PCPD
H K
PCPD.org.hk
Information Leaflet
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Bring Your Own Device (BYOD)

Executive Summary

Bring your own device ("**BYOD**") is an organisational policy that allows employees to use their own mobile devices to access the organisation's information, including personal data collected by the organisation. For the purpose of this leaflet, personal data collected by an organisation is referred to as "organisation-collected personal data".

Organisations should bear in mind the following issues related to personal data privacy:

1 In allowing BYOD, an organisation is effectively transferring organisation-collected personal data from a secured corporate system to an employee's less secure device, over which the organisation has far less effective control. It is important to realise that even though the personal data is stored on a device owned by the employee, the organisation remains fully responsible for compliance with the Personal Data (Privacy) Ordinance (the "**Ordinance**") in respect of this personal data. Organisation should therefore establish administrative, physical and technical measures to ensure that such personal data is protected and reinforce these measures through written policies, notifications and training.

2 While protecting personal data transferred or collected by BYOD equipment, an organisation is reminded that such BYOD equipment also contains private information about employees, their family members and other individuals. Any protective measures implemented by the organisation should also respect such private information.

3 In order to fulfil their obligations under the Ordinance, organisations should consider:

- (a) whether there is sufficient reminder to employees not to misuse organisation-collected personal data downloaded to or stored in BYOD equipment;
- (b) whether sufficient technical measures are in place to enable BYOD equipment for accessing or storing organisation-collected personal data while respecting private information, for example:
  - (i) Any alternatives to storing the organisation-collected personal data directly in the BYOD equipment – can data be stored in corporate system and is only accessed via (instead of stored in) the BYOD equipment?
  - (ii) Any effective control system for accessing personal data – family members and others having access to the BYOD equipment would not be able to access organisation's personal data if the employee's username and password are required to access such data; and
  - (iii) Any security measures, including independent encryption, that should be applied in order to protect the organisation-collected personal data accessed via or stored in the BYOD equipment, so that those having unauthorised access to the BYOD equipment will only gain access to encrypted personal data.

4 As a best practice, an organisation planning to allow BYOD should also consider:

- (a) establishing a BYOD policy describing its governance (e.g., roles and responsibilities of the organisation and the employees; approval procedure for deployment, etc.);
- (b) conducting a risk assessment (e.g., to determine how the BYOD policy and practice can be implemented);
- (c) applying technical solutions to reduce or contain the risks; and
- (d) devising a monitoring and review mechanism to ascertain compliance to the BYOD policy while keeping up with any business changes.

Introduction

BYOD is a practice that is becoming increasingly popular in organisations. When employees use their own mobile devices such as smartphones and tablets to access and work with their employer's organisational information, such information is effectively transferred from a secured corporate system to an employee's less-secure device. This leaflet highlights the personal data privacy risks that an organisation needs to be aware of when it develops a BYOD policy. It also suggests best practices in allowing employees to use BYOD equipment to access and work with the corporate system that contains personal data.

Given the various features of BYOD equipment, different types of organisation's information involved, as well as the rapid development in information and communication technologies, the issues and measures identified in this leaflet may not be universally applicable, and readers therefore need to consider their applicability to the ways they use a particular type of BYOD equipment.

As this leaflet focuses mainly on personal data privacy protection, readers should refer to other relevant technical or industry guidance on more detailed IT security aspects when deploying a particular BYOD.

BYOD and the Ordinance

Apart from the specific risks and controls highlighted in this leaflet, an organisation deploying BYOD that stores or processes personal data should also familiarise itself with the six Data Protection Principles[1] ("**DPPs**") and other requirements under the Ordinance.

While an organisation might have devised general policy on the protection of personal data privacy as required under the Ordinance and its six DPPs, the transfer of personal data to and its retention by BYOD equipment pose specific privacy risks to such data. An example is the risk to the security of the data when it is transferred from a secured corporate system to BYOD equipment. It is important to note that even though the personal data is stored on a device owned by the employee, the organisation remains fully responsible for compliance with the Ordinance in respect of that personal data. If an organisation wishes to remotely manage an employee's BYOD equipment or track its location in case it is lost, there is a "reverse" flow of the employee's private information stored in the BYOD equipment back to the organisation's system. This also poses personal data privacy risks to the employee, and the organisation is fully responsible for compliance with the Ordinance in respect of that data also.

Broadly speaking, BYOD practice may impact the following aspects of the DPPs:

(a) The retention and erasure of data (DPP2)

An organisation needs to ascertain if personal data should be retained in BYOD equipment and, if so, whether and how its organisation's retention and erasure policy can be applied equally and effectively to the personal data so retained, e.g., by simply extending such policy to cover the data in the BYOD equipment.

(b) The control of the transfer of personal data and its subsequent use (DPP3)

An organisation should establish sufficient controls as to how the organisation-collected personal data is to be accessed and used by its employees. Policies on the use of data should be applicable equally to an organisation's equipment and to an individual's BYOD equipment. When organisation-collected personal data is allowed to be transferred to, and/or retained in the BYOD equipment, the organisation may have less control over how the data is accessed or used by its employees, compared with the data being stored centrally. The organisation may therefore need to provide reminders to its employees and devise policies and controls (where appropriate) to ensure that such personal data cannot be used for a new purpose by its employees without obtaining consent from the data subjects concerned.

(c) The protection of personal data when being transferred to and later retained in BYOD equipment (DPP4)

An organisation's protection policy for the security of its collected personal data should be equally applicable to the data transferred to and retained in its BYOD equipment.

Given that BYOD equipment may be inherently

[1] See www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html for details.

insecure[2] by design or by the ways it is used, the use of BYOD equipment without additional safeguards may not satisfy the security requirements under DPP4.

However, a conflict may arise if corporate security measures are implemented to BYOD equipment without due regard to the employee's concerns about his own personal data privacy. For example, in order to protect the personal data in BYOD equipment, an organisation may wish to remotely access BYOD equipment to track its location or to ensure that there has been no installation of unauthorised applications ("**apps**"). Such arrangements, however, may infringe the personal data privacy of the employee because the organisation may then have access to the employee's private information stored in the BYOD equipment.

Therefore, to guard against the risks of BYOD equipment that is lost or compromised[3], organisation should employ security measures to protect personal data stored in the BYOD equipment, instead of using tools that are commonly available for protecting organisation-own mobile equipment, such as Mobile Device Management. In practical terms, this means a combination of the following techniques:

1. To prevent organisation-collected personal data from being stored in BYOD equipment;
2. To control access to such personal data that is stored in BYOD equipment (for example, using dedicated username and password in addition to screen locks); and
3. To encrypt such personal data that is stored in BYOD equipment using encryption method that is not built-in the BYOD equipment and which is appropriate to the sensitivity of the personal data.

These techniques are elaborated upon in the "Best Practices" section of this leaflet.

(d) Data access and correction rights in respect of data retained in BYOD equipment (DPP6)

Irrespective of whether personal data is retained by an organisation in its central corporate system or in its BYOD equipment, the rights of an individual to access and correct his personal data remain the same. An organisation, therefore, needs to ensure that its obligations in respect of the access to and correction of personal data can still be discharged, particularly in the cases where personal data may be retained only in BYOD equipment. Measures to back up the organisation's data stored in BYOD equipment to a storage controlled by the organisation should therefore be considered.

Best Practices

The following practices should be considered by an organisation to ensure its use of BYOD complies with personal data protection requirements.

(a) Establishing a BYOD policy

An organisation must establish a BYOD policy detailing:

1. Respective roles, obligations and responsibilities of the organisation and its employees in a BYOD practice;
2. Criteria by which an organisation decides the information and apps accessible by BYOD equipment; and criteria that determine what kind of BYOD equipment may be allowed, such as the types of equipment, operating systems and other technical standards;
3. Technical solutions applied in the protection of personal data belonging to the organisation and that belonging to its employees, e.g., disallowing personal data accessible via BYOD equipment to be saved in the equipment, or if such data is stored in the BYOD equipment, it must be isolated from other apps (e.g. through "sandboxing" technique) or encrypted; and
4. Mechanisms by which an organisation may monitor the compliance of the BYOD policy and practice, and the consequence of non-compliance.

(b) Conducting a risk assessment

A risk assessment should be conducted to ascertain the types of personal data to be accessible by, or stored in, the BYOD equipment, and the harm and likelihood of its loss or unauthorised disclosure. Based on the result of

[2] Many smartphones are not built with security in mind. Even if they are, they may be jailbroken by their owners thus disabling protection.

[3] Compromised equipment includes smartphones that have been jailbroken or device that are infected with malicious software.

such risk assessment and the technical capability of an organisation, the organisation should then review, and decide on the types of personal data to be accessible by a particular type of BYOD equipment and develop proportionate access controls and security measures to protect the data.

Given that an employee's equipment may contain considerable personal data relating to himself, his family and others, any access to, monitoring or erasure of such employee's personal data in the BYOD equipment without justification or the employee's knowledge could create friction in its staff relations. The risk assessment therefore must address the personal data privacy implications in respect of both the organisation's data (including the organisation-collected personal data) and the employee's personal data.

If an organisation lacks the technical ability to properly assess the risks or take measures to ensure adequate protection of the personal data in its BYOD practice, it should seek outside assistance. The organisation must, however, bear in mind that while a contractor may be responsible for providing the design and procedures in protecting personal data in a BYOD practice, the organisation will be accountable and liable for any privacy breach committed or caused by the contractor[4]. The organisation therefore must ensure its specified security requirements are fulfilled by its contractor. Readers may refer to the information leaflet entitled *Outsourcing the Processing of Personal Data to Data Processors*[5] for more information.

(c) Applying technical solutions

Control software or apps may be used in BYOD equipment to protect personal data transferred to it and to enhance the security of the equipment. They may be used to remotely wipe or lock BYOD equipment, or to track its physical location and to detect whether it has been 'jailbroken' or infected with malware, or even to track websites visited. It is also possible, for example, to implement measures to lock access or automatically delete data if incorrect passwords are entered a certain number of times in succession. As these protective measures involve the surrendering of certain control of the BYOD equipment to the organisation, an employee may be concerned of being monitored both during and outside of working hours and exposing his own personal data. An organisation should communicate very clearly to its employees their respective rights and obligations in the personal data protection policy of the BYOD practice before adopting the above protective measures[6]. Alternatively, an organisation may consider, where appropriate, allowing these measures to be controlled by its employees themselves. For example, an employee could be equipped with his own account to locate, wipe or find his own BYOD equipment. In allowing this approach, however, organisations must be cognisant of the fact that employees may as a result be in a position to control the erasure of data stored in the BYOD equipment. Appropriate back-up measures should therefore be considered.

The following technical features may protect both the security of an organisation's personal data and its employee's personal data privacy. Given the technical nature of these features, an organisation may need to seek advice from IT professionals as to whether and, if so, how such features may be implemented:

1. An independent and additional layer of password protection or access control, in addition to the BYOD equipment's default screen locks, should be imposed on the organisation-collected personal data stored in the equipment. Dedicated passwords, two-factor authentication, time-out after inactivity and other enhanced security controls guard against access to the data by its employee's family members or others, who may share the use of or have access to the BYOD equipment. Furthermore, it may be necessary to install software to enforce complex passwords that can be used by employees or issue guidelines for employees to use only complex passwords;

2. Organisation-collected personal data stored in the BYOD equipment should be properly encrypted by mechanisms other than by the one offered by the equipment itself, so that in the event of data loss,

---

4 Under section 65(2) of the Ordinance, any act done or practice engaged in by a person as agent for another person with the authority of that other person shall be treated as done or engaged in by that person as well as by him.

5 Available at www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/dataprocessors_e.pdf

6 Organisations should refer to the "Privacy Guidelines: Monitoring and Personal Privacy at Work" for more details in relation to electronic monitoring of employees, available at: www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf

or if the equipment is compromised, it is harder for those who have access to the data to make use of the data;

3. The transmission of organisation-collected personal data to and from the BYOD equipment should be properly authenticated and encrypted so that it cannot be intercepted by an unauthorised party, e.g., when a BYOD equipment is connected to an unsafe Wi-Fi network that may redirect communication to a fraudulent server; and

4. Auto-erasure of the organisation-collected personal data stored in BYOD equipment may be implemented as a precautionary measure when warranted by the sensitivity of the personal data and the necessary arrangement that a copy of the data is available. For example, when a BYOD equipment is lost and has no connection to the organisation's servers for a pre-defined period, or when there are repeated attempts to log-in to the equipment, auto-erasure may proactively prevent possible subsequent data loss.

(d) Monitoring and review

As the threats to and vulnerabilities of information and communications technology equipment emerge, an organisation that allows BYOD must regularly review and update its policy and measures, and monitor their compliance. It should fine-tune and revise its protection policy and measures in the light of technological advancement or business change. Changes to the nature and/or sensitivity of personal data being stored in BYOD equipment should also be regularly evaluated and corresponding changes made to the policy.

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

First published in August 2016