Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

1.1. *Banking on your personal data: recent guidance issued to banks*

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.

1.1.1. *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:

1.1.1.1. *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;

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong. Tel.: +852 2843 2211.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.
URL: http://www.mayerbrown.com

http://dx.doi.org/10.1016/j.clsr.2015.01.010

(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 their 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.

*1.1.1.2. 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$8000.

1.1.1.3. 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.

1.1.1.4. 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.

1.1.1.5. 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.

1.1.1.6. 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.

1.1.1.7. Disclosing customers' personal data to financial regulators and law enforcement agencies. Even if requested by a governmental agency or regulatory authority to disclose a 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) the 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