law – provided such access is necessary and proportionate in meeting the employer's legitimate objective.

CONSULTING THE WORKFORCE

The ICO's view is that employers should seek and document the views of workers or their representatives on proposed monitoring unless there is a good reason not to; where an employer elects not to do so it should record its decision along with a clear explanation.

While workforce consultation can potentially pre-empt any employee concerns about the use of monitoring and help shape an employer's approach, many employers may already have various forms of monitoring in place where the staff have not been consulted. The draft Monitoring Guidance does not address what is expected of the employer in such a scenario.

OBJECTIONS TO MONITORING

The draft Monitoring Guidance addresses a worker's qualified right to object to an employer collecting and processing personal data through monitoring if the lawful basis relied upon is the employer's legitimate interests. Where an objection is made, the employer must carry out a balancing exercise considering the worker's interests, rights and freedoms with its identified legitimate interests to assess if those legitimate grounds override those of the worker.

Having regard to the right to object, employers should ensure that their internal procedures facilitate the recognition of such objections and that they are dealt with both in the context of the Data Protection Legislation and good employment practices. Common law, health and safety and Equality Act obligations, amongst other things, may be relevant factors in any balancing exercise.

The draft Monitoring Guidance also addresses an employer's right to refuse to comply with an objection if it is manifestly unfounded or excessive. Employers have long been in search of clearer guidance on when a data subject access request (DSAR) or objection can be treated as manifestly unfounded or excessive. Unfortunately, the example provided in the consultation that "A worker repeatedly sends different requests to you on a regular basis with the stated intention to cause disruption" does not really take matters any further forward; in reality such stated intentions are few and far between even if employer and employee alike know this to be the case.

The Data Protection and Digital Information Bill proposes changing this exception to apply where a request or objection is vexatious or excessive. If this were to become law, we would expect to see further ICO guidance as to how "vexatious" should be interpreted.

COVERT MONITORING

The ICO accepts that covert monitoring may be required in exceptional circumstances such as to prevent or detect suspected criminal activity or

gross misconduct; however, the suggested context in which it is carried out is quite restrictive. Amongst other things, it is suggested that covert monitoring:

- should only be authorised by the highest authority in the workplace;
- should not be used to capture communications that workers would reasonably expect to be private, such as personal emails; and
- should only be carried out after a DPIA has been conducted.

The first bullet point above in particular could be challenging as, read literally, this would be a company's CEO or equivalent. The second bullet point can also create difficulties in practice where workers use company email systems to send personal emails.

Other elements of the draft Monitoring Guidance in relation to covert monitoring are not surprising; for example, it must be strictly targeted at obtaining evidence within a set timeframe which should be limited to the shortest time possible and must not continue after the investigation is complete.

AUTOMATED DECISION MAKING

In some cases, monitoring practices involve automated decision making. Some monitoring software can send automated push notices; for example, reminding individuals to take a break from their desks, making suggestions on how to improve their productivity, or indicating that they are about to access a restricted website. Other software may be used to monitor productivity and output for the specific purpose of calculating pay.

If monitoring involves automated decision making that is used to inform legal or similarly significant decisions about workers (such as quantum of pay), an employer will be subject to additional obligations and restrictions under the UK GDPR, including restrictions as to when such processing can be lawfully carried out, information obligations with respect to impacted workers and obligations to give effect to the right of impacted workers to request human intervention to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge an automated decision. These restrictions can restrict how companies carry out certain processes – for example, they can lead to the insertion of a human decision maker in a process in order to bring it outside of the scope of the relevant UK GDPR restrictions, which can have consequences for cost, efficiency and consistency.

The draft Monitoring Guidance states that, if automated systems are designed as decision-support tools (i.e. being used to inform, rather than make, decisions), and are therefore outside the scope of the UK GDPR restrictions and obligations in relation to automated decision making, the employer should ensure that a human can, in broad terms, meaningfully review, interpret and check the automated recommendation. It would have been helpful if the ICO had provided examples of the types of monitoring-related automated decision making that fall into either this category or the restricted category of automated decisions with 'legal or similarly significant' effect for the data subject.

The Data Protection and Digital Information Bill proposes changing the restrictions on automated decision making with a legal or similarly significant effect for the data subject in a manner that would allow such automated decisions to be carried out in a broader range of circumstances. They would,

however, still remain subject to safeguards in relation to employee transparency and rights to challenge.

VIDEO MONITORING EMAILS, INSTANT MESSAGING AND PHONE CALLS

Each of the above forms of monitoring are addressed in some detail. Some key points to note:

- Continuous video or audio monitoring of workers is only likely to be justified in rare circumstances.
- The ICO considers that it would not usually be proportionate to monitor or record the content of calls in all cases. It may be undertaken if it is necessary to provide evidence of business transactions, comply with law, or for training or quality control purposes.
- Monitoring the content of emails and messages will be difficult to justify where monitoring network data would meet the employer's purpose.

PERSONAL DEVICES AND PERSONAL COMMUNICATIONS ON WORK DEVICES

The draft guidance implicitly suggests that monitoring an employee's personal devices (mobile phone, laptop etc.) is permissible (subject to compliance with the Data Protection Legislation) but only to monitor business related communications where the worker is using their own personal devices for work.

Equally, the ICO considers that it will be difficult to justify accessing a worker’s personal communications on any work device.

The use of personal devices for work purposes and work devices for personal purposes should be expressly addressed in an employer's policies whatever approach is adopted. The ICO suggests that employers consider banning the private use of work devices and blocking problematic websites. In practice this may not be realistic and in any event the ICO's view is that such a policy would not usually justify accessing an employee's private communications on work devices. There appears to be a tension between the ICO's view here and an employer's interest in ensuring adherence to workplace policies and discipline (and, in some cases, an employer's legal obligations in relation to certain conduct or risks e.g. prevention of insider trading).

An employer needs to be clear in its policies and day-to-day practice whether employees can, or are expected to, use private devices for work and, if so, what monitoring and/or access to the communications may be required and for what purposes. If access to personal devices is contemplated the practical issues around this should be carefully considered; there will be significant amounts of private personal data on such devices and many employees will understandably object to it being accessed. A more practical approach, in line with the approach of many financial regulators is to ban the use of private devices for any work-related matters.

POLICIES, PROCEDURES, AND DAY-TO-DAY WORKING PRACTICES

Not only should an employer's privacy notice accurately reflect the nature of the employer's processing in terms of monitoring activity but, in addition, an

employer's policies and procedures may also require updating. Failure to do so can give rise to adverse personnel relations issues with employees and employee representatives, in some cases potentially lead to allegations that the implied term of trust and confidence has been breached and may impact on the fairness of disciplinary action. For example, if an employer intends to use data gathered from monitoring for capability or conduct purposes and general enforcement of policies (e.g. personal phone/internet usage) that should be made clear in its procedures.

The draft guidance also makes the point that what happens in practice should align with the written policies and procedures as workers base their expectations of privacy not only on policy but also on practice. The ICO's view is that excessive monitoring set out in a policy does not make it lawful, just because it is documented. In any event, it is good practice to align practices with procedures; failure to do so will otherwise potentially compromise the fairness and reasonableness of any disciplinary or other corrective action.

TIMELINE AND ACTION POINTS

Although the ICO consultation does not close until 11 January 2023, the draft guidance gives employers a clear indication of the ICO's expectations. In any event, employers are already required to comply with the Data Protection Legislation; as such consideration should be given to:

- Conducting an audit of all current monitoring in the workplace;
- Identifying the purpose(s) of the monitoring;
- Identifying the lawful basis for the processing and any special category condition;
- Assessing whether data privacy notices, policies, procedures and day-to-day practices require updating (for example, acceptable usage, disciplinary and grievance procedures);
- Factoring into policies and practices any regulatory guidance or requirements in relation to the use and/or monitoring of personal devices;
- Auditing retention policies to assess if they adequately address monitoring data; and
- For multinational employers, assessing whether a 'global' approach to workforce monitoring is possible. If not, care will need to be taken to adequately address local law requirements in relevant jurisdictions.

WEBCAMS: A QUICK GLOBAL STRAW POLL

In the Dutch case (Chetu Inc.) (referred to above) the employee worked as a telemarketer for the Dutch branch of the US parent, Chetu Inc. In the US an instruction to keep the webcam on whilst logged into work was lawful; however, the Dutch court considered that the instruction to leave the camera on was contrary to the employee's right to respect for his private life.

This case illustrates that a global approach to employee monitoring is likely to be challenging for multi-nationals as evidenced by the quick straw poll below.

Global straw poll: Can an employer insist that its employees keep their desk webcams switched on whilst they are logged on (whether at home or in the office)?

Jurisdiction	Yes	No	Possibly: its complicated
Hong Kong			X
United Kingdom			X
US	X		
Spain		X	
Belgium			X
France		X	
Luxembourg			X
Italy		X	
The Netherlands		X	

In those jurisdictions where the answer is: *'Possibly: its complicated'* it will invariably depend on the factual circumstances including: the purpose of the monitoring; whether the webcam monitoring will be permanent or only during specific calls/timeslots; whether there are other means to achieve the purpose.

In some jurisdictions such as France and Spain the data protection authorities have already provided guidance on the issue of monitoring.

ICO Consultation The consultation is open until **11 January 2023**.

ICO draft guidance on monitoring at work

ICO Impact scoping document

2020 YouGov Survey Remote-working Compliance YouGov Survey (skillcast.com)

Chetu Inc Judgment

CLIFFORD
CHANCE

CONTACTS

Alistair Woodland
Partner
Global Co-Head of Employment

T +44 20 7006 8936
E alistair.woodland
@cliffordchance.com

Floris van de Bult
Partner
Global Co-Head of Employment

T +31 20 711 3158
E floris.vandebult
@cliffordchance.com

Tania Stevenson
Knowledge Director
Employment Group

T +44 20 7006 8938
E tania.stevenson
@cliffordchance.com

Rita Flakoll
Knowledge Director
Telecoms, Media & Technology

T +44 20 7006 1826
E rita.flakoll
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ