Given the private nature of banking services and as banks serve the vast majority of the public, the banking industry is one of the private sectors in Hong Kong for which the Hong Kong Privacy Commissioner receives most complaints. For the same reasons, data privacy compliance by the banking industry attracts particular attention, not only from the regulatory authorities, but also from the public. Due to the sensitive nature of the information handled by the banking industry, the consequences of personal data being mishandled, lost, leaked or stolen can be very serious. The risk is heightened by the increased threat of cyber crime. In October 2014, both the Privacy Commissioner and the Hong Kong Monetary Authority (“HKMA”) issued guidelines to banks on how to protect personal data. This article focuses on the handling of customer data by banks.

The Privacy Commissioner’s Guidance Note

On 6 October 2014, the Privacy Commissioner issued a Guidance Note on the Proper Handling of Customers’ Personal Data for the Banking Industry (“PC Guidance Note”). The PC Guidance Note provides the banking industry with tailored advice on how to ensure compliance with the Personal Data (Privacy) Ordinance (“PDPO”). This advice addresses the following aspects:

PERSONAL INFORMATION COLLECTION STATEMENTS

On or before the collection of a customer’s personal data, a bank is required to notify the customer of certain information in accordance with the PDPO. It is recommended that such notice be provided in the form of a personal information collection statement (“PICS”), which can be provided in the application form used to collect the customer’s personal data, or attached to the form as a separate notice. The PICS must specify:

a. the purposes for which the customer’s personal data may be used;
b. the classes of persons to whom the customer’s personal data may be transferred;
c. whether or not it is mandatory or optional for the data requested to be provided, and the consequences for failing to provide it;
d. the customer’s right to access and correct his personal data held by the bank, and the name, job title and address of the bank officer who is responsible for handling data access or correction requests.

Banks are advised to communicate effectively the PICS to its customers. The PICS should be in clear and simple language easily readable and understandable, and should also be easily accessible. Banks should therefore take into account the language used and the layout and presentation of the PICS (e.g., simple English or Chinese, reasonable font size, headings to facilitate reading, etc). Banks should ensure that the PICS is presented to customers in a conspicuous manner. They should also consider providing the customers with a help desk or enquiry hotline to assist them in understanding the PICS.

If personal data is collected from a customer over the phone or electronic means, the bank is still required to comply with the PICS requirement. The bank will have to keep good records of having communicated the PICS to a customer before or at the time of collecting his personal data.

HONG KONG IDENTITY CARDS (“HKID”)

Banks are required by law and HKMA regulatory guidelines to perform KYC and AML due diligence on customers and potential customers. Banks are therefore allowed by the PDPO to collect their HKID numbers. However, a bank may not collect HKID number from a non-customer, unless otherwise required by law.
For example, a bank is required by the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO") to collect the HKID number of a non-account holder when carrying out an "occasional transaction" for them. Examples of an occasional transaction include money changing of an aggregate value of at least HK$120,000, or wire transfer of an aggregate value of at least HK$8,000.

CUSTOMER RECORDS

Banks should take all reasonably practicable steps to ensure that a customer's contact details are accurate and up-to-date, to ensure that bank statements and other correspondence are not sent to the wrong person. Banks should put in place automated or manual checking procedures to ensure that all information (and variations) provided by the customer from time to time has been correctly entered onto the bank's records.

RETAINING CUSTOMERS PERSONAL DATA

Under the PDPO, a customer’s personal data must not be kept for longer than is necessary. As such, banks should implement clear data retention policy to ensure that personal data is erased after the purposes for which it was collected have been fulfilled. When determining the period of retention, banks should take into account the purposes for which the personal data is to be used and any applicable regulatory or legal requirements on record-retention periods (e.g., Banking Ordinance, AMLO, Securities and Futures Ordinance, Companies Ordinance, Inland Revenue Ordinance, etc.).

Exceptions may also be made where a longer retention period is justified. Examples include where it is necessary to retain the data as it relates to a current or impending legal action or complaint, or is needed to facilitate performance of a contractual obligation.

As regards retention of a customer's bankruptcy data, the Privacy Commissioner advises banks to retain for no longer than 8 years. The rationale for the 8-year period is that a bankrupt individual would normally be discharged between 4 to 8 years from the commencement of bankruptcy, and so it is not necessary for a bank to retain bankruptcy data for longer than 8 years.

SHARING CUSTOMERS' PERSONAL DATA WITHIN THE SAME BANKING GROUP

Banks should not allow unrestricted sharing of their customers’ personal data amongst group entities. Intra-group sharing of customer data has to comply with the PDPO. The PICS should inform a customer of the intra-group sharing, and the sharing of data should not be excessive having regard to the purposes for which data is collected and used and other relevant circumstances. In any other case, a bank is not permitted to share customer data within the group unless with the customer’s express consent or unless the bank may rely on a specific exemption in the PDPO.

A bank should establish a group policy on the sharing of customer data. It should also keep up-to-date logs on the transfer of customer data within the group.

TRANSFERRING CUSTOMERS' PERSONAL DATA OUTSIDE HONG KONG

All requirements in the PDPO regulating transfer of personal data apply to a bank transferring customer data, whether within Hong Kong or to a place outside of Hong Kong. In addition, the Privacy Commissioner has been considering an effective date for section 33 of the PDPO. In the meantime, the Privacy Commissioner advises banks to take into account the requirements of section 33 in communicating to customers their practices and arrangements relating to transfer of data if they intend to transfer data outside of Hong Kong.

DISCLOSING CUSTOMERS' PERSONAL DATA TO FINANCIAL REGULATORS AND LAW ENFORCEMENT AGENCIES

Even if requested by a governmental agency or regulatory authority to disclose customer's personal data, a bank should exercise caution and should not make indiscriminate disclosure. Banks should not assume that disclosure requests from governmental agencies or regulatory authorities are automatically and invariably mandatory and binding on banks. Before accommodating a disclosure request, a bank should duly assess the request and determine whether the bank may rely on a legal ground for making disclosure. Typical legal grounds include:

a. disclosure is directly related to the original purposes for which the customer data was collected;
b. the customer has given express consent for disclosure; or

c. the disclosure is permitted by virtue of a specific exemption in the PDPO, including where the disclosure is required or authorised by law or a court order binding on the bank, or is required in relation to any legal proceedings in Hong Kong.

**USING CUSTOMERS’ PERSONAL DATA IN DEBT COLLECTION**

Banks should specify in the PICS that debt collection agents is one of the classes of persons to whom they may transfer customers’ personal data. In the absence of that, a bank will have to obtain a customer’s express consent before transferring his data to debt collection agents. It is also good practice for a bank to make readily available to a customer of its debt collection policies and practices.

A bank will remain responsible for contravention of the PDPO by its debt collection agents. As such, banks should impose back-to-back contractual obligations on debt collection agents that are consistent with the PDPO and other obligations on the bank. In addition, a bank should not disclose excessive customer data to debt collection agencies.

The same requirements apply with respect to other service providers and data processors appointed by the bank. A bank is required to adopt contractual or other means to manage its service providers and data processors. The PC Guidance Note expressly states that a simple provision requiring a service provider or data processor to comply with the PDPO or the laws of Hong Kong will not exonerate the banks from liability under the PDPO.

**PROTECTING CUSTOMERS’ PERSONAL DATA DURING OFF-SITE MARKETING CAMPAIGNS**

Where banks organise off-site marketing activities to promote their products, this will likely involve the collection of personal data. A bank should implement clear policies and procedures to ensure secure handling of personal data by its marketing staff. The policies and procedures should, among other things, require the staff to keep any forms or documents containing customer data securely stored in a locked container and securely transported to the bank’s premises, and prohibit the staff from bringing them home.

**COLLECTING AND PROTECTING CUSTOMERS’ PERSONAL DATA IN E-BANKING SITUATIONS**

The PC Guidance Note contains advice specifically applicable to e-banking services offered by banks. Particular attention is drawn to the following aspects:

a. when a customer logs onto a bank’s e-banking platform to apply for the e-banking services and provide his personal data on-line, he should be given the PICS before his personal data is collected – the PICS can be given online either on the same webpage or through a prominent link;

b. any online form should follow the paper equivalent, and any mandatory items or optional items to be completed should be clearly labelled;

c. where cookies are used, it is good practice to disclose the bank’s policy regarding cookies, including what kind of information is stored on the cookies and whether a customer may opt out of the cookies and the consequences of opting out; and

d. it is good practice to inform customers of the specific security measures applicable to online transmission of their personal data.

**HANDLING DATA ACCESS REQUESTS**

Individuals are entitled to request access to any of their personal data held by the bank. If the bank receives data access request, it is required to respond within 40 calendar days by providing the requested data or notifying the individual that it does not hold his personal data. The bank is allowed to charge a reasonable fee for complying with the data access request, restricting to the direct costs incurred by the bank in complying with the data access request.

**MAKE PRIVACY POLICIES AND PRACTICES GENERALLY AVAILABLE**

Banks must take all reasonable practicable steps to ensure that their privacy polices and practices, are accessible by the general public. A banks may post a statement of such policies and practices on its website and include a link on its homepage or other pages where personal data is collected. Such link should be clearly marked, e.g., “Privacy Policy Statement”. It is recommended that the privacy policy
statement include information such as the kinds of personal data the bank holds, the main purposes for which the data is used, the bank’s data retention policy, its data disclosure and transfer policies, etc.

Consequences of breaching the PDPO

Whilst breach of the PC Guidance Note will not in itself constitute an offence, the Privacy Commissioner will take it into account and is likely to weigh unfavourably against the bank in a case or complaint brought before the Privacy Commissioner alleging a contravention of the PDPO.

When the PDPO was amended in 2012, several changes relating to enforcement notice were introduced. More important changes include increased penalties for breaching multiple enforcement notices or for repeated contravention of the PDPO on the same facts after an enforcement notice has been issued and complied with. Further, the Privacy Commissioner is empowered to issue an enforcement notice whether or not the breach is actually continuing or whether or not he is of the opinion that the breach is likely to continue or be repeated (which was a pre-requisite before the PDPO was amended).

The HKMA Circular

On 14 October 2014, the HKMA issued a Circular on Customer Data Protection (“HKMA Circular”). The HKMA Circular focuses on the controls to prevent and detect loss or leakage of customer data and procedures for addressing and reporting such incidents.

The HKMA expects all authorised institutions to complete a critical review of the adequacy and effectiveness of their existing controls and procedures by the first quarter of 2015. In conducting the review, an AI should have regard to the guidance provided in the HKMA Circular and other applicable guidance issued by the HKMA. If the review reveals weakness or areas for improvements, the HKMA expects an AI to implement appropriate measures promptly to strengthen the controls.

Major aspects addressed by the HKMA Circular include the following:

a. appoint a designated senior officer or committee to oversee the protection of customer data, and the handling and reporting of any loss or leakage of customer data;

b. classify customer data according to its sensitivity and risk level, and put in place security controls based on the assessed risk levels;

c. have in place policies and procedures covering system controls, physical security controls, mobile computing, etc.;

d. implement an awareness programme to remind staff members at least annually of:
   » the importance of complying with the AI’s data security policies and procedures;
   » their obligation to promptly report any data leak or loss of data; and
   » the disciplinary actions that may be taken against staff members for violation of the internal security policies and procedures, or failure to report a data leak or loss;

e. have in place access controls to prevent any unauthorised access of customer data, including restricting access to designated staff members on a need-to-know basis; disabling and preventing the use of tools to download massive amounts of data, unless management approval has been obtained, etc;

f. have in place controls over the transmission of customer data to external networks and systems, including implementing strong data encryption, preventing access to Internet services that can store data (e.g., external email accounts, cloud service) or file-sharing software, and having controls to detect suspicious activities, such as any massive downloading of data;

g. control the ability of staff members to store customer data on portable storage devices, including:
   » restricting or preventing the use of portable storage devices;
   » deploy password protect and data encrypt portable storage device and backup tapes;
   » record the use of portable storage devices;
   » record the reporting of any loss of a portable storage device;
   » erase data from the portable storage device when no longer needed;

h. ensure the secure disposal or destruction of customer data stored on paper or any other media;
i. control the use of personally owned computer devices by staff members in relation to their employment (i.e., “Bring Your Own Device” policy):
   » staff members should generally only use devices provided by and owned by the AI;
   » however, if an AI has a “Bring Your Own Device” policy, it should comply with the Hong Kong Association of Banks’ standards on minimum controls;

j. implement physical security controls where customer data is stored, and whenever customer data is being relocated or transported, including security guards, CCTV, etc;

k. engage independent third parties to conduct periodic audits on the adequacy of and compliance with the AI’s controls over customer data;

l. have in place controls over the handling of customer data by third party service providers, including imposing contractual obligations on them to comply with the AI’s policies and procedures; and

m. report any loss or leakage of customer data to the HKMA, the relevant customers and the Privacy Commissioner where appropriate. The HKMA expects an AI to provide justification for a decision not to report.

Banks should complete the critical review by Q1 2015 in accordance with the HKMA Circular and take necessary and timely steps in light of the results of the review.

Conclusion

Banks are under increased scrutiny from the Privacy Commissioner and HKMA, as well as the general public. There is also heightened expectation for banks to treat data protection as an integral part of their overall compliance infrastructure.

The potential consequences of non-compliance include investigations, fines, civil claims and reputational damage. It is therefore very important for a bank to design and implement an effective data protection compliance policy that addresses all legal and regulatory requirements from various sources that are applicable to it having regard to the nature and scale of business, and its circumstances and needs. For a bank that is part of an international group, the compliance policy will have to address not only requirements under Hong Kong law but also foreign laws and group policies. Apart from management commitment and oversight, a key component of the compliance policy is staff awareness and training.

Whilst cyber security and employee data handling are beyond the scope of this article, we have designated teams and experts to provide advice on those topics. Please contact us if you require further assistance.
Contact Us

For inquiries related to this Legal Update, please contact the following persons or your usual contacts at our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Sara Or
Partner
T: +852 2843 2268
E: sara.or@mayerbrownjsm.com

Karen Lee
Associate
T: +852 2843 4452
E: karen.hf.lee@mayerbrownjsm.com

Mayer Brown JSM is part of Mayer Brown, a global legal services organisation, advising many of the world's largest companies, including a significant portion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. Our legal services include banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

OFFICE LOCATIONS
AMERICAS: Charlotte, Chicago, Houston, Los Angeles, New York, Palo Alto, Washington DC
ASIA: Bangkok, Beijing, Hanoi, Ho Chi Minh City, Hong Kong, Shanghai, Singapore

Please visit www.mayerbrownjsm.com for comprehensive contact information for all our offices.

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is intended to provide a general guide to the subject matter and is not intended to provide legal advice or be a substitute for specific advice concerning individual situations. Readers should seek legal advice before taking any action with respect to the matters discussed herein. Please also read the Mayer Brown JSM legal publications Disclaimer. A list of the partners of Mayer Brown JSM may be inspected on our website www.mayerbrownjsm.com or provided to you on request.

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"), The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown JSM, a Hong Kong partnership; and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated; Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.