Unit 5: GDPR Case Studie

For this activity I have chosen the following case study:
https://dataprotection.ie/en/pre-gdpr/case-studies#20163

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

I would argue that in this case study, there are the following three different aspects which GDPR addresses:

- 5. Storage limitation – There were insufficient control masures on the retention of dormant user accounts.
- 6. Integrity and Confidentiality – The security level for personal data was not high enough to prevent or defend attacks such as a brute force attack.
- 7. Accountability – as there was a data breach, due to the controller was not able to demonstrate compliance to GDPR with the proccesses which were in place.

How was it resolved?

The company concerned has taken these two measures:

- Implementation of passwords which require more than one factor
- Implementation of a comprehensive data retention policy

If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?

If this was my organisation, I would have applied the following measures:

- 2FA
- Email notification after password change to affected account
- Account blocking after 10 incorrect login attempts
- Use system which detects anommalies (odd number of login attempts, suspicious login location, etc.)
- Propose data protection training for all employees to management
- Find out whether the inactive user data must be legally retained, if so, store it to a secure archive, if not, delete it.