The importance of GDPR

Mike Morris 20th July 2019

I read today that British Airways has been fined £183 million by the Information Commissions Office for failing to defend their website from a "sophisticated, malicious criminal attack", under the Data Protection Act 2018 (the UK implementation of the European General Data Protection Regulations). Hackers managed to divert users of the British Airways website to their own, fraudulent site and so managed to harvest the details of half a million people. There is a lot of information that can be collected from an airline website user, not the least of course is financial data. But think how much more information could be harvested if hackers gained access to patient clinical data. At the very least you might receive unwanted advertising for products that claim to treat something that may be wrong with you – at worst, maybe blackmail to prevent a condition that you wanted to remain private from getting into the public domain?

If you stop to consider it, having your personal information available to members of the public could be pretty awful. Of course, most of us are unlikely to share financial data as we know the risk, but would you want to share information on your relationships; whereabouts; social habits; travel plans; illnesses; education; dietary preferences; sexual preferences; religion, etc? If the government passed a law to say that we all had to disclose this sort of information, there would be a public outcry.

No one would willingly share information like this would they? No? Have a look at a young person's Facebook entries.

It is part of the social need to have the largest number of friends. Not friends that the older generations would recognise of course, but Facebook friends – 75% of whom are never met face to face – and some of which are false personas.

As we grow older, we are more likely to perceive the risks and less likely to share personal information, but once on the World Wide Web, it stays there. It is currently impossible to track down every copy of every piece of information related to one subject, there will always be residual information somewhere.

So next time you get frustrated over the time it takes for the NHS' information systems to be upgraded and to become part of the "Facebook Age", consider this: it takes time to ensure security of patient information and to ensure that such information cannot be hacked. You may be happy for some of your information to be "leaked" now, but in 20 years' time, when you are standing for public office election, you may reconsider.

The NHS and other public bodies take time to make changes because they have to check the ramifications, obvious and obscure, of making those changes. It is their job to protect us from present and future embarrassment, so let's allow them the time to do it.

Meanwhile, safeguard your website from attack – you many not be the criminal but you are responsible and you may suffer a greater penalty than the perpetrator – BA did!

xtention