QBE European Operations

Professional liability

Guidance on 'Bring your own device' (BYOD)

QBE

Guidance on 'Bring your own device' (BYOD)

The ICO has published helpful guidance explaining some of the risks organisations must consider when allowing personal devices (so-called 'bring your own device' or 'BYOD' practices) to be used to process work-related personal data and ways to help ensure compliance with the Data Protection Act 1998 in connection with BYOD policies.

The ICO admits that the cost of introducing the suggested controls may be 'quite significant' and might be greater than the initial savings expected through having a BYOD policy, but suggests that the sum will be insignificant if one considers the likely reputational damages flowing from a data breach.

Some of the key recommendations from the guidance are:

- Being clear on the types of personal data that can be processed on personal devices
- Registering personal devices with remote locate and wipe facilities so to allow the confidentiality of personal data to be maintained in the event of loss or theft
- Being clear with staff about which types of personal data may be processed on personal devices
- Using strong passwords to secure personal devices and ensuring that access to a personal device is locked or personal data automatically deleted if an incorrect password is inputted too many times
- Enabling encryption to store data on personal devices securely
- Using public cloud-based sharing and public backup services, which have not been fully assessed for security and other features, with extreme caution, if at all.

The ICO also published the results of a survey on BYOD practices. The survey, commissioned by the ICO and carried out by YouGov, suggests that 47% of UK adults now use their personal smartphone, laptop or tablet computer for work purposes, but less than 30% of these users are provided with guidance on how their personal devices should be used in this capacity. The ICO states that this raises concerns that people may not understand how to look after the personal data accessed and stored on their personal devices.

Heidi Watson from Clyde & Co's Employment team has made the following comment in relation to BYODs.

> *This ICO guidance highlights the dangers of allowing employees to use their own devices for work emails. The statistics show this is a common practice whilst many employers have not given thought to limiting the risks. Employers will need robust policies to ensure employees do not put sensitive data at risk and, where they breach the policies, to enable employers to take suitable disciplinary action. Whilst there are benefits to allowing employees the flexibility of BYODs, it is clear that employers need to give serious thought to whether their current data protection or e-communications policies provide sufficient protection against the inherent dangers.*

Further advice should be taken before relying on the contents of this summary.

Neither QBE European Operations nor Clyde & Co LLP accepts any responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary.

Clyde & Co LLP is a limited liability partnership registered in England and Wales. Authorised and regulated by the Solicitors Regulation Authority. QBE's legal and regulatory status is detailed in the small print at the bottom of this page.

Clyde & Co LLP's Professional Indemnity Team has kindly given us full permission to reproduce this document. Information is correct as at November 2013.

QBE European Operations

Plantation Place
30 Fenchurch Street
London
EC3M 3BD

tel +44 (0)20 7105 4000

www.QBEeurope.com

4649/GuidanceOnBOYD/Nov2013