KPMG
cutting through complexity

# HKMA's Customer Data Protection Requirements – 2014 Updates

## KEY REGULATORY UPDATES

### Customer Data Protection

On 14 October 2014, the Hong Kong Monetary Authority (HKMA) issued a new circular, *Customer Data Protection*, which sets out the new requirements relating to the handling of customer data. In particular, it outlines clear requirements around the transmission of customer data via internet services and corporate emails. Additionally, it references the new control standards issued by the Hong Kong Association of Banks (HKAB) regarding the use of staff-owned smartphones. The circular can be downloaded from the HKMA website (http://www.hkma.gov.hk).

Banks are notified of this new requirement and a hard deadline to assess compliance with the circular has been set for Q1 2015.

## TAKING A CLOSER LOOK

Since the introduction of the *Customer Data Protection* circular in July 2008, the regulatory requirements for the protection of customer data have remained largely unchanged. The new circular issued in October 2014 introduces a number of new requirements in relation to customer data protection. It is essential for banks to be aware of the following key updates in the circular, including the requirement to:

- Comply with a standard of minimum controls issued by the HKAB in terms of the standards for 'bring your own device'[1]
- Automatically detect the unauthorised transfer of customer data through corporate emails on a real-time basis
- Identify the locations of customer data in the bank's network (e.g. file server or staff laptops) and implement logical access controls to prevent unauthorised access
- Identify premises or service providers that have access to a large amount of sensitive customer data and implement specific data protection controls
- Have an independent party perform regular audits to ensure the adequacy of customer data protection controls and compliance with the circular

### Quick Compliance Check

Have you considered the following?

- **Data is classified** according to sensitivity levels with commensurate data protection controls.
- **An annual staff awareness programme** has been implemented for all staff regarding customer data protection.
- **Use of staff-owned mobile devices** is compliant with the recomended standards issued by the HKAB.
- **Data leakage protection (DLP) tools** are deployed to automatically detect the leakage of customer data via corporate emails on a real-time basis.
- **Controls are in place** to detect the unauthorised downloading of customer data to portable storage media.

[1] The HKAB issued the 'Recommended Standards of BYOD for Work by Bank Staff' on 13 October 2014. The standards supplement the HKMA *Customer Data Protection* circular regarding the control requirements for personally owned computing devices.

# IMPACT ON EXISTING PRACTICES

| | Existing Practices | New Practices |
|---|---|---|
| Mobile Devices | • Staff cannot use their own devices such as smartphones or home PCs for work purposes. This limits the potential of a mobile workforce that is commonly adopted in many other industries. | • Mobile workforce and home connectivity via personal devices can be explored if there are appropriate policies in place which are compliant with the stipulated requirements. |
| Use of Emails | • Basic keyword filtering control to detect the leakage of sensitive information. Generally, the approach is more relaxed and only focuses on keywords such as 'confidential'. | • Rigorous requirements are defined for real-time detection of customer data leakage, including email attachments and compressed files (e.g. zip files) on a real-time basis. |
| Customer Data on Servers | • There are standard logical access controls (e.g. usernames & passwords) for applications and databases. | • A complete picture of all locations of customer data in the bank's network must be mapped out, and access controls should be implemented according to sensitivity levels (i.e. risk-based controls). |
| Customer Data Processing Centres | • Standard physical access controls such as access cards and surveillance cameras are used. | • Stringent physical controls, such as having a paper-free working environment, prohibit printing and photocopying, and staff activities monitoring is now stipulated. |
| Audits & Assessments | • Assessments are performed by the IT team and there are ad hoc internal audits on data leakage protection controls. | • Periodic audits performed by an independent party on the adequacy of customer data protection controls are now required. |

# HOW CAN KPMG HELP?

As stipulated in the *Customer Data Protection* circular, banks are now required to complete a critical review of the adequacy of existing data protection controls by the end of Q1 2015 and implement new controls where required. KPMG can help you navigate through the complex regulatory requirements by identifying gaps where immediate focus will be required. The KPMG approach to data protection focuses on People, Process and Technology. KPMG can help filter your complex requirements, build them into your everyday operational processes, conduct user awareness training and implement the technical tools required to enable these controls.

# CONTACT US

For inquiries related to this update, please contact us:

**Henry Shek**
Partner, Advisory
KPMG China
**T:** +852 2143 8799
**E:** henry.shek@kpmg.com

**Kelvin Leung**
Senior Manager, Advisory
KPMG China
**T:** +852 2847 5052
**E:** kk.leung@kpmg.com

**Alvin Li**
Senior Manager, Advisory
KPMG China
**T:** +852 2978 8233
**E:** alvin.li@kpmg.com

**Sidney Kwong**
Manager, Advisory
KPMG China
**T:** +852 2847 5177
**E:** sidney.kwong@kpmg.com