Use of CCTV footage in a disciplinary process.

We received a complaint from an individual regarding the use of CCTV footage by their employer in a disciplinary process against them. The complainant informed us that while employed as a security officer, their employer had used their personal data, in the form of CCTV footage, to discipline and ultimately dismiss them. The complainant stated that they had not been given prior notification that CCTV footage could be used in disciplinary proceedings.

In the course of our investigation, the employer informed us that the complainant had worked as a night officer assigned to client premises, and had been required to monitor the CCTV system for the premises from a control room. The employer's position was that, upon being assigned to the client premises in question, the complainant had been asked to read a set of "Standing Operating Procedures" which indicated that CCTV footage could be used in an investigative process concerning an employee. The employee had also been asked to sign a certificate of understanding to confirm that he had read and understood his responsibilities. The employer maintained that the CCTV system in place at the client premises was not used for supervision of staff as there was a supervisor at the premises during office hours between Monday and Friday.

The employer informed our investigators that it was the complainant's responsibility, as the sole night security officer on duty at the client premises, to monitor the CCTV system for the premises from the control room. The requirement to have a night security officer on duty in that control room for that purpose was a term of the employer's contract with its client. The employer was also contractually obligated under its contract with its client to carry out routine audits of employee access cards (which were swiped by the holder to gain access to various locations in the client premises). The employer told us that during such an audit, it had discovered irregularities in data derived from the complainant's access card which could not be the result of a technical glitch as those irregularities were not replicated in the access card data of the complainant's fellow night officers. These irregularities suggested that the complainant had been absent from their assigned post in the control room for prolonged periods of time on a number of separate occasions. On the basis of the access card data irregularities and upon noting the apparent absence of the employee from the control room during prolonged periods, the employer had commenced an investigation into the employee's conduct. During the course of this investigation, the complainant disputed the accuracy of the access card data, and had sought that the employer provide further evidence of his alleged prolonged absences from the control room. The employer had therefore obtained CCTV stills at times when the access card data suggested the complainant was away from their post in order to verify the location of the complainant. The employer maintained that because the CCTV system was independent of the access card data system, it was the only independent way to verify the access card data. The employer also provided us with minutes of a disciplinary meeting with the complainant where they had

admitted to being away from the control room for long periods. The employer also informed us that the complainant had later admitted in an email, also provided to us, that the reason for these absences was that the complainant had gone into another room so that they could lie down on a hard surface in order to get relief from back pain arising from a back injury.

We queried with the employer what the legal basis was for processing the complainant's personal data from the CCTV footage. The employer's position was that as a result of its contractual obligations to its client (whose premises were being monitored), if an adverse incident occurred during a period of absence of the assigned security officer (the employee) from the control room, that would potentially expose the employer to a breach of contract action by its client which could lead to significant financial and reputational consequences for the employer. On this basis the employer contended that it had a legitimate interest in processing CCTV footage of the employee for the purpose of the disciplinary process. Under Section 2A(1)(d) a data controller may process an individual's personal data, notwithstanding that the controller does not have the consent of the data subject, where the processing is necessary for the purposes of the legitimate interests pursued by the data controller. However, in order to rely on legitimate interests as a legal basis for processing, certain criteria have to be met as follows:

There must be a legitimate interest justifying the processing;

The processing of personal data must be necessary for the realisation of the legitimate interest; and

The legitimate interest must prevail over the rights and interests of the data subject.

Having considered the three step test above, the Commissioner was satisfied that the employer had a legitimate interest in investigating and verifying whether there was misconduct on the part of the employee (or whether there was a fault in the access card security system). Furthermore, the Commissioner considered that the use of the CCTV footage was necessary and proportionate to the objective pursued in light of the seriousness of the allegation because it was the only independent method of verifying the accuracy of the access card data. The Commissioner noted that the CCTV footage was used in a limited manner to verify other information and that the principle of data minimisation had been respected. Finally, given the potential risk of damage to the employer's reputation and the need to ensure the security of its client's premises, the Commissioner was satisfied that the use of CCTV footage for the purpose of investigating potential employee misconduct, which raised potential security issues at a client premises, in these circumstances took precedence over the complainant's rights and freedoms as a data subject. On the issue of whether the controller had provided the complainant with notice of the fact that their personal data might be processed through the use of CCTV footage, the Commissioner was satisfied that there had been adequate notice of this by way of

the SOP document which had been acknowledged by the complainant signing the certificate of understanding.

This Commissioner therefore, formed the view that the employer had a legal basis for processing the complainant's personal data contained in the CCTV footage under Section 2A(1)(d) of the Data Protection Acts 1988 and 2003.

This case demonstrates that the legal basis of legitimate interests will only be available to justify the processing of personal data where, in balancing the respective legitimate interests of the controller against the rights and freedoms of the data subject, the particular circumstances of the case are clearly weighted in favour of prioritising the legitimate interests of the controller. It is an essential that in order to justify reliance on this legal basis that the processing in question is proportionate and is necessary to the pursuit of the legitimate interests of the controller.

Ref:

https://dataprotection.ie/en/pre-gdpr/case-studies#201710

Specific Aspect of GDPR Addressed:

This case study primarily examines the legitimate interest and legal basis for processing personal data under the GDPR, particularly in utilising CCTV footage within a disciplinary process. The pertinent aspects of GDPR to be considered are:

1. Article 6(1)(f) Legitimate Interests: This allows for the processing of personal data when it is necessary for the legitimate interests of the data controller, provided the rights and freedoms of the data subject do not override these interests.

2. Transparency and Fair Processing (Articles 1214): The case also touches on the requirement for transparency, as employees must be informed about how their data will be used, including the use of CCTV footage for disciplinary purposes.

How It Was Resolved:

The Data Protection Commissioner, a regulatory authority responsible for enforcing data protection laws, resolved the case. They determined that the employer had a

legitimate interest in using the CCTV footage to investigate the security officer's alleged misconduct. The Commissioner concluded that:

The processing of CCTV footage was necessary and proportionate to verify the accuracy of the access card data.

The employer's legitimate interest in ensuring security and fulfilling contractual obligations outweighed the employee's privacy rights.

The Standard Operating Procedure (SOP) document serves as a comprehensive guide to the organization's processes and procedures. It effectively informs employees about the potential use of CCTV footage, detailing the circumstances under which CCTV footage could be used, the rights of the employee, and the process for handling such data.

Thus, the Commissioner upheld the employer's use of the CCTV footage, ruling that it was lawful under GDPR.

Steps to Mitigate the Issue as an Information Security Manager:

As an Information Security Manager, to mitigate similar issues, the following steps could be taken:

1. Develop and Implement Clear Policies:

Create or update privacy policies explicitly stating how CCTV footage may be used, including for disciplinary purposes.

Ensure that these policies comply with GDPR, specifically regarding transparency and the legitimate interest legal basis.

2. Employee Notification and Training:

Ensure that all employees are clearly informed, through documented policies (e.g., SOPs), that CCTV footage may be used for investigative or disciplinary actions.

Provide regular training sessions on data protection rights and responsibilities, including the specific use of CCTV in the workplace.

3. Data Protection Impact Assessment (DPIA):

Conduct a DPIA specifically for the use of CCTV systems, evaluating potential risks to employee privacy and ensuring that the organisation's legitimate interests do not override individual rights.

4. Minimisation and Purpose Limitation:

Ensure that CCTV footage is only used for the purposes specified in the privacy policy and that only relevant footage is accessed and retained.

Regularly review and audit the use of CCTV footage to ensure compliance with data minimisation.

5. Regular Audits and Reviews:

Periodically audit the use of CCTV footage and related data processing activities to ensure ongoing compliance with GDPR.

Review and update the legitimate interest assessment regularly, especially when there are changes in how CCTV is used.

6. Record Keeping:

Maintain detailed records of all instances where CCTV footage is used for disciplinary actions, including the rationale for its use and how it complies with GDPR.

By implementing these steps, an organisation can better manage the use of CCTV footage in disciplinary processes while ensuring compliance with GDPR and protecting employee rights.