MSS
THE PERSONNEL PEOPLE

EMPLOYER UPDATE

Surveillance Of Employees At Work

Whilst there may be legitimate reasons why an employer may wish to monitor his/her employees using surveillance, there are serious risks involved for the employer in doing so, the most notable of which is the risk of invading an employee's privacy in the workplace.

A recent case in the Employment Appeals Tribunal has highlighted the risks for employers in relation to the implementation of secret surveillance of employees and in taking disciplinary action against employees on the basis of evidence acquired through surveillance operations.

Recent Case- Unfair Dismissals Act 1977-2007

The Employment Appeals Tribunal heard that the employer had summarily dismissed the claimant for gross misconduct including; fraud, falsification of records and inaccurate fraudulent recording of financial transactions, in particular, handing in expense forms for business trips not taken.

This action was taken on the basis of a surveillance operation carried out by the company. The company had placed a tracking device on the respondent's vehicle and used independent Investigators to carry out surveillance of the claimant on two occasions. The Company claimed that the surveillance was implemented following a "trigger" of poor sales performance.

This use of surveillance was not known by the employee, either before or during the operation.

The Tribunal deemed the dismissal Unfair for the following reasons;

- The surveillance equipment used was without the knowledge of the employee.
- The letter sent to the employee did not sufficiently set out the allegations against him.
- The Company failed to provide the evidence collected through surveillance in advance of the meeting and failed to give the employee a reasonable opportunity to consider the evidence in accordance with their disciplinary policy.
- Insufficient time was taken in reaching the decision to dismiss the employee, the employee having been notified fifteen minutes after the conclusion of the Meeting.

Whilst the Tribunal was satisfied that the employee had made a significant contribution towards the dismissal and had reduced the compensation amount to reflect this, the employee was still awarded a compensation amount of **€30,000.**

We would advise that employers note the following guidelines;

- Conduct surveillance operations fairly.
- Issue a policy outlining when monitoring or surveillance may take place and ensure this is circulated to all employees.
- Have legitimate reasons for implementing surveillance footage. (Note: A third party may disallow an employer to rely on surveillance, where it is deemed covert and goes beyond the intended purpose.)
- Strike a balance between protecting employer's legitimate interests and minimising the invasive nature of monitoring for employees.
- Adhere to the company's disciplinary policy, ensuring to conduct fair disciplinary investigations, in

considering whether disciplinary action is warranted.

Employees are extensively protected by both the Data Protection Act 1998-2003 and by privacy related law under the European Court of Human Rights.

Surveillance under the Data Protection Act 1998-2003

The surveillance of employees at work involves "data processing" and is subject to the following principles of the Data Protection Act;

- The data or information must be obtained and processed fairly.
- The data must be kept only for a specified and lawful purpose.
- The data must not be used in any manner incompatible with that purpose.
- The data must be adequate, relevant and not excessive in relation to that purpose.
- The data must not be kept for longer than is necessary for that purpose.
- Security measures should be taken to ensure the data is kept safe and secure.

European Court of Human Rights Case

In **Copland v United Kingdom (2007),** a case in the European Court of Human Rights**,** the court gave a ruling against a college which had monitored the employees email, telephone and internet usage.

The court ruled that Article 8 of the ECHR which states that "everyone has the right to respect for his private and family life, his home and his correspondence", was breached and that just as the employee "had a reasonable expectation as to the privacy of calls made from her telephone…the same expectation should apply in relation to…email and internet usage".

Code of Practice on Protection of Worker's Personal Data

The International Labour Office (ILO) devised a **Code of Practice on the Protection of Worker's Personal Data** and whilst it is not legally binding, it is influential when third parties such as Tribunals are making decisions. It recommends the following;

- The reasons for and schedule of monitoring, as well as the methods to be used, should be informed to employees.
- The intrusion to workers must be minimised.
- **Secret Monitoring** should only be used if it conforms to national legislation or if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing.

If employers wish to succeed in cases where the employee's privacy is at issue, it is strongly advisable that employers have devised a **Data Protection Policy**, and that it is implemented fairly and sets down the employer's position in relation to any surveillance of employees which they decide to engage in.

It must also incorporate the requirements set down by the Data Protection Act 1998-2003 and take into account the other recommendations and recent case law outlined above.

This update is provided by the MSS HR Support Service

Further details on the Update or about our services may be obtained from

John Barry/ Tara Lacey/ Amy Vickers at - Tel: 01 8870690

Email: hr@mssirl.com - website: www.mssirl.com