www.mplegal.im

LEGAL

REVIEW

A ‘simple’ data protection breach: to report to the Information Commissioner or not to report?

back home forward

contact us

September 2019

Advocates, Solicitors & Attorneys
an incorporated legal practice

september 2019

A 'simple' data protection breach: to report to the Information Commissioner or not to report?

"I hit "send" and then realised I had sent it to the wrong email address" is a well coined phrase probably used by all of us at one stage in our career (if not more!). Very few people can attest to never having made this simple human error and yet the error itself is more than that, it's a potential data protection breach which needs consideration – without undue delay and within 72 hours. Predictive email addresses are usually the key factor in this mistake occurring.

The recent data protection laws which enact the general data protection regulations (GDPR) can make simple human errors like this, important ones for companies (and all controllers/processors). Companies should continue to raise awareness of the significance of this human error with all of their staff. We are over one year into the new legislation and you may think that you have heard enough about GDPR; perhaps you believe that you were scared unnecessarily that the Information Commissioner would call you and fine you €20 million immediately (or £1 million if you are lucky enough to live on the Isle of Man), or maybe you read this content in the knowledge that your company is compliant, feeling prepared to take on any data protection issue as and when it arises – if so, you are in a good place.

A moment of inward reflection is necessary for companies to ask themselves the question *"so what actually happens if a staff member sends the email to the wrong email address?"* If your company's answer does not involve an assessment and some reference to internal procedures with an emphasis – hopefully in bold red font – on 72 hours, then it is (generally speaking) likely that you would not be compliant with data protection laws. The answer is of course to be pro-active, not re-active.

The 72 hour clock starts from the moment the staff member appreciates the mistake and confirms that the breach has occurred. It's a simple human error so this may not be until a week later when they come to send a chaser email to the individual or company, or it may be instantaneous. More embarrassing (albeit probably most often) is when you send the email and the response is what triggers the realisation that you have sent it to the wrong email address. The question is then whether you report to the Information Commissioner and, if you are to report, you must do so without undue delay and within 72 hours. The reality of the 72 hour period means that your company must react immediately and has less than 72 hours from the time of knowledge of the breach to determine whether to report the breach or not. Given that any normal company works on average 9 hour days and individuals actually have more time out of the office than in the office in any 24 hour period, you can see how easily the 72 hours can quickly fly-by. It's not 72 working hours, it is 72 hours. If a company cannot notify the

A 'simple' data protection breach: to report to the Information Commissioner or not to report?

Information Commissioner within the 72 hours then it must be able to justify the delay.

Should you report? Various factors will need to be given consideration when your company is deciding whether to report or not, this decision should ideally be given to management or the data protection officer but ultimately someone accountable. A non-exhaustive list of things to consider might include:

1. On the whole, what are the consequences of the breach?
2. What risk does this breach present to the individual(s)?
3. The personal data contained within the email, was it sensitive or special category (as defined in GDPR) in nature?
4. Is the personal data contained within the email already accessible to the public via other means?
5. How many individual's personal data have you breached?
6. To what extent has the personal data which has been shared, been recovered? I.e. have you been able to recall the email?
7. Have reassurances been obtained from the unintended individual receiving the email that the email has been deleted (including deleted from the deleted items), has not been forwarded or circulated in any way and has not been printed?
8. What harm could be caused to the subject of the personal data due to the breach?
9. Should the individual(s) to whom the personal data belongs be informed?

It would be prudent for a company to have in its procedures a checklist of considerations for data protection breaches so as not to overlook a key consideration. An example referred to often is where, in open and active court proceedings, you are sharing details of court pleadings with an unintended party. In such circumstances, a vast amount of the personal data may already be available to the public by virtue of requesting a court transcript.

A company is obliged to inform the individuals of a breach occurring where the breach is likely to result in a high risk to their rights and freedoms. The company in breach must do so without undue delay. A company, when assessing risk should be looking to categorise the risk into three categories: (i) no risk, (ii) a risk, or (iii) a high risk. It is common sense to apply a simple test: the more sensitive the data or the greater volume of data, the higher the risk. If the consequence of the breach is more severe, for example the breach could result in mental or physical harm, damage to reputation or identity theft, it is also likely in those circumstances that the risk would be higher.

It is recommended that a security breach management plan be implemented which provides guidance to a company's staff members as to what to do in the event of

A 'simple' data protection breach: to report to the Information Commissioner or not to report?

a breach. It is also recommended that a company keeps an adequate record of the breaches and reviews their policies and procedures to ensure compliance. As a company, you cannot protect against all human error but you can be ready to react to ensure that you are data protection compliant. And on a preventative basis, a basic reminder to all staff always to double check the email recipients before sending will never go amiss.

Advocate Amelia Quinn is an associate at M&P Legal and an accredited data protection practitioner. This article provides general guidance, specific advice is needed on particular cases.

M&P LEGAL

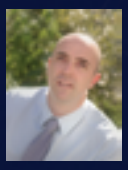
REVIEW

back home forward

contact us

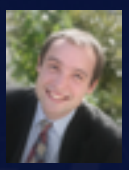
Profiles

Click on a profile to be taken to our web site for full details



Christopher J Murphy
Joint Managing Director
cjm@mplegal.im

John T Aycock
Joint Managing Director
jta@mplegal.im



Christopher M Brooks
Consultant
cmb@mplegal.im

Damian P Molyneux
Director
dpm@mplegal.im

Consuelo Suay
Consultant
csc@mplegal.im

Amelia J Quinn
Associate Advocate
ajq@mplegal.im

Carol A Young
Conveyancing Manager
cay@mplegal.im

Niall M Prentice
Senior Paralegal Assistant
nmp@mplegal.im