Bring Your Own Device—protecting data on the move

Olivia Whitcroft, Solicitor and Principal of OBEP,

examines data protection issues that arise with the growing use of 'Bring Your Own Device', and suggests ways that the challenges may be overcome

Ten years ago, employees were plotting how to convince their employers to buy them a company BlackBerry. The decade prior to that had seen the evolution of mobile phones, laptops and PDAs, which employees had gradually urged their companies to provide to them for business use. Smartphones which combined several functionalities were next on the list.

Employees have, of course, got what they wanted. In the UK, the recent ICT report from the UK's Office of National Statistics indicated that in 2011, 56% of businesses in the UK provided staff with a portable device such a laptop, smartphone or PDA.

Data protection advisers have been kept busy by the mobile revolution, advising organisations on the compliance and security risks that portable devices present, including:

- technical security measures such as encryption, access control (including passwords), backups, and restricting risky activities (including use of external USB devices or internet access); and
- organisational controls such as asset registers, training and strict policies on use.

Such policies should prohibit or restrict the use of company devices for personal matters. Using personal devices for business use has traditionally been a big 'no' for employees who work with personal or confidential information.

However, it is gradually becoming more and more difficult to keep personal and work lives separate when it comes to mobile devices and data. Workers are getting fussy, demanding even more choice and convenience. Specifically:

- employees want to choose their own device. Everyone has their personal favourites ("you like an Android and I like an iPhone; you want Windows and I want Ubuntu… let's call the whole thing off.."); and
- employees want one device for home and work. An Ofcom Communications Market Report in 2011 indicated that smartphones are being used to manage the overlap between personal and work lives. People do not want to carry two smartphones around with them, nor take company laptops home to work over the weekend when they have perfectly good laptops at home already.

And so we are faced with the challenges of Bring Your Own Device.

What is Bring Your Own Device?

'Bring your Own Device' or 'BYOD' is the term used to describe employees using personally-owned devices (such as smartphones, laptops or tablets) for business purposes. This may include making business phone calls and storing customer contact details, or (much broader) access to, and use of, business networks, documents and databases.

One concerning matter is that where an organisation has not yet considered this as an option (and therefore never explicitly addressed BYOD within policies or communications to staff), its employees are probably, to some extent, doing it anyway. This unauthorised and uncontrolled BYOD carries substantial risks of data protection and security breaches. Therefore, organisations need to (and are starting to) adapt to the BYOD world, either by permitting some level of BYOD within strict boundaries, or raising awareness and controls around the prohibition. As well as addressing the risks, organisations are also seeking to embrace potential benefits of BYOD (see below).

Data protection considerations for BYOD

Responsibility as a data controller: Responsibility for compliance with data protection rules currently lies with the 'data controller', being the party who determines the purposes for which and the manner in which personal data are processed. Therefore, where an employee's personal devices are used for business purposes, the employer will be the data controller in relation to the processing (which includes storage or use) of personal data on such device for such business purposes. This means that the employer, rather than the owner of the device, has the responsibility for ensuring that the use of the device complies with data protection law.

An underlying consequence of BYOD is that an employer will lose some control over choice and use of the employee's device. Maintaining control is of course a core part of being a data controller. With the capacity of mobile devices for data storage increasing, and their size decreasing, there is a risk that a lot of personal data are slipping out of the required control.

Security: European data protection law requires organisations to implement 'appropriate technical and organisational measures' to protect personal data against misuse, loss or damage. This security requirement is clearly a key consideration for BYOD.

In applying technical measures to business equipment, organisations have traditionally undertaken risk assessments of their chosen devices and applied standard security controls across the board (including hardware, software, network and internet access control, anti-virus measures, storage limits and backups). With personal devices, it is more difficult for an organisation to assess the risks and apply common measures across varying hardware, software and applications which employees may have selected.

From the organisational perspective, employees' personal devices are not company 'assets', so strict rules governing use may no longer be appropriate. For example, instructing employees not to take their personal laptop to the pub or away on holiday with them may not be practical. Also, employees will not be 'returning' their personal devices when they leave the organisation.

In addition, it is more difficult for organisations to monitor and enforce security controls being applied in practice, and to keep track of what devices are out there and what personal data may be held or used on them.

Fair and lawful processing: A core principle of data protection law is that personal data shall be processed 'fairly and lawfully'. In relation to the requirement to process data 'fairly', this includes consideration of what data subjects' reasonably expect to be done with their data, and whether there are unjustified adverse effects on them.

For example, do customers expect their information to be carried around on various personal smartphones whether on business or pleasure?

In relation to the second mentioned requirement — to process data 'lawfully' — an organisation will need to consider whether it is subject to any other legal requirements which may limit the devices on which data may be processed, or to which data may be transferred. For example:

- does the organisation have contractual obligations to a customer imposing data storage and transfer limitations, or other confidentiality measures?; and
- could the copying of documents to externally-owned devices be an infringement of a third party's intellectual property rights?

Specified and lawful purposes: Data protection law requires personal data to be processed only for specified and lawful purposes. If data collected for a legitimate business purpose are mixed up with other data on an employee's personal device, there is a higher risk of them being misused for an unrelated (and potentially unlawful) purpose. In addition, when an employee leaves an organisation and takes his mobile device with him, if business information is still stored on such device, it is no longer being processed for a legitimate business purpose.

Quality and retention of data: An organisation must ensure that personal data which it uses are adequate, relevant, not excessive, accurate and up to date. Further, it must not retain personal data for longer than is necessary for the purposes for which they are used.

Several potential issues related to these requirements arise with BYOD, particularly if activities are not part of, or connected to, the organisation's central systems and databases. In particular, data may be created, stored and used more informally on a personal device, and an organisation may be less aware of, or have less control over, the scope of personal data being processed. This increases the risks that:

- excessive personal data are being created and stored on the device;
- inadequate data are being transferred from the device to the organisation's central systems;
- data are not updated and amended consistently with other business databases; and
- data are not periodically reviewed and deleted when no longer required.

Access to data: One of the most prominent rights of individuals under data protection law is to access a copy of their personal data being held by an organisation by making a 'subject access request' or 'SAR'. Any personal data held or used by employees on devices on behalf of the organisation will fall within the scope of this right.

Organisations therefore need to ensure that employees' personal devices fall within the scope of searches undertaken in response to an SAR, and that they are permitted to gain access to the devices to respond to such a request. Following on from the risk of 'excessive' data being stored (see above), organisations may inadvertently find themselves obliged to disclose information which they had not intended to create or store.

On a related note, and one which goes beyond the protection of personal data alone, an organisation will want to ensure that it can access all business data stored on the device (for its own commercial needs or if investigated by a data protection or other regulator). This can be a particular risk when an employee leaves an organisation, taking the personal device with him.

Transfers of data overseas: European data protection law imposes a prohibition on transferring personal data

(Continued on page 12)

(Continued from page 11)

outside of the European Economic Area unless the country of transfer ensures an adequate level of protection for personal data.

Where employees take mobile devices away with them on business or on holiday, this would constitute a transfer of any personal data stored on such devices. The UK regulator, the Information Commissioner's Office ('ICO'), has taken the view that if an employee takes a company laptop overseas, the company's security measures applied to the laptop may (depending on the circumstances) be sufficient to ensure adequate protection. However, if an employee's personal laptop or smartphone is taken overseas (and it is more likely that such devices will be taken on holiday as well as business trips), it may not be protected by the same security measures and procedures. Further, it may be difficult to limit the data which are stored or accessed from such device.

Privacy of the owner of the device: The above data protection considerations focus on the use by an employee of his personal device for business purposes. The employee will also be using his personal device for other, non-business purposes, and has his own rights as a data subject. Therefore, in implementing measures to control use of business data, the employer must not go too far and contravene the data protection and privacy rights of the employee (for example through excessive monitoring of use, or access to data).

> ***"Whilst BYOD will not be right for everyone, in the spirit of "if you can't beat 'em, join 'em", facilitating some level of BYOD within boundaries may be more secure than unauthorised BYOD without boundaries. This can also result in increased productivity (and therefore revenues)."***

How to address the data protection risks

Risk assessment: The starting point in addressing BYOD is to carry out an assessment specific to the organisation and its activities in order to determine the following:

- taking into account both the benefits and the risks, whether the BYOD is permitted and, if so, the extent to which it is permitted;
- to the extent that the BYOD *is not* permitted, how to protect against unauthorised use of personal devices; and
- to the extent that the BYOD *is* permitted, how to address the above data protection issues (and other concerns).

If widespread BYOD is to be implemented, a more formal privacy impact assessment may be prudent (for guidance on these, see the ICO's Privacy Impact Assessment Handbook, copy available at: www.pdpjournals.com/docs/88087)

Security measures: In order to maintain some control over personal devices and the data on them, the following measures can be considered:

- identify permitted hardware and software, and carry out a separate risk assessment of each device or type of device to be used;
- include each permitted device on an asset register;
- apply or require minimum security measures for each device (such as encryption, passwords, virus protection, remote wiping, controls over applications downloaded);
- implement a system for monitoring and auditing use of personal devices;
- require business documents or information to be accessed from the device via a secure connection rather than stored on the device itself; and
- if business data may be stored on the device, implement automatic synching of data with the organisation's central systems.

Policies and awareness: Staff awareness of the risks and limitations will be critical to successful implementation of BYOD. Policies, training and other communications should address the following:

- clearly outline the extent of permitted use of personal devices and the limitations on use (for example, if personal devices are only to be used for limited purposes or types of data, or to access but not store data);
- ensure that employees understand the data protection issues and steps they can take to protect data, for example not to overstep the mark in using business information for personal reasons, taking care not to lose data, and reporting any lost/stolen devices or other security breaches;
- ensure that employees are bound to return or erase business data and software when they leave the organisation or change their device;
- let employees know the impact on their own privacy, for example that their activities may be monitored and the employer may need to audit and access their personal device; and
- outline the consequences if employees breach the rules, for example disciplinary proceedings or direct liability under the national data protection law.

To the extent that the organisation does not permit the use of personal devices for business purposes, policies and training on the risks and limitations should still be provided. This is to ensure staff understand what they should not be doing, and to enable the organisation to have recourse if the rules are breached. The organisation may still wish to maintain some rights to monitor personal devices if there is suspicion that employees are acting in breach of policy.

Benefits and next steps for BYOD

As technology and culture progress, employees demand more flexibility — this is not a new issue. Adapting to these changes, however, is not just about keeping employees happy. Despite the challenges of technology, blanket prohibitions do not always result in a more secure solution, as employees find a less secure way to get round the prohibitions.

Whilst BYOD will not be right for everyone, in the spirit of "if you can't beat 'em, join 'em", facilitating some level of BYOD within boundaries may be more secure than unauthorised BYOD without boundaries. This can also result in increased productivity (and therefore revenues).

If managed properly, BYOD can also bring additional data protection and security benefits. For example, if staff are permitted to use their home computer to securely access the company network, this avoids the need for them to carry business laptops on the train home, or to save business documents on unencrypted memory sticks to transfer to a different location. This, in turn, reduces the risk of mobile devices (and the data on them) being left on the train and accessed by unauthorised parties.

Whether permitted or prohibited, employers need to be alert to BYOD and find a solution appropriate to their needs in consideration of data protection and security concerns. Effective communication, implementation and enforcement of the solution will be key to its success.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.co.uk