World Data Protection Report™

September 27, 2016

Hong Kong

Bring Home the Data? New Hong Kong Data Privacy Guidelines for BYOD Policies



By Gabriela Kennedy and Karen H.F. Lee

Gabriela Kennedy is a partner at Mayer Brown JSM in Hong Kong. She can be reached at gabriela.kennedy@mayerbrownjsm.com.

Karen H.F. Lee, is a senior associate at Mayer Brown JSM in Hong Kong. She can be reached at karen.hf.lee@mayerbrownjsm.com.

On Aug. 31, the Hong Kong Privacy Commissioner (PC) issued a new Information Leaflet to highlight the personal data privacy risks that employers need to address when developing a Bring-Your-Own-Device (BYOD) practice. This new Information Leaflet has been issued against the backdrop of increasing cybersecurity concerns, particularly in the financial industry.

Cybersecurity Risks

BYOD practices are not new. They are now almost common place, to the point where they are now taken for granted. It is at such times that risks are overlooked in the rush to “be like everyone else” and have a BYOD practice in place. BYOD practices introduce new vulnerabilities to a company's cybersecurity. As BYOD policies allow employees to use their own personal devices (e.g. tablets, laptops, smart phones, etc) for employment related activities, companies have less control on how their employees access and use personal data belonging to the company (e.g. customer data). Unlike organisation-owned devices, personal devices are generally more vulnerable to cyberattacks or to accidental data leaks.

It is no surprise that the financial industry, which has been the most active with regard to cybersecurity, has also taken the lead in relation to BYOD practices, due to the sensitive nature of personal data handled by banks and the significant consequences that may be suffered if data is stolen, lost or misused. Since at least 2014, the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC) have been actively requiring financial institutions to step up their risk management and cybersecurity measures. In October 2014, the HKMA issued a revised Circular on Customer Data Protection, which removed restrictions on BYOD policies for financial institutions, but required them to comply with the Recommended Standards of Bring Your Own Devices for Work by Bank Staff in Hong Kong issued by the Hong Kong Association of Banks. In parallel, on Oct. 6, 2014, the PC also issued a Guidance Note on the Proper Handling of Customers' Personal Data for the

Banking Industry. Gabriela Kennedy, Sara Or and Karen Lee, Banking On Your Personal Data: Recent Guidance Issued to Banks, Mayer Brown JSM (Dec. 23, 2014).

One of the more recent developments in the financial industry was HKMA's announcement on May 18 of the launch of a new cybersecurity fortification initiative (CFI). The CFI aims to enhance the cybersecurity of Hong Kong's financial industry through:

(a) the introduction of a cybersecurity risk assessment framework;

(b) making appropriate training available to ensure a steady supply of qualified cybersecurity professionals; and

(c) setting up a cybersecurity intelligence platform for financial institutions to share information to enhance collaboration.

Protecting Personal Data

On Aug. 31, the PC issued the Information Leaflet to try and help companies continue to comply with the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO), as BYOD practices are becoming increasingly widespread across all industries.

Although companies may already have in place general policies on data protection with which their employees are required to comply, BYOD practices present their own risks and introduce new concerns which need to be specifically addressed through individual policies. Companies need to protect both personal data accessed and used by its employees on their devices (e.g. customer data), and also employees' personal data transmitted from their device back to their employer.

Retention of Personal Data

Companies must assess whether or not to allow their employees to save personal data on their personal devices, and how their internal retention and erasure policies need to be amended to deal with such situations. Under the PDPO, data users must take all practical steps to ensure that personal data held by them is not retained for longer than necessary in order to fulfil the original purpose (or a directly related purpose) of collection. A company may be in breach of the PDPO if their employees continue to maintain customers' personal data on their device, beyond the relevant retention period.

In practice, it will be difficult for an employer to be certain that all business related information is no longer retained by a former employee (e.g. stored on their personal devices). Whilst employer's internal policies may make it a requirement that employees erase or return all work-related data stored on their personal devices, verifying and enforcing this in practice may be more difficult.

We would recommend that companies:

(a) prohibit and implement technical measures to prevent employees from saving any work-related data (including personal data) on their personal device, and requiring all documents and data to be saved on the company's secure system, which can be remotely accessed by the employee via their device;

(b) alternatively, implement technical measures that enable the company to remotely delete all company data stored on the employee-owned device, without affecting any of the employees' other personal data or documents (this will require any company data to be segregated and stored

in one area of the device); and

(c) require employees to sign an undertaking to delete all data stored on their personal device once it is no longer needed for the relevant work-related purpose and once their employment comes to an end.

Transfer and Use of Personal Data

Companies must establish controls on how personal data collected by them can be accessed, used and transferred by their employees – both on company-owned equipment and on employees' personal devices. Companies should implement policies and send regular reminders to prevent their employees from using such data in breach of the PDPO, by clearly stating how the data can be used, to whom it can be transferred, etc.

Security Measures

Personal devices are inevitably less secure then company-owned equipment. Companies generally spend time and money on implementing robust systems and safeguarding measures to prevent cyberattacks and misuse of data. In comparison, personal smartphones or tablets are relatively vulnerable to attacks or viruses. Companies must ensure that their employees' personal devices have in place additional safeguards to protect them.

However, the implementation of security measures on an employee's device must be balanced against the employee's own right to privacy, and the usual measures that a company might employ in respect of company-owned devices may not be appropriate for employee-owned equipment. For example, implementing tracking software on an employee-owned device or having the ability to remotely access the device are unlikely to be appropriate and may infringe the employee's data privacy rights. Therefore, some of the safeguarding measures proposed by the PC include less intrusive methods, e.g. preventing company-owned data from being stored locally on the employee's devices, using dedicated usernames, passwords and screen locks, and encrypting the personal data stored on the device, which must be commensurate to the sensitivity of the data. Another alternative would be to implement technical solutions to segregate company-owned data from other information in the employee-owned device, which can then be wiped remotely without affecting any other data of the employee.

Data Access and Correction Requests

A company's obligation to comply with data access and data correction requests of data subjects under the PDPO, applies equally to any personal data of such data subjects that are stored by the company's employees on their personal devices. Therefore, companies must have an internal procedure in place to enable them to comply with such requests, e.g. making sure that all company-owned data is backed up on a system controlled by the company, and not only saved on an employee's device.

Best Practices

Under the Information Leaflet, the PC recommends that companies establish a BYOD policy, conduct a risk assessment and apply technical solutions to protect personal data. Companies must also carry out regular reviews to assess compliance with their current internal policies and check for new threats and vulnerabilities, and update their policies and measures accordingly.

Before implementing a BYOD policy, companies should carry out a risk assessment to determine the types of personal data that can be accessed or stored on an employee's device, and the potential harm and likelihood of unauthorised loss or disclosure. The risk assessment should also take into account the privacy implications on the amount of personal data of the employee (or their friends and family), which can be accessed on their device. Based on the results of its risk assessment, a company should then develop its BYOD policy and determine what technical solutions be implemented.

The BYOD policy must set out the specific roles and responsibilities of the company and its employees, and the criteria by which a company determines what can be accessed via the employee-owned device and the type of device allowed. The BYOD policy must also specify the technical methods utilised to protect the personal data owned by the company and its employees' personal data, and how the company monitors compliance with the policy and what are the consequences for non-compliance.

The technical solutions implemented by a company to protect company-owned data, must be balanced against the employees' right to privacy. Some of the PC's recommended security measures include implementing an independent and additional password protection and access control, on top of the employee-owned device's current security setting (i.e. requiring complex passwords and double authentication, and automatic time-out following inactivity, etc); additional encryption of company-owned personal data stored on, or transmitted to and from, the employee-owned device; and automatic deletion of sensitive company-owned personal data stored on the employee-owned device in certain circumstances (e.g. repeated input of incorrect passwords, etc).

Conclusion

Does the adoption of a BYOD practice bring benefits that outweigh the data privacy and cybersecurity risks it introduces? Do your internal policies and practices sufficiently take into account and minimise the risks presented by your BYOD practice? Do your internal policies sufficiently protect the employees' right to privacy in respect of their personal devices?

A balance needs to be struck between protecting the personal data collected by a company and respecting the privacy of their employees' own personal data. Whilst security measures need to be robust, they cannot be so intrusive as to infringe the employees' own right to privacy or result in a potential unfair or excessive collection of employees' personal data stored on their device. A detailed risk assessment should be carried out, and a BYOD policy implemented to address the specific concerns presented by BYODs. Such assessments and internal policies cannot be static. In light of the fast-paced changes in technology, companies must carry out regular reviews of their internal policies and security measures to stave off any vulnerabilities that could result in cyberattacks or accidental loss or disclosure by employees.

General Information

Date Filed	Tue Sep 27 00:00:00 EDT 2016
Citation	DK:BNA A0K1B2P5K8
Topic(s)	Technology Law; Communications & Media; Privacy & Information Law