**Initial Post - Agne Angelides**

I have chosen the case study ‘Disclosure of Personal Data via a Social Media App' (Data Protection Commission, 2017), which overviews a situation during which a job position application cover letters have been photographed using a personal mobile phone and shared on a social media Platform by one of the retailer’s employees.

The said occurrence was in breach of the GDPR Article 5: Principles relating to processing of personas data (GDPR, 2018). The article requires for the data will be collected for the specified purpose only (in this case, employment) and to be processed in a way that ensures the data security.

The commissioner who reviewed this case has found the retailer was in breach of the data protection laws specific to the UK (Data Protection Acts 1988 and 2003), equivalent to the current GDPR at the time.

Whilst the retailer had the policies in place disallowing use of personal phones at a workplace which the employee was in violation of, additional security related steps could have been taken by the company, such as:

* Annual employee behaviour code and personal data security training (CIPD, 2021).
* Inclusion of the restrictive covenants in the employment contract (Harper James, 2021) to prevent the employee from performing certain activities after the employment termination has been issued.
* The recruitment data should be accessible by senior staff on the need to know basis only (Maxfield, 2021).

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