WILLIAM FRY

Employers Beware – How Safe Is Personal Data Held by Your Company?

On 21 June 2016, the Irish Data Protection Commissioner (the "Commissioner") published its annual report for 2015. One case study relating to the removal of records from the workplace to a private residence will be of particular interest for employers.

The facts

The case study concerned a complaint made to the Commissioner by a member of the Defence Forces that his personal data was not being kept safe by the Defence Forces. The complainant had made an internal complaint and a military investigating officer (MIO) was appointed to review it. The Defence Forces Ombudsman was appointed to review the process of the handling of the complaint, and it emerged that the MIO could not supply notes of the interview he had conducted with the complainant as he had brought them home, where they were subsequently lost or damaged following a burglary and flooding at the MIO's house.

The Commissioner's findings

The Defence Forces acknowledged that the loss of data should not have occurred. However, they stated that while such an action would normally constitute an offence under the Defence Act 1954, the MIO was no longer a serving member and was no longer subject to military law. Nevertheless, the Commissioner found that the Defence Forces had contravened Section 2(1)(d) of the Data Protection Acts 1988-2003 by "*failing to take appropriate security measures against unauthorised access to, or unauthorised alteration, disclosure of destruction of the complainant's personal data when it allowed it to be stored at an unsecure location, namely a private house*."

Lessons to be learned

This case study is of significant importance for employers as there are various workplace scenarios in which staff may need to take home files containing personal data. The Commissioner's finding acts as a reminder that extreme caution should be exercised to ensure there is no risk to the security of personal data in such a situation. A system recording the taking and returning of files should be in place, as well as approved measures for the safekeeping of personal data while files are outside of the workplace. Employers should ensure that employees are prohibited from emailing official files from workplace email accounts to personal email accounts, as in such a

scenario, the data controller (i.e. the employer) loses control of the personal data, which they are obliged by law to safeguard.

Please contact Catherine O'Flynn, Partner on the William Fry Employment & Benefits Team, at catherine.oflynn@williamfry.com or +353 1 639 5136 should you have any queries.

Follow us on Twitter @WFEmploymentlaw