Bracher Rawlins
SOLICITORS

77 Kingsway London WC2B 6SR
Tel: 020 7404 9400
Fax: 020 7404 9401

DX 168 London/Chancery Lane
www.bracherrawlins.co.uk

BYOD – Are you at risk of a fine of up to £500,000?

If your employees use their own smartphone for work, YOU may be in breach of the Data Protection Act…and subject to a fine up of up to £500,000

Do you remember when all your mobile phone could do was take calls and send text messages?

Now, nearly everyone has a smartphone or tablet. Anyone, anywhere, can pick up emails, interact on social media, access the Internet, do their weekly shop, the list goes on and on.

So, it is hardly surprising that more than 50% of us are using our own devices (laptops, tablets, and smartphones) for business purposes. This practice is known as Bring Your Own Device (BYOD).

What is surprising is that some employers do not have a BYOD policy to let employees know what is, and more importantly what is not, allowed.

Employers that do not have a BYOD policy run the risk of being in breach of the Data Protection Act 1998 (the DPA). If you think that's probably not a big deal, think again. A serious breach of the DPA carries a fine of up to £500,000.

The DPA places obligations on "data controllers". To all intents and purposes this is the business or organisation that holds the data i.e. your business in relation to data you hold on your clients or staff.

Under the DPA, data controllers are required to take appropriate security measures to prevent unauthorised or unlawful processing, accidental loss of, or destruction or damage to personal data.

Guidance issued by the Information Commissioner's Office (the ICO) warns that, "it is crucial that the data controller ensures that all processing for personal data which is under his control remains in compliance with the DPA".

This is where the concern over an employee's use of his or her own devices comes in. Allowing employees to use their own devices for work purposes is most likely beneficial to the employer in terms of cost and efficiency. But, as the device is owned by the user, the employer has less control over the data that is being processed.

What would happen, for example, if a device used by one of your employees was lost, stolen or hacked? Or if an employee decided to use the data for their own private purposes?

To deal with this, employers should have a robust BYOD policy in place. By doing so, they can stay in control of the personal data for which they are responsible, regardless of who

owns the device. The policy can also ensure they do so without encroaching on the employee's rights in relation to their own data.

The policy should be updated regularly to take account of changes to technology and security software (as well as changes in the law, of course).

If you do not have a BYOD policy, your organisation is vulnerable. We recommend that you get in touch with us to put one in place as soon as possible.