Use of Shared Drives and Data Protection

Email sent to all staff on 30th April 2018

Dear Colleagues

Please give this your immediate attention. I cannot stress the importance of you acting on this email advisement.

Two data breaches have been brought to my attention in the lasts few days both of which relates to the use of and access to shared drives on computers.

Please note if you place any personal information on a shared drive, wherever that shared drive is located, it is IMPERATIVE to ensure that it kept secure and safe while it is on the drive. This is the responsibility of each and every staff member that puts information on to a shared drive and also the manager that is responsible for that particular work area.

That is :

1. You must ensure only Institute personnel in your area that require access to it to do their duties, have access to it. IF ANYONE ELSE HAS ACCESS TO IT EVEN WITHIN YOUR OWN DEPARTMENT– THEN THAT IS A BREACH OF DATA PROTECTION LEGISLATION. IF PERSONNEL HAVE MOVED DEPARTMENTS THEIR ACCESS TO THAT DRIVE SHOULD BE IMMEDIATELY REMOVED AND DOCUMENTED.

2. If you must keep these records, please ensure they are up to date – IF THEY ARE NOT UP TO DATE, THAT COULD BE DEEMED EXCESSIVE RETENTION OF DATA AND AGAIN IS A BREACH OF DATA PROTECTION LEGISLATION. You must be able to prove why you have the data in first place, what you are doing with it, how long you intend to keep it and how you will purge it.

3. Such records must be kept secure – as noted above, a. access should be clearly monitored and a security access log kept along with b. an audit of when the shared drive is reviewed and updated. IN THE EVENT OF A DATA BREACH FROM MAY ONWARDS, WHEN I REPORT A BREACH TO THE OFFICE OF THE INFORMATION COMMISSIONER, AS WE ARE OBLIGED TO DO, THEY WILL EXPECT MANAGERS TO PRODUCE THIS LOG TO DEMONSTRATE VIGILANCE IN THIS REGARD.

While I have noted all of the above to you before during meetings, information notices, correspondence and in conducting DP audits and interactions on breaches or possible breaches of DP etc, I would seriously urge you to now take on board my advisement on this matter. While the misuse of a shared drive constitutes a data breach now, from May 25th with implementation of new DP/GDPR legislation, such breaches have much more serious consequences for everyone in the Institute with the introduction of data subjects ability to litigate and the right of the Data Commissioner to apply monetary penalties for non-compliance with the new legislation. If non-compliance is determined by the DP Commissioner, excuses of ignorance or lack of time/resources will not be entertained.

Despite all our interactions on the above, I can absolutely guarantee based on what I have seen/learned to date, that if I were to access any of the shared drives in operation in DkIT this morning, 100% of them would be non-compliant with Data Protection in some capacity so action is key and the onus for compliance is on everyone.

REMBEMBER : Personal data relates to any data where any living individual could be identified by putting together one or more pieces of personal data for example for students it might be the likes of:
Name, address, date of birth, email, telephone no, student ID, programme of study, photo, continuous assessments / grade results, correspondence, PPS no, nationality, gender,

Kind regards

Loretto Gaughran
Freedom of Information Officer
Data Protection Office