E-Portfolio Activity – GDPR Case Studies

There are several case studies from 2014 – 2018 concerning GDPR related issues and breaches. Chose a case study (should be unique to each student) and answer the following questions:

- *What is the specific aspect of GDPR that your case study addresses?*
- *How was it resolved?*
- *If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?*

Chosen case: Use of CCTV footage in a disciplinary process

Under the following link you can access the case study: https://dataprotection.ie/en/pre-gdpr/case-studies#201704

What is the specific aspect of GDPR that your case study addresses?

The case study addresses the aspect of GDPR related to the **legal basis for processing personal data**, specifically whether the use of CCTV footage in a disciplinary process is justified under the principle of **legitimate interest**.

How was it resolved?

The Data Protection Commissioner concluded that the employer had a legitimate interest in using CCTV footage to investigate the employee's conduct. The processing was deemed necessary, proportionate, and in accordance with the principle of data minimization. The employer also provided adequate notice to the employee through documentation, leading to the conclusion that the processing was lawful under the Data Protection Acts 1988 and 2003.

As an Information Security Manager, to mitigate issues related to the use of CCTV footage in disciplinary processes, I would take the following steps:

1. **Clear Policy and Communication**: Ensure that all employees are informed through clear policies (e.g., in the employee handbook) about the use of CCTV footage, including its potential use in disciplinary actions.
2. **Legitimate Interest Assessment**: Regularly conduct and document a legitimate interest assessment to justify the use of CCTV in line with GDPR requirements.
3. **Data Minimization**: Use CCTV footage only when necessary and ensure it's only used to address specific incidents, minimizing data usage.
4. **Training**: Provide regular training to employees on data protection and the proper use of surveillance tools.
5. **Access Control**: Implement strict access control to CCTV footage, ensuring that only authorized personnel can view or process the data.
6. **Regular Audits**: Perform regular audits to ensure compliance with data protection laws and internal policies.