# GDPR Case Study: Disclosure of Personal Data via a Social Media App

This case study primarily addresses the GDPR principle of purpose limitation, specifically how organizations must ensure personal data is only used for its intended purpose. In this instance, job application materials containing personal data were misused by being shared on social media, completely diverging from their intended recruitment purpose. The case also highlights responsibility of a data controller to ensure their organization remains accountable for their employees' handling of personal data, even during employment transitions.

The Commissioner resolved this case by finding the retailer in violation of Section 2A(1) of the Data Protection Acts 1988 and 2003. This ruling was particularly significant as it rejected the retailer's defense that the incident was unavoidable due to the employee's impending departure. The decision reinforced that data controllers maintain responsibility for personal data protection regardless of employee circumstances or intent.

As an Information Security Manager addressing this specific incident, I would focus on three key areas of mitigation:

First, I would implement a secure digital application process to replace physical CV submissions. This would include an applicant tracking system with appropriate access controls and audit logging, eliminating the need for paper documents that can be easily photographed or shared inappropriately.

Second, I would establish a clear chain of custody for any physical applications that must be accepted. This would involve a secure reception point where documents are immediately scanned and stored digitally, with the physical copies securely destroyed. Staff handling these documents would work in areas where mobile devices are prohibited and monitored through both technical controls and supervision.

Finally, I would create specific data handling procedures for the recruitment process. This would include training for all staff involved in recruitment on their data protection responsibilities, clear guidelines on appropriate handling of applicant information, and specific procedures for securing personal data during employee transitions. The procedures would be backed by regular audits and spot checks to ensure compliance.

These focused measures directly address the vulnerabilities exposed in this incident while remaining practical to implement and maintain.