Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 4 April 2013

BYOD: The Situation in the United Kingdom and Tips for Employers

By Purvis Ghani and Oliver Yaros, of Mayer Brown International LLP, London.

Bring your own device ("BYOD") is a new phenomenon taking over the workplace. Your business may have permitted limited personal use of telephones and work stations for some time, but now the reverse is becoming reality. Now individuals at all levels in companies, from the board of directors downwards, are increasingly arming themselves with a bewildering array of interconnecting smartphones, tablets and laptops, and they want to be able to use their own devices at work, for work. And given the potential reduction in information technology hardware procurement costs and the increase in general employee satisfaction and productivity this could bring, it is not surprising that many organisations are encouraging its adoption.

But aside from the danger of turning your IT support function into a small software development house to build the interfaces you need to connect your systems with them, there are a number of risks that need to be addressed before you can enable employees to bring their own devices to work. For example:

- How will you ensure that work data will not be merged with an employee's personal data?
- How do you make sure that family members who may handle the device do not access work data?
- What happens if/when the employee loses his tablet or quits his job?

Essentially, the business will remain responsible for how these devices are used for work purposes, so you need to consider how to secure your data in a way which complies with privacy and employment law.

In the United Kingdom, that will mean that you will principally need to consider how to comply with the Data Protection Act 1998, the European Convention on Human Rights, the Regulation of Investigatory Powers Act 2000 and the Telecommunications Regulations 2000.

Helpfully, the UK Information Commissioner's Office ("ICO") recently published BYOD guidance for employers on how to comply with the Data Protection Act 1998 (*see WDPR, March 2013, page 39*).

As a starting point, you should, of course, draft a BYOD policy to document how your business will implement BYOD and achieve compliance with the law.

Here are five steps that will help you prepare for implementing BYOD in your workplace:

Know Thyself

Before you can allow employees to use their own devices, you will need to establish:

- What types of data (personal data, sensitive personal data, business critical or confidential data) may be stored or accessed from these devices?
- Who has (or should have) access to which types of data (does/should the CFO have access to all types of data or just certain categories)?
- What should employees be allowed to do with data using their devices (view it from/save it to the employer's secured network, save it locally, share it with other connected devices)?

Once you have ascertained the answers to these questions, you should be in a position to start preparing a BYOD policy, which should set out in clear terms the rules by which your employees will need to abide when using their own devices for work, the criteria which will be used to assess which devices and applications can be used in connection with your systems, and the safeguards which will need to be in place to protect your data.

A BYOD policy with clear rules on the use of devices will help you deal more effectively with any employees who breach the policy. But the reverse is also true, and, without a BYOD policy, it will be harder to justify subjecting an employee to disciplinary proceedings. For example, if the employee's actions are a sufficiently serious breach of permitted use that results in dismissal, the absence of a policy setting out such rules could lead to the dismissal being found to be unfair under the Employment Rights Act 1996. A well-drafted BYOD policy can help mitigate the risk of such a claim.

Know Thy Enemy

Of course, it will not be possible for you to support every device an employee may want to use for work purposes. You will need to identify which devices and which applications you intend to allow your employees to use, and have a system in place to review this on an ongoing basis. For instance, if a security flaw is discovered in one particular version of a device's operating system, you may want to suspend access to your data from devices using that operating system until those devices have upgraded their operating systems to the next version.

You will also need to consider whether you should, and are lawfully able to, monitor employees' actions on their personal devices. Employees' use of email and internet communications can cause problems for employers if misused in such a way that results in liability or embarrassment for the employer. For example, an employee could subject a colleague to harassment and discrimination on email or social networking sites, which could result in liability for the employer if done during the course of work. Therefore, monitoring can be justified as a means of trying to limit potential liabilities.

However, monitoring is a far greater challenge when dealing with personal devices, and much will depend on how the employee is able to access the relevant data. For example, if the employee needs to access the relevant data by having to log on to your network, it will generally be easier to monitor such communications, but if an employee were to use his/her own private email to send communications, it is highly unlikely that you would be able to monitor his/her private email account.

Regardless of how the employee accesses the data, it is recommended that you comply with the employment practices code published by the ICO, which sets out guidance on monitoring. You will need to consider the extent to which any proposed monitoring would infringe on the employee's right to a private life under Article 8 of the European Convention on Human Rights and the justification for any proposed monitoring.

The rules governing interception of communications under the Regulation of Investigatory Powers Act 2000 and the Telecommunications Regulations 2000 are also more likely to be an issue when considering monitoring communications sent through personal devices. They set out the circumstances in which monitoring of certain communications can take place without consent.

However, if genuine and informed consent to monitor can be obtained from employees, then any such monitoring is more likely to be lawful under the Data Protection Act 1998, the European Convention on Human Rights, the Regulation of Investigatory Powers Act 2000 and the Telecommunications Regulations 2000.

Decide How the Data Will be Accessed

Will your employees be copying work data onto their devices, or will they be accessing data remotely from your private network or other cloud (possibly via an app)? Whichever method is chosen, it will be important to ensure that measures are in place to ensure that work materials will be properly segregated from an employee's personal files (*e.g.*, by containing or enabling access to work materials only from a specific program or application on the employee's device, and by ensuring that they are not backed up with an employee's personal files). You will also need to put measures in place to ensure that any work data that the employee has access to or stores on his device is subject to the same document retention policies that are in place in the workplace.

Decide How the Data Will be Protected

In addition to monitoring which devices and apps are safe for employees to use for work purposes, it will be very important to make sure that any upload or download of information onto the employer's system is kept secure wherever that takes place (*e.g.*, via Wi-Fi networks); that no work information can be downloaded from the employee's device onto an unauthorised USB stick or other storage device (whether it is physically connected, by Bluetooth or by remote connection); and that the employee's device and the work data on it can be accessed only by virtue of a personal identification number and/or password and that it automatically locks after a short period of inactivity (*i.e.*, so that other people who may have access to the device cannot mistakenly view and/or alter work documents).

Employees' employment contracts should contain appropriate obligations to ensure that your information is protected. First and foremost, make sure to include con-

   ISSN 1473-3579

fidentiality obligations that also cover information held on personal devices. Secondly, take particular care where employees are allowed to communicate by email on personal devices. The High Court has recently held that there is no right of ownership in an email, and so, unless it contains confidential information or copyright material, it is unlikely you would be able to retrieve these emails from the employee if sent on a personal email account. The way to deal with this is to ensure that your contracts of employment have express provisions requiring employees to make work-related emails and other communications available to the employer on request.

Decide What Will Happen if/when the Device is Lost or an Employee Leaves Your Employment

Should an employee lose his/her device or leave your employment, you will need to ensure that you have mechanisms in place which allow you to prevent the device from being used to continue to access work data. This could be achieved either by revoking the requisite passwords used to access the data and/or by remotely deleting the work data (and/or any applications used to access work data remotely) from the device. Most devices would need to be registered in advance in order to allow you to use a remote deletion tool, and you would also need to be sure that it will enable you to delete work data only and not a former employee's personal files, making proper segregation of data used on or accessed from the device vital.

If the device is lost, you may be able to identify its location using geolocation applications. However, you must be careful not to use this in ways that you have not informed your employees about or for inappropriate purposes, such as monitoring an employee's commuting habits or movements on a sick day, inadvertently monitoring an employee's relatives who might be using the device or tracking an employee's activities while he or she is on holiday.

Where an employee has been allowed to use a personal email account, the same issue relating to ownership in emails as highlighted above arises once that employee leaves your company. It is important again that the contract of employment deals with this issue by requiring employees to inform the employer what work-related material they have on their devices (or internet email accounts), along with an obligation to comply with the employer's instructions in relation to such material.

The ICO's guidance, "Bring your own device (BYOD)," is available at http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx.

The ICO's "the employment practices code" is available at http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.ashx.

Purvis Ghani is a Senior Associate in the Employment practice and Oliver Yaros is a Senior Associate in the Intellectual Property and IT group of Mayer Brown International LLP, London. They may be contacted at pghani@mayerbrown.com and oyaros@mayerbrown.com.