Data Protection Act 1998

Bring your own device (BYOD)

ico.
Information Commissioner's Office

Contents

Introduction

The Data Protection Act 1998 (the DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

This is part of a series of guidance, which goes into more detail than the Guide, to help data controllers fully understand their obligations and promote good practice.

This guidance explains to data controllers what they need to consider when permitting the use of personal devices to process personal data for which they are responsible.

Overview

- Bring your own device raises a number of data protection concerns due to the fact that the device is owned by the user rather than the data controller.
- 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.
- Protecting data in the event of loss or theft of the device will need to be considered but not to the exclusion of other risks.
- Data controllers must also remain mindful of the personal usage of such devices and technical and organisations used to protect personal data must remain proportionate to and justified by real benefits that will be delivered.

What the DPA says

The seventh principle says: appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data.

It means you must have appropriate security in place to prevent the personal data you hold from being accidently or deliberately compromised. This is relevant if personal data is being processed on devices which you may not have direct control over.

What is BYOD?

1. Consumer electronic devices such as smart phones and tablet computers have seen a huge rise in popularity, available features and capability. Many data controllers are faced with demands from employees, board members or even clients wishing to use these devices in the workplace to carry out their jobs. This might mean that individuals' own devices are used to access and store corporate information, as well as their own.

2. This trend is commonly known as 'bring your own device' or BYOD.

3. Permitting a range of devices to process personal data held by an organisation gives rise to a number of questions a data controller must answer in order to continue to comply with its data protection obligations. **It is important to remember 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.**

What are the risks?

4. The underlying feature of BYOD is that the user owns, maintains and supports the device. This means that the data controller will have significantly less control over the device than it would have over a traditional corporately owned and provided device. The security of the data is therefore a primary concern given that the data controller may have a large number and a wide range of devices to consider. The controller will need to assess:

    - what type of data is held;
    - where data may be stored;
    - how it is transferred;
    - potential for data leakage;
    - blurring of personal and business use;

- the device's security capacities;
- what to do if the person who owns the device leaves their employment; and
- how to deal with the loss, theft, failure and support of a device.

5. The Data Protection Act 1998 (DPA) requires that the data controller must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

What are the benefits?

6. An effective BYOD policy can lead to a number of benefits including improved employee job satisfaction, overall morale increase, increased job efficiency and increased flexibility. By considering the risks to data protection at the outset, a data controller has the opportunity to embed data protection at the core of its business activities and to raise overall standards, for example by specifying the types of personal data that can be stored on particular devices and which should not (say, the storage of particularly sensitive data could be denied or restricted to devices with a high level of encryption).

7. A BYOD policy and implementation plan could also lead to a better separation of data. For example, an organisation might wish to place restrictions on particular internet sites accessed via the corporate network to reduce the likelihood of data leakage or the inappropriate use of corporate communication systems. The organisation could then set-up a Wi-Fi network, separate from the corporate system, and allow employees to connect to this network with their personal devices.

What to consider?

8. The specific risks that a BYOD policy addresses will be unique to each organisation. However, considering the points set out in this guidance can help to ensure that the risks associated with BYOD are appropriately managed.

9. The starting point should be to audit the types of personal data you are processing and the devices, including their ownership, which will be used to hold it. An important question to consider is which personal data can be processed on a personal device (that

is one owned by an employee) and which must be held in a more restrictive environment. You must also consider whether employees' use of their own devices will mean that the employer ends up processing non-corporate information about the owner of the device and possibly others who use it, for example family members. Consider whether the controls you have in place are appropriate for any sensitive personal data being processed.

10. You should determine the impact a move to BYOD would have on services you share with other organisations and whether or not this would contravene any existing agreements. **BYOD must not introduce vulnerabilities into existing secure environments.**

Having a clear BYOD policy

11. It is important that users connecting their own devices to your IT systems clearly understand their responsibilities.

12. Do not forget that an important component of any policy is audit and on-going monitoring of compliance. Regular checks will ensure that the policy is being adhered to.

Top tips:

- Implement and maintain an Acceptable Use Policy to provide guidance and accountability of behaviour;
- Consider your need for a Social Media Policy if BYOD leads to an increased use of social media;
- Be clear about which types of personal data may be processed on personal devices and which may not; and
- Include all relevant departments (including IT & HR) and the end users in the development of an Acceptable Use Policy.

Where is the personal data stored?

13. Personal data being processed via a personal device might be stored in one, or a combination, of the following locations:

- On the device;
- On a server within the organisation's IT network (or other private cloud); or
- In a private, community or public cloud.

14. Regardless of where the data is stored, you will have to take appropriate measures to protect against unauthorised or

unlawful access, for example if the device is lost or stolen. This remains your responsibility as the data controller.

15. Such measures can include controlling access to the data or device using a password or PIN, or encrypting the data. You should remember that the loss or theft of the device is not the only means by which unauthorised or unlawful access may occur. For example, a device may be shared amongst family members in a way that is inappropriate if personal data for which you are the data controller is stored on it.

16. If personal data is stored in a remote location, either within the corporate network or in the public cloud, then it is important to consider the security of the access credentials in the event of loss or theft of the device. For example, if a device is used to access a cloud service and permits users to remain logged in between sessions, unauthorised access to the device could easily result in an unauthorised disclosure of personal data.

17. You should identify the type of storage media on the device. Some devices may use an easily removable memory card, such as a micro or mini SD card, meaning that a loss or theft of data may go unnoticed for some time.

18. Devices may offer additional protection through the option to sandbox or ring-fence data, for example by keeping data contained within a specific app. If this is the case, and you are relying on this as a security measure, you should consider how you will verify these features in order to ensure the confidentiality and integrity of the data. Devices may also offer the ability to restrict access to certain apps or data types based on geographic location or require an additional level of authentication.

19. Where personal data is stored on a device it will be important to consider the safe and secure deletion of the data throughout the lifecycle of the device, and particularly if the device is to be sold or transferred to a third-party.

Top tips:

- Use a strong password to secure your devices;
- Use encryption to store data on the device securely;
- Ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times;

- Ensure that the device automatically locks if inactive for a period of time;
- Make sure users know exactly which data might be automatically or remotely deleted and under which circumstances; and
- Maintain a clear separation between the personal data processed on behalf of the data controller and that processed for the device owner's own purposes, for example, by using different apps for business and personal use.

How is the data transferred?

20. BYOD arrangements generally involve the transfer of data between the personal device and the data controller's corporate system. The transfer process can present risks, particularly where it involves a large volume of sensitive information.

21. A major risk to the security of the data in transit will be a so-called 'man-in-the-middle' attack, or other types of interception carried out during the transfer process. However, you should not ignore other risks of disclosure, such as an email being sent to the wrong address.

22. Forcing all traffic through an encrypted channel such as a VPN, or HTTPS for individual services, can offer some security when using an un-trusted connection, for example an open Wi-Fi network in a coffee shop. However, if you are offering a VPN connection back through the corporate network you should be mindful of any internet monitoring software you have in operation, especially during periods of personal use. If the device sends data via non-corporate systems (for example a public email service) then there is limited opportunity to audit activity.

23. Technology exists for some platforms to monitor the data transferred for data leakage and loss. This can provide a valuable insight to the data types held on the device but also have privacy implications if monitoring during periods of personal usage.

24. Do not forget that transferring data using public cloud services such as SaaS storage, email or social networks can also leave the data at risk of interception by the cloud service provider or a foreign law enforcement authority, if that public cloud service provider is based overseas.

25. If you use removable media to transfer data (USB drives or CDs), you must also consider the safe and secure deletion of the data on the media, once the transfer is complete.

26. You may want to consider disabling some of the interfaces which might be used to connect to other devices, such as Wi-Fi or Bluetooth, as these can be used to connect to a range of external peripherals such as a printer or other storage device. You should consider any conflict this may present with your current endpoint control policy.

27. Providing guidance to employees on how to assess the security of Wi-Fi networks, such as those found in hotels and cafes, might be useful and you and your employees should be aware that some devices may automatically connect to open Wi-Fi networks as they are found by the device.

28. Some devices may offer an automated backup facility which stores a backup of data on the device to the user's cloud-based account or to the user's personal computer. As data controller, you will need to ensure that, if this facility is enabled, it will not lead to an inappropriate disclosure of personal data.

Top tips:

- Transfer of personal data via an encrypted channel will offer the maximum protection;
- Use public cloud-based sharing and public backup services, which you have not fully assessed, with **extreme caution, if at all**; and
- Take care that monitoring technology remains proportionate and not excessive, especially during periods of personal use

How will you control the device?

29. As previously mentioned, the loss or theft of the device is a major risk factor, given the relatively weak control that the organisation may have over a device that is owned by an employee. Therefore you should consider the steps you will take in advance, in order to ensure the confidentiality of any personal data stored on the device. You must also consider how you will manage personal data held on employees' personal devices should they leave your employment.

30. Most modern devices offer a facility to locate them remotely and delete data on demand, or this can be managed by third-party software - also known as Mobile Device Management. Such a service can provide some assurance that any data stored on the device could be securely deleted. However, devices often have to be pre-registered with such a service to be able to use this facility.

31. Mobile device management services may allow you to record or track the device in real time, even if the device is not reported stolen. As with monitoring technology, data controllers will need to ensure that data collected as part of a remote locate facility is only used for the specified purpose and not for on-going surveillance or monitoring of users. Users of the device should be fully informed as to how any tracking of the device takes place and any consequences of this for them.

How will you secure the device?

32. You should determine how you will ensure that vulnerabilities in the operating system or other software on the device are appropriately patched or updated. You should be aware that security updates may be dependent on the manufacturer of the device or communications provider (for example, the mobile phone operator) rather than directly from the operating system manufacturer and may not be made available immediately or at all for any particular device. **Any such vulnerability must not put personal data processed on these devices at risk**.

33. You could achieve this protection by restricting the choice of operating systems available to users. Again this could be difficult where the employer does not own the device. You should also consider how to manage employees who might 'root' or 'jailbreak' devices, a process which may remove some of the default security controls an operating system has in place.

34. You might also need to consider who is authorised to install third-party software (apps) on the device and the available source of apps which can be installed on devices. Some devices allow owners to install apps from untrusted and unverified market-places. Such untrusted sources may have a higher prevalence of malicious apps. You must also take care not to overstate the guarantees that an 'official' market-place may offer. Such outlets may only provide cursory glances at applications and fail to block all instances of malware.

35. You should decide how you might support the devices your employees bring into the workplace, and how to manage the data for which you are responsible if those devices are returned or sold by the owner. For example, if a user's device breaks and is returned to the manufacturer under a warranty can you ensure the protection of the personal data for which you are responsible?

Top tips:

- Register devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft;
- Make sure you have a process in place for quickly and effectively revoking access a device or user might have in event of a reported loss or theft;
- Limit the choice of devices to those which you have assessed as providing an appropriate level of security for the personal data being processed; and
- Provide guidance to users about the risks to downloading untrusted or unverified apps

Monitoring at work

36. The ICO has previously published guidance for employers on the topic of monitoring at work.

37. The Employment Practices Code explains that employees have legitimate expectations that they can keep their personal lives private and that they are entitled to a degree of privacy in the work environment. If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered.

38. By definition, some of the use of an employee's device will be personal in nature. At certain times of the day this is likely to increase such that all usage would be considered personal (for example evenings and weekends).

39. Technical measures which you may consider to protect the personal data for which you, as data controller are responsible, may increase the level of workplace monitoring, such as recording the geo-location of devices or monitoring of internet traffic.

40. You should also be clear as to whether or not you may be monitoring the device usage of other individuals who may not be employees such as family members.

Top tips:

- When drafting a BYOD Acceptable Use Policy, consider the guidance in the ICO's Employment Practices Code;

- Before undertaking monitoring, identify clearly the purpose(s) behind the monitoring and the specific benefits it is likely to bring; and
- Ensure that workers are clear about the purpose of any monitoring and satisfied that it is justified by real benefits that will be delivered.

Other data protection risks?

41. Whilst the security of the device may be the primary concern, a BYOD policy should facilitate compliance with all aspects of the DPA.

42. Usage of BYOD could raise the risk that personal data is processed for a purpose different from that for which it was originally collected. You must ensure that users of devices know their responsibilities in terms of only using corporate personal data for corporate purposes.

43. If copies of data are stored on many different devices, say as an attachment in an email, there is an increased risk that personal data will become out-of-date or inaccurate over time. There is also an increased risk that it will be retained for longer than is necessary, due to the fact that it is more difficult to keep track of all copies of the data. Using devices to connect to a single central repository of data can help mitigate this risk.

44. There is also a risk of data leakage in that data could be accidentally lost or disclosed without the user's (and therefore your) knowledge. For example, a copy and paste action may retain data on the clipboard which is mistakenly posted to a social networking site or an accidental forward of an email to all individuals in the address book.

45. Furthermore, if multiple copies of data are stored on many different devices, you may find that it is more difficult to respond to the rights of the data subject. For example, how can you guarantee that you will comply with a subject access request if you are not aware of all the devices on which personal data may be stored?

Other risks?

46. Public authorities subject to the Freedom of Information Act (FOIA) will also need to consider their obligations in this area. If

multiple copies of data are stored across many different devices, you may find that it is more difficult to respond to requests for information, especially within the required time schedule. Remember that a public authority's corporate information is still subject to FOIA even if held on a personally owned device.

47. Your organisation may be subject to other legislation and/or regulatory requirements so you must ensure that these are taken into account with your BYOD policy.

Summary

48. BYOD raises a number of data protection concerns due to the fact that the device is owned by the user rather than the data controller. However, it is crucial that as data controller you ensure that all processing for personal data which is under your control remains in compliance with the DPA. Particularly in the event of a security breach, you must be able to demonstrate that you have secured, controlled or deleted all personal data on a particular device.

Further information

You can find out more about encryption from the following URL:

⇒http://www.ico.gov.uk/news/current_topics/Our_approach_to_encryption.aspx

You can find out more about asset disposal from the following URL:

⇒http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/it_disposal.aspx

You can find out more about cloud computing from the following URL:

⇒http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/cloud_computing.aspx

You can find out more about how to ensure your employees' personal details are respected and properly protected at work from the following URL:

⇒http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx