KPMG

cutting through complexity

PCPD Guidance Note 2014 – Proper Handling of Customers' Personal Data for the Banking Industry

December 2014

Guidance to the banking industry

In October 2014, the Office of the Privacy Commissioner for Personal Data (PCPD) released the new *Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry ("the Guidance Note")*. According to the PCPD, the banking industry has long been among the top three private sector organisations against which complaints are made, and the number of complaints keeps growing. The new Guidance Note is no doubt an effort to reiterate to banks the importance of complying with the relevant data protection requirements under the Personal Data (Privacy) Ordinance.

Apart from reiterating the data protection principles, the Guidance Note also provides renewed insights for a number of common banking operation initiatives (please see the 'Key data privacy concerns' on the right). With the continued regulatory focus on the proper handling of customer data, it is time for banks to revisit their existing information governance and data management processes to ensure robust controls throughout the entire data life cycle.

KEY DATA PRIVACY CONCERNS

1. Intra-group sharing of data

The intra-group sharing of data refers to the practice of sharing customer data with entities in the same banking group such as the head office of the bank. According to the Guidance Note, banks are advised to inform the customers regarding such sharing of data in the Personal Information Collection Statement (PICS). It is also important that the use of such data by the intra-group entities is restricted to the purpose directly related to the original collection purpose. The banks should also have a monitoring mechanism in place to track the whereabouts of the shared data and keep proper logs to record the movement of the data.

2. Transfer of data outside Hong Kong

In the event of any transfer of personal data outside Hong Kong, the banks should take note of the data protection requirements on (1) data subject notification; (2) accuracy of the transferred data; (3) not changing the original purpose of data collection; and (4) proper data protection and disposal. Additionally, banks should take note of section 33 of the Privacy Ordinance regarding the allowable conditions for the transfer of personal data outside Hong Kong – although not currently in force, it may be implemented in the near future.

PCPD Guidance Notes 2014 – Proper Handling of Customers' Personal Data for the Banking Industry

3. Protection of personal data collected off-site

For personal data collected off premises (e.g. off-site marketing events), banks should establish clear policies and practical measures to ensure the secure handling of customer data collected off-site. Some examples of practical measures include encrypting portable storage devices (e.g. USB drives and laptops), logging of customer data received, using locked containers for hard copy documents and transmitting data safely to the bank's premises.

4. Data handling in an e-banking environment

Banks with internet banking channels should take note of the *Internet Guidance Note* issued by the PCPD in April 2014 regarding the detail principles for collecting, displaying and transmitting personal data through the internet. In addition to the *Internet Guidance Note*, the PCPD has specifically set out in the new banking Guidance Note requirements regarding (1) the display of PICS on the e-banking website; (2) information stored in cookies; and (3) the security of data transmission through the internet.

5. Handling of data access request

Banks should be aware of the *Data Access Request (DAR) Guidance Note* for processing DAR from customers. In general, banks are required by section 19(1) of the Privacy Ordinance to comply with customers' DAR within 40 calendar days. The DAR request can include customers' documents such as signed contracts, written records of communications, risk profiles and records of investment objectives. Banks should have the relevant DAR compliance processes in place to ensure prompt compliance with customers' data access requests.

How Can KPMG Help?

KPMG can help your organisation to assess compliance with the PCPD requirements and advise leading practices to assist you in formulating a robust strategy for the handling of customers' personal data. Examples of leading practices include:

- Holistic information governance
- Proper data handling awareness
- Customer information asset management
- Data life cycle strategy
- Data protection strategy

For more information regarding the emerging regulatory requirements, please contact one of our Information Protection and Business Resilience team leaders.

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