[**Jonathan Ashmore**](https://www.my-course.co.uk/user/view.php?id=16729&course=8028)

**Initial Post**

This case study refers to the use of CCTV footage in a disciplinary process of a security guard who was required to monitor the CCTV system at night. Irony aside, the complainant’s defence stated he was unaware that the company could use CCTV footage in disciplinary meetings and was a breach the employee’s personal data 2003 (Data Protection Commission, n.d.). This pre-GDPR complaint came under the Republic of Ireland’s Data Protection Acts 1988-2003 (Data Protection Commission, 2017).

The specific GDPR that addresses this case is Article 6(1)(f) which states the following:

‘[where] processing is necessary for the purpose of the legitimate interests pursued by the 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’ (www.gdpreu.org, 2020).

The Data Protection Commissioner’s view was the company had a legal basis, *legitimate interests,* for using the CCTV footage for disciplinary proceedings as the complainant’s actions could cause reputational and financial loss to the company. Furthermore, the business had used the footage in a minimal manner to corroborate other findings, and the employee had read and signed a Certificate of Understanding and Standard Operating Procedures. Therefore, the Commissioner found in favour of the company.

If I was an information Security Manager, I would have implemented two processes. Annual fraud training for all employees including misuse of company assets and inaccurate reporting of time (Halvorson, 2022). Annual reading and signing of updated company policies in line with legal and contractual obligations of both parties such as Safeguarding, GDPR, SOP, Employee Code of Conduct, and Workplace health and safety (www.indeed.com, 2020).

‌

When you summaries anything from the above text reference it to (Jonathan,2022) ;