GDPR and Employee Surveillance

The regulatory framework around employee surveillance is complex and easy to fall foul of. A few years ago, West Yorkshire Fire Service faced criticism when a 999 operator, who was on sick leave, found a GPS tracker planted on her car by a private detective hired by her bosses.

At present all employers have to comply with the Data Protection Act 1998 (DPA) when conducting surveillance, as they will be gathering and using personal data about living identifiable individuals. Part 3 of the Information Commissioner's Data Protection Employment Practices Code (Employment Code) is an important document to follow to avoid DPA breaches. It covers all types of employee surveillance from video monitoring and vehicle tracking to email and Internet monitoring.

When the General Data Protection Regulation (GDPR) comes into force (25th May 2018) it will replace the DPA. The general rules applicable to employee monitoring as espoused by the DPA and the Employment Code will remain the same. However there will be more for employers to do to demonstrate GDPR compliance.

Data Protection Impact Assessment

One of the main recommendations of the Employment Code is that employers should undertake an impact assessment before undertaking surveillance. This is best done in writing and should, amongst other things, consider whether the surveillance is necessary and proportionate to what is sought to be achieved.

Article 35 of GDPR introduces the concept of a Data Protection Impact Assessment (DPIA) (also known as a Privacy Impact Assessment) as a tool, which can help Data Controllers (in this case employers) identify the most effective way to comply with their GDPR obligations. A DPIA is required when the data processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). Employee surveillance is likely to be high risk according to the criteria set out by the Article 29 Working Party in its recently published draft data protection impact assessment guidelines.

The GDPR sets out the minimum features which must be included in a DPIA:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Data Controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.

- An assessment of the risks to individuals.
- The measures in place to address risk, including security, and to demonstrate that the Data Controller is complying with GDPR.

Before doing a DPIA, the Data Protection Officer's advice, if one has been designated, must be sought as well as the views (if appropriate) of Data Subjects or their representatives. In some cases the views of the Information Commissioner's Office (ICO) may have to be sought as well. In all cases the Data Controller is obliged to retain a record of the DPIA.

Failure to carry out a DPIA when one is required can result in an administrative fine of up to 10 million Euros, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Our recent blog post and forthcoming DPIA webinar will be useful for those conducting DPIAs.

Article 6 – Lawfulness

All forms of processing of personal data (including employee surveillance) has to be lawful by reference to the conditions set out in Article 6 of GDPR (equivalent to Schedule 2 of the DPA). One of these conditions is consent. Article 4(11) states:

> *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

As discussed in our previous blog post, consent will be more difficult to achieve under GDPR. This is especially so for employers conducting employee surveillance. According to the Information Commissioner's draft guidance on consent under GDPR:

> *"consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis."*

Employers (and public authorities) may well need to look for another condition in Article 6 to justify the surveillance. This could include where processing is necessary:

- for compliance with a legal obligation to which the Data Controller is subject (Article 6(1)(c));

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller (Article 6(1)(e)); or

- for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (Article 6(1)(f)).

Legitimate interests (Article 6(1)(f)) will be a favourite condition amongst employers as usually the surveillance will be done to prevent or detect crime or to detect or stop abuse of the employers' resources e.g. vehicles, internet and e mail facilities etc.

Public Authorities

Article 6 states that the legitimate interests condition shall not apply to processing carried out by public authorities in the performance of their tasks. Herein lies a potential problem for, amongst others, local authorities, government departments, and quangos.

Such organisations will have to consider the applicability of the legal obligation and public interests/official authority conditions (Article 6(1)(c) and Article 6(1)(e)) respectively). We can expect lots of arguments about what surveillance is in the public interest and when official authority is involved. If the surveillance involves a public authority using covert techniques or equipment to conduct the surveillance, it is easy to assume that Part 2 of the Regulation of Investigatory Powers Act 2000 ("RIPA") applies and so the latter condition is met. However, the Investigatory Powers Tribunal has ruled in the past that not all covert surveillance of employees is regulated by RIPA (See C v The Police and the Secretary of State for the Home Department (14th November 2006, No: IPT/03/32/H),).

More detail on the RIPA and human rights angle to employee surveillance can be found in our blog post here. More on the DPA angle here.

We also have a specific blog post on the legal implications of social media monitoring as well as a forthcoming webinar.

Transparency

All Data Controllers, including employers, have an obligation to ensure that they are transparent in terms of the how they use employee's information. Consideration will also have to be given to as to what extent general information will have to be supplied to

employees in respect for the employer's surveillance activities (See our blog post on Privacy Notices).

Surveillance of employees can be a legal minefield. Our forthcoming webinar on GDPR and employee surveillance will be useful for personnel officers, lawyers, IT staff and auditors who may be conducting or advising on employee surveillance.

Act Now *can help with your GDPR preparations. We offer a GDPR health check service and our workshops and GDPR Practitioner Certificate (GDPR.Cert) courses are filling up fast.*