LEWIS SILKIN

Ius Laboris UK Global HR Lawyers
LEWIS SILKIN

Bring your own device (BYOD)

Inside

Why BYOD?
The role of technology
Issues to consider
Solutions
Checklist

Introduction

According to a global study in 2011 by the Aberdeen group, 75% of the 415 companies surveyed allow their employees to use their own device e.g. laptops, tablets and smart phones, for business purposes. Similarly, a survey by BT in 2012 of 2,000 IT users and managers in 11 countries found that more than four out of five companies surveyed permit their employees to connect their own device to the corporate network or will do so within the next two years. This trend is commonly referred to as 'bring your own device' (BYOD).

The trend now has the attention of the Information Commissioner who has recently published guidance to promote good practice.

BYOD gives rise to a number of practical and legal issues. This Inbrief considers the main issues that employers should consider when rolling-out a BYOD scheme and sets out possible solutions and practical tips for dealing with them.

Why BYOD?

The trend to BYOD presents both risks and benefits. Benefits include:

- It's potentially cheaper; as employees invest in their own devices
- A solution to the 'two pocket problem' - enabling employees to carry one device rather than two (one for business and one for personal use)
- It improves employee engagement and productivity because employees use devices that they want and know how to use
- It enhances recruitment strategies by attracting techno savvy candidates

The risks for employers include a loss of control of the company's data which is no longer stored and transmitted using the employee's devices and networks. BYOD may have a negative impact on employee behaviour - employees may feel that their use of their own device should not be regulated by their employer. Security risks may arise where the device is shared with the employee's friends and family or left unlocked in a 'friendly' environment or the device is lost or stolen. Also, an employee's expectation of privacy in relation to information stored on his or her own device is likely to be significantly greater than information stored on a device that is owned by the employer.

These risks are not new - employers may have identified them in relation to remote workers who use, for example, their family PC for work. The risks are likely to be exacerbated as BYOD becomes more widespread.

The role of technology

Technical measures can mitigate many of the risks.

Mobile Device Management (MDM) software can allow employers to manage remotely and configure many aspects of a device. Typical security features include locking the device after a period of inactivity, executing a remote wipe of the device, location tracking features and preventing the installation of unapproved 'apps'. Employers should carefully review the features provided by MDM software and decide which should be used to address any risks identified.

Employers can also create a corporate 'sandbox' for the device. This is essentially a separate, secured container for the storage of company data. Importantly, if the employer needs to send a wipe command to the employee's device, the deletion could be limited to the company data in the sandbox. The success of this approach, however, depends on the simplicity of its use and employees correctly storing company data.

A further option is desktop virtualization software, such as Citrix. Citrix allows employees to access securely data stored on the corporate network using their own device. Provided that employees are prohibited from downloading company data to their personal device, this data will stay on a secure server. This will eliminate (or at least limit) the amount of company data stored on an employee's device. Again, it depends on the extent to which employees comply with any policies prohibiting the copying of company data onto their own device.

Issues to consider

Ownership

Employers should consider who owns the device and remind employees that all company data belongs to the employer. Under a 'classic' BYOD scheme, the employee will use their own device. The question of ownership might not be straightforward where the employer contributes to the cost of the device and/or reimburses the employee for their use of it. Ownership (of the device and content) should, therefore, be made clear in any policy.

The data protection regime

The Data Protection Act 1998 (DPA) regulates the processing of personal data. All of the obligations under the DPA fall on the "data controller" – the person who determines the purpose and way in which data is processed. "Processing" involves obtaining, holding and using data and changing or deleting it.

Employers should not assume that simply because an employee's personal device is used to conduct their business, they are the data controller of all data on the device. Such an assumption might result in the employer processing (including deleting) the employee's personal data (and data of the employee's friends and family). This may, depending on the circumstances, involve a breach of the DPA and technically would require an assessment about

the identity of the data controller in relation to each class of personal data on the device before accessing, processing or deleting it.

Monitoring

Traditionally, employers have sought to monitor their employees' use of their electronic systems in the workplace e.g. an employee's usage of the employer's telephone systems, any internet sites that the employee visits and email content and traffic. Employees may be reluctant to provide consent to their employer carrying out monitoring when they access the corporate network using their own device.

Employers should evaluate the risks faced by their business and assess whether monitoring would reduce/eliminate them.

Employers could consider requiring employees to consent to monitoring as a condition of participating in the BYOD scheme and cancelling an employee's access to the corporate network if consent is withdrawn. This will not necessarily meet the requirements of the DPA as the employee's consent may not have been freely given and can be easily withdrawn.

Security

The DPA requires data controllers to take appropriate security measures to prevent unauthorised or unlawful processing, accidental loss of or destruction or damage to personal data. This is one of the most onerous duties on data controllers under the DPA.

The Information Commissioner's Office (ICO) guidance focuses on data security. The guidance makes clear that the data controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing. The guidance recommends:

- Auditing and assessing risk - where is data held, what type of data is stored or transferred, what's the potential for data leakage, how easily might employee's blur personal and business use, what impact will cloud based services have on security, what is the risk of interception etc.
- Addressing these risks by appropriate security measures
- Understanding the security features of different devices
- Maintaining a list of approved models and keeping up to date with change
- Using technology to monitor how data is transferred to and from the device

The ICO recommends that portable devices used to store and transmit personal information should be encrypted. A failure to protect data using encryption software may lead to the ICO taking enforcement action against an employer. Also, employers may face reputational damage if personal data of their customers or clients is brought into the public domain.

Gaining access to the device

Employees may be reluctant to hand over their own device and allow their employer to review its content, particularly where the employer needs to gain access to the device to conduct an investigation into an allegation of misconduct.

Employers should consider requiring their employees to deliver up their device and password for inspection upon (periodic) request as a condition of their participation in the BYOD scheme. If the employee refuses to co-operate the employer could consider disciplining (and potentially dismissing) him or her for failing to follow a reasonable management instruction. This will not secure any company data on the device. Whether a dismissal in these circumstances would be fair would depend on the facts.

If an employer uses an employee's username and password without proper authority to access the employee's personal device, it is highly unlikely that the employer would be processing the employee's personal data 'fairly and lawfully', as required by the DPA. Furthermore, this would amount to an offence under the Computer Misuse Act 1990 (CMA). This is because, under the CMA, it is a criminal offence to gain unauthorised access to any computer or data held in any computer. There is no definition of "computer" in the CMA, which leaves the interpretation of this word potentially broad. Devices such as tablets and smart phones could, therefore, be caught.

Wiping the device

Employers may wish to wipe a device on termination of employment or if it is lost or stolen.

If the employee's personal data and company data are not separated on the device e.g. by a sandbox, all the data on the device would be wiped. If the employee has not recently backed up their personal data, the wipe could result in a significant loss of potentially irreplaceable data to the employee.

Ideally, employers should consider using software that separates company data and personal data on the device but also require employees to consent to all data on the device being deleted as a condition of their participation in the BYOD scheme. Any deletion should, from an employee relations perspective, be limited to company data where possible but policies should seek to exclude liability if the employee's data is lost. Any onerous conditions of the BYOD scheme, such as wiping the device, should be expressly brought to the attention of employees. This may manage employee expectations and reduce the risk of employees withdrawing their consent.

Tax

Where an employer provides a mobile phone device to its employees for business use, HMRC's stance is that this does not amount to a benefit in kind and, as such, is not subject to tax. Similarly, if employees seek reimbursement for business calls on their personal mobile telephone, this is not subject to tax.

HMRC have been clear, however, that devices that have telephone functionality (e.g. iPads, tablets or laptops) but which use the internet to make and receive calls are not classified as mobile phones. This is because their 'primary purpose' is not to make or receive telephone calls over a telecommunications network. As such, these types of devices may not fall within the tax exemption.

If an employer operates a BYOD scheme whereby the employee owns the mobile phone but uses it for work purposes and the employer pays the telephone company directly for the cost of using the device, this will need to be

earnings. If the employee will not be using the mobile phone solely for business purposes, tax would be payable in these circumstances.

Solutions

To manage many of the risks associated with a BYOD scheme an employer will need to consider the ICO guidance on security referred to above. In addition employers will need to:

- Create a BYOD policy and procedure to accompany the roll-out of any BYOD scheme and publish these (in a staff handbook, notice board and/or on-line). These should set clear rules of what is and what is not appropriate and the implications of any breach
- Develop awareness of the risks and issues among employees by training employees to use technology correctly
- Remind employees about their obligations in respect of company data (and other employees data)

Checklist

When rolling out any BYOD scheme, employers should consider the following:

- Identify the risks by undertaking a risk assessment
- Who owns the device and what will happen on termination
- Making participation in the scheme subject to compliance with the BYOD conditions and all of the other applicable policies and procedures
- Requiring employees to install (and not modify) a security package that protects their device and the data on it, including encryption software as a condition of participation
- How any technical measures will work in practice e.g. will employees be prohibited from downloading company data to their device?
- To what extent the employer will monitor use of the device
- Requiring the device and passwords to be delivered-up for specific inspection, upon reasonable request
- Reporting requirements if the device has been lost/stolen
- Obtaining consent to remote wipe the device in the event of loss, theft or termination of employment and clearly explaining the consequences
- A statement of the employee's obligations under the DPA to safeguard the personal data of third parties and the consequences of not doing this
- Confirming that participation in the BYOD scheme is a privilege, not a right

For further information on this subject please contact:

Alexander Milner-Smith
Partner
+44 (0) 20 7074 8196
alexander.milner-smith@lewissilkin.com

Rachel Ward
Senior Associate
+44 (0) 20 7074 8040
rachel.ward@lewissilkin.com