The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 11

HONG KONG

Yuet Ming Tham[1]

I OVERVIEW

The Hong Kong legal framework concerning privacy, data protection and cybersecurity is consolidated under one piece of legislation, the Personal Data (Privacy) Ordinance (PDPO). All organisations that collect, hold, process or use personal data (data users) must comply with the PDPO, and in particular the six data protection principles (DPPs) in Schedule 1 of the PDPO, which are the foundation upon which the PDPO is based. The Office of the Privacy Commissioner for Personal Data (PCPD), an independent statutory body, was established to oversee the enforcement of the PDPO.

This chapter discusses the recent data privacy developments, including new legislation and guidelines, and major enforcement actions in Hong Kong from September 2015 to August 2016. It will also discuss the current data privacy regulatory framework in Hong Kong, and in particular the six DPPs and their implications for organisations, as well as specific data privacy issues such as direct marketing, issues relating to technological innovation, international data transfer, cybersecurity and data breaches.

II THE YEAR IN REVIEW

i Proposed legislation and administrative measures

On 9 October 2015, the PCPD published Guidance on Data Breach Handling and the Giving of Breach Notifications to assist data users in handling data breaches, and in mitigating the loss and damage caused to the data subjects concerned, particularly when sensitive personal

1 Yuet Ming Tham is a partner at Sidley Austin.

data is involved. It replaces the previous Guidance on Data Breach Handling and the Giving of Breach Notifications issued in June 2010, and places renewed focus on the relationship between data users and data processors.[2]

In October 2015, the PCPD also published a revised version of the Best Practice Guide for Mobile App Development. This provides a comprehensive guide for professionals in the mobile application business on specific risk areas in personal data privacy.[3]

On 1 December 2015, the PCPD published a guidance note on Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting Children. This came after a local study on websites and mobile applications targeting children highlighted several aspects in which local websites and apps were lagging behind their global counterparts. The guidance note aims to provide practical suggestions and good practices for these websites and mobile apps for the protection of personal data of children.[4]

In April 2016, the PCPD published a Revised Code of Practice on Human Resource Management. This is aimed at providing practical guidance to employers and their staff on the proper handling of personal data relating to several phases of the employment process. While the Code of Practice is not legally binding, a failure to abide by the mandatory provisions under the Code would weigh unfavourably against the data user in any case that comes before the Privacy Commissioner for Personal Data. Similarly, any court, magistrate or the Administrative Appeals Board is entitled to take into account any such failure in deciding if a data user has breached the PDPO.[5]

Again in April 2016, the PCPD published a revised Code of Practice on the Identity Card Number and other Personal Identifiers, which outlines appropriate principles in handling HKID card numbers and personal identifiers such as passport numbers. Similar to the Guidance on Property Management Practices, this Code is not legally binding, and failures to abide by the mandatory provisions would give rise to presumptions against the data user in legal proceedings concerning the PDPO.[6]

Again in April 2016, the PCPD published revised Privacy Guidelines: Monitoring and Personal Data Privacy at Work, which aim to provide employers with guidance on proper measures to be taken in assessing whether employee monitoring is appropriate for their businesses, along with guidance on how employers may develop privacy-compliant practices in the management of personal data obtained from employee monitoring.[7]

On 26 June 2016, the PCPD published Guidance on the Proper Handling of Customers' Personal Data for the Beauty Industry. This was released in response to complaints to the PCPD filed against beauty and fitness companies relating to their direct marketing

2 www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf.

3 www.pcpd.org.hk//english/resources_centre/publications/files/Best_Practice_Guide_for_Mobile_App_Development_20151103.pdf.

4 www.pcpd.org.hk//english/resources_centre/publications/files/guidance_children_e.pdf.

5 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf

6 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/picode_en.pdf.

7 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf.

practices and their transfer of customers' personal data to third parties without consent. This guidance includes practical guidelines, such as direct marketing tips and data security tips for the beauty industry, on compliance with the requirements under the PDPO.[8]

In June 2016, the PCPD also published a guidance note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users. A data subject's right to make a data access request is vested under Section 18 of the PDPO, and it enables an individual to be informed of whether a data user holds his or her personal data, while also allowing an individual to obtain a copy of this personal data from a data user.[9]

In August 2016, the PCPD published revised Guidance on Property Management Practices, which is aimed at providing guidance to property management bodies in handling common personal data issues such as the issuance of resident cards, recoding of personal data of visitors and the use of CCTV surveillance within property premises.[10]

ii Data privacy complaints

A total of 1,690 complaints were received by the PCPD in 2014–2015, a 10 per cent decrease from the previous year. Although there has been an increase in the number of complaints in relation to the use of information and communications technology (ICT), the number of direct marketing-related complaints dropped as the public and organisations have become more familiar with the requirements under the new direct marketing regime.

The record-high 223 ICT-related complaints in 2014–2015 represented an 89 per cent year-on-year increase. Of these, 98 related specifically to use of social networks, 79 were about use of smartphone applications, 66 concerned disclosure or leakage of personal data on the internet, 34 involved cyberbullying and 11 related to other subtopics. The Privacy Commissioner sees the rising trend as principally attributable to the increasing popularity of smartphones and the internet.[11]

iii Enforcement actions

On 9 September 2015, the PCPD published a media statement on the conviction of Hong Kong Broadband Network Limited, a telecommunications service provider, for the failure to comply with the requirement from a data subject to cease to use his personal data in direct marketing. This was in contravention of Section 25G9(3) of the PDPO, and the service provider was fined HK$30,000. This was the first conviction since the penalty level of the offence was raised under the new direct marketing regulatory regime, which came into operation on 1 April 2013 under the PDPO.[12]

On 14 September 2015, the PCPD released a media statement on Links International Relocation Limited, a storage service provider. Links International was fined HK$10,000 for the offence of using the personal data of a customer in direct marketing without taking

8 www.pcpd.org.hk//english/resources_centre/publications/files/BeautyIndustry_ENG.pdf.

9 www.pcpd.org.hk//english/resources_centre/publications/files/DAR_e.pdf.

10 www.pcpd.org.hk//english/resources_centre/publications/files/property_e.pdf.

11 www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport15_03.pdf. (Note that the 2015–16 PCPD Annual Report has yet to be published.)

12 www.pcpd.org.hk/english/news_events/media_statements/press_20150909.html.

specified actions under Section 35C of the PDPO. This was the second conviction under the direct marketing regulatory regime following that of Hong Kong Broadband Network Limited.[13]

On 3 November 2015, the PCPD also released a media statement regarding the conviction of Hong Kong Professional Health Group Limited under Section 35G(3) for the failure to comply with the requirement from its client to cease to use his personal data in direct marketing. The company was fined a total of HK$10,000. The PCPD has revealed that it received 1,005 complaints from 1 April 2013 to 31 October 2015, with 538 (54 per cent) of complaints concerning the failure of companies to comply with customers' opt-out requests.[14]

On 23 December 2015, the PCPD released a report announcing that it has commenced an investigation into the security vulnerability of the SanrioTown website. The website is operated by Sanrio Digital (HK) Limited, which made an announcement that the personal data of 3.3 million of its users could be accessed publicly owing to a security vulnerability. This included names, e-mail addresses, dates of birth and encrypted passwords.[15]

On 30 December 2015, the PCPD released a media statement regarding the conviction of an individual for the offence of providing personal data to a third party for use in direct marketing without consent and without taking the specified actions under Section 35J of the PDPO. He was fined HK$5,000. This was the first conviction of the new offence under Section 35J of the PDPO.[16] Another individual was charged under Section 35C, but was acquitted on the facts of the case.

On 16 May 2105, the PCPD published a media statement on GMS (Asia Pacific) Limited, a marketing company, being fined a total of HK$16,000 for two charges relating to the use of personal data in direct marketing without consent under Section 35C of the PDPO, and the failure to comply with an opt-out request under Section 35G of the PDPO.[17]

iv Increasing public awareness

In January 2015, the PCPD launched a privacy awareness campaign with the theme 'Developing Mobile Apps: Privacy Matters'. The former Privacy Commissioner for Personal Data, Mr Allan Chiang, mentioned during the campaign inauguration ceremony that it is the PCPD's aim to embrace the next wave of ICT advancements, so as to enhance economic and social development. However, Mr Chiang also emphasised that consumer privacy and data security remain PCPD's priority.[18]

On 31 July 2015, the PCPD also released a revised information leaflet entitled 'Protect Privacy by Smart Use of Smartphones' to help smartphone users minimise the personal data privacy risks associated with the use of smartphones.[19]

13 www.pcpd.org.hk/english/news_events/media_statements/press_20150914.html.
14 www.pcpd.org.hk/english/news_events/media_statements/press_20151103.html.
15 www.pcpd.org.hk/english/news_events/media_statements/press_20151223.html.
16 www.pcpd.org.hk/english/news_events/media_statements/press_20151230.html.
17 www.pcpd.org.hk/english/news_events/media_statements/press_20160516.html.
18 www.pcpd.org.hk/english/news_events/media_statements/press_20150108.html.
19 www.pcpd.org.hk/english/news_events/media_statements/press_20150731.html.

III REGULATORY FRAMEWORK

i The PDPO and the six DPPs

The PDPO entered into force on 20 December 1996, and it was recently amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance). The majority of the provisions of the Amendment Ordinance entered into force on 1 October 2012, and the provisions relating to direct marketing and legal assistance entered into force on 1 April 2013.

The PCPD has issued various codes of practice and guidelines to provide organisations with practical guidance to comply with the provisions of the PDPO. Although the codes of practice and guidelines are only issued as examples of best practice and organisations are not obliged to follow them, in deciding whether an organisation is in breach of the PDPO, the Privacy Commissioner will take into account various factors, including whether the organisation has complied with the codes of practice and guidelines published by the PCPD. In particular, failure to abide by certain mandatory provisions of the codes of practice will weigh unfavourably against the organisation concerned in any case that comes before the Privacy Commissioner. In addition, a court is entitled to take that fact into account when deciding whether there has been a contravention of the PDPO.

As mentioned above, the six DPPs of the PDPO set out the basic requirements with which data users must comply in the handling of personal data. Most of the enforcement notices served by the PCPD relate to contraventions of the six DPPs. Although a contravention of the DPPs does not constitute an offence, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

DPP1 – purpose and manner of collection of personal data

Principle

DPP1 provides that personal data shall only be collected if it is necessary for a lawful purpose directly related to the function or activity of the data user. Further, the data collected must be adequate but not excessive in relation to that purpose.

Data users are required to take all practicable steps to ensure that on or before the collection of the data subjects' personal data (or on or before first use of the data in respect of item (d) below), the data subjects were informed of the following matters:

a the purpose of collection;

b the classes of transferees of the data;

c whether it is obligatory to provide the data, and if so, the consequences of failing to supply the data; and

d the right to request access to and request the correction of the data, and the contact details of the individual who is to handle such requests.

Implications for organisations

A personal information collection statement (PICS) (or its equivalent) is a statement given by a data user for the purpose of complying with the above notification requirements. It is crucial that organisations provide a PICS to their customers before collecting their personal data. On 29 July 2013, the PCPD published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PICS. It is recommended that the statement in the PICS explaining

what the purpose of the collection is should not be too vague and too wide in scope, and the language and presentation of the PICS should be user-friendly. Further, if there is more than one form for collection of personal data each serving a different purpose, the PICS used for each form should be tailored to the particular purpose.

DPP2 – accuracy and duration of retention

Principle

Under DPP2, data users must ensure that the personal data that they hold are accurate and up-to-date, and are not kept longer than necessary for the fulfilment of the purpose.

After the Amendment Ordinance came into force, it is provided under DPP2 that if a data user engages a data processor, whether within or outside Hong Kong, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than necessary for processing the data. 'Data processor' is defined to mean a person who processes personal data on behalf of a data user and does not process the data for its own purposes.

It should be noted that under Section 26 of the PDPO, a data user must take all practicable steps to erase personal data held when the data are no longer required for the purpose for which they were used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased. Contravention of this Section is an offence, and offenders are liable for a fine.

Implications for organisations

The PCPD published the Guidance on Personal Data Erasure and Anonymisation (revised in April 2014), which provides advice on when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and physical destruction. For example, it is recommended that dedicated software, such as that conforming to industry standards (e.g., US Department of Defense deletion standards), be used to permanently delete data on various types of storage devices. Organisations are also advised to adopt a top-down approach in respect of data destruction, and this requires the development of organisation-wide policies, guidelines and procedures. Apart from data destruction, the guidance note also provides that the data can be anonymised to the extent that it is no longer practicable to identify an individual directly or indirectly. In such cases, the data would no longer be considered as 'personal data' under the PDPO. Nevertheless, it is recommended that data users must still conduct a regular review to confirm whether the anonymised data can be re-identified and to take appropriate actions to protect the personal data.

DPP3 – use of personal data

Principle

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. 'Prescribed consent' means express consent given voluntarily and that has not been withdrawn by notice in writing.

Implications for organisations

Organisations should only use, process or transfer their customers' personal data in accordance with the purpose and scope set out in their PICS. If the proposed use is likely to fall outside the customers' reasonable expectation, organisations should obtain express consent from their customers before using their personal data for a new purpose.

DPP4 – Data security requirements

Principle

DPP4 provides that data users must use all practicable steps to ensure that personal data held are protected against unauthorised or accidental processing, erasure, loss or use.

After the Amendment Ordinance came into force, it is provided under DPP4 that if a data user engages a data processor (such as a third-party IT provider to process personal data of employees or customers), whether within or outside Hong Kong, the data users must adopt contractual or other protections to ensure the security of the data. This is important, because under Section 65(2) of the PDPO, the data user is liable for any act done or practice engaged in by its data processor.

Implications for organisations

In view of the increased use of third-party data centres and the growth of IT outsourcing, the PCPD issued an information leaflet entitled 'Outsourcing the Processing of Personal Data to Data Processors' in September 2012. According to the information leaflet, it is recommended that data users incorporate contractual clauses in their service contracts with data processors to impose obligations on them to protect the personal data transferred to them. Other protection measures include selecting reputable data processors, and conducting audits or inspections of the data processors.

The PCPD also issued the Guidance on the Use of Portable Storage Devices (revised in July 2014), which helps organisations to manage the security risks associated with the use of portable storage devices. Portable storage devices include USB flash cards, tablets or notebook computers, mobile phones, smartphones, portable hard drives and DVDs. Given that large amounts of personal data can be quickly and easily copied to such devices, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policies and practice. The guidance note recommended that a risk assessment be carried out to guide the development of an organisation-wide policy to manage the risk associated with the use of portable storage devices. Further, given the rapid development of technology, it is recommended that this policy be updated and audited regularly. Some technical controls recommended by the guidance note include encryption of the personal data stored on the personal storage devices, and adopting systems that detect and block the saving of sensitive information to external storage devices.

DPP5 – privacy policies

Principle

DPP5 provides that data users must publicly disclose the kind of personal data held by them, the main purposes for holding the data, and their policies and practices on how they handle the data.

Implications for organisations

A privacy policy statement (PPS) (or its equivalent) is a general statement about a data user's privacy policies for the purpose of complying with DPP5. Although the PDPO is silent on the format and presentation of a PPS, it is good practice for organisations to have a written policy to effectively communicate their data management policy and practice. The PCPD published a guidance note entitled Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their

PPS. In particular, it is recommended that the PPS should be in a user-friendly language and presentation. Further, if the PPS is complex and lengthy, the data user may consider using proper headings and adopting a layered approach in presentation.

DPP6 – data access and correction

Principle

Under DPP6, a data subject is entitled to ascertain whether a data user holds any of his or her personal data, and to request a copy of the personal data. The data subject is also entitled to request the correction of his or her personal data if the data is inaccurate.

Data users are required to respond to a data access or correction request within a statutory period of 40 days. If the data user does not hold the requested data, it must still inform the requestor that it does not hold the data within 40 days.

Given that a substantial number of disputes under the PDPO relate to data access requests, the PCPD published a guidance note entitled Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users, dated June 2012, to address the relevant issues relating to requests for data access. For example, although a data user may impose a fee for complying with a data access request, a data user is only allowed to charge the requestor for the costs that are 'directly related to and necessary for' complying with a data access request. It is recommended that a data user should provide a written explanation of the calculation of the fee to the requestor if the fee is substantial. Further, a data user should not charge a data subject for its costs in seeking legal advice in relation to the compliance with the data access request.

ii Direct marketing

New direct marketing provisions under the PDPO

The new direct marketing provisions under the Amendment Ordinance entered into effect on 1 April 2013, and introduced a stricter regime that regulates the collection and use of personal data for sale and for direct marketing purposes.

Under the new direct marketing provisions, data users must obtain the data subjects' express consent before they use or transfer the data subjects' personal data for direct marketing purposes. Organisations must provide a response channel (e.g., e-mail, online facility or a specific address to collect written responses) to the data subject through which the data subjects may communicate their consent to the intended use. Transfer of personal data to another party (including the organisation's subsidiaries or affiliates) for direct marketing purposes, whether for gain or not, will require express written consent from the data subjects.

New Guidance on Direct Marketing

The PCPD published the New Guidance on Direct Marketing in January 2013 to assist businesses to comply with the requirements of the new direct marketing provisions of the PDPO.

Direct marketing to corporations

Under the New Guidance on Direct Marketing, the Privacy Commissioner stated that in clear-cut cases where the personal data are collected from individuals in their business or employee capacities, and the product or service is clearly meant for the exclusive use of the corporation, the Commissioner will take the view that it would not be appropriate to enforce the direct marketing provisions.

The Privacy Commissioner will consider the following factors in determining whether the direct marketing provisions will be enforced:

a the circumstances under which the personal data are collected: for example, whether the personal data concerned are collected in the individual's business or personal capacity;

b the nature of the products or services: namely, whether they are for use of the corporation or for personal use; and

c whether the marketing effort is targeted at the business or the individual.

Amount of personal data collected

While the Privacy Commissioner has expressed that the name and contact information of a customer should be sufficient for the purpose of direct marketing, it is provided in the New Guidance on Direct Marketing that additional personal data may be collected for direct marketing purposes (e.g., customer profiling and segmentation) if the customer elects to supply the data on a voluntary basis. Accordingly, if an organisation intends to collect additional personal data from its customers for direct marketing purposes, it must inform its customers that the supply of any other personal data to allow it to carry out specific purposes, such as customer profiling and segmentation, is entirely voluntary, and obtain written consent from its customers for such use.

Penalties for non-compliance

Non-compliance with the direct marketing provisions of the PDPO is an offence, and the highest penalties are a fine of HK$1 million and imprisonment for five years. At the time of writing, the PCPD has not published any cases relating to contravention of the new direct marketing provisions, and it remains to be seen how the new direct marketing provisions will be enforced by the PCPD.

Spam messages

Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the Unsolicited Electronic Messages Ordinance (UEMO). Under the UEMO, businesses must not send commercial electronic messages to any telephone or fax number registered in the do-not-call registers. This includes text messages sent via SMS, pre-recorded phone messages, faxes and e-mails. Contravention of the UEMO may result in fines ranging from HK$100,000 to HK$1 million and up to five years' imprisonment.

In early 2014, the Office of the Communications Authority prosecuted a travel agency for sending commercial facsimile messages to telephone numbers registered in the do-not-call registers. This is the first prosecution since the UEMO came into force in 2007. The case was heard before a magistrate's court, but the defendant was not convicted because of a lack of evidence.

Person-to-person telemarketing calls

Although the Privacy Commissioner has previously proposed to set up a territory-wide do-not-call register on person-to-person telemarketing calls, this has not been pursued by

the government in the recent amendment of the PDPO.[20] Nevertheless, under the new direct marketing provisions of the PDPO, organisations must ensure that they do not use the personal data of customers or potential customers to make telemarketing calls without their consent. Organisations should also check that the names of the customers who have opted out from the telemarketing calls are not retained in their call lists.

On 5 August 2014, the Privacy Commissioner issued a media brief to urge the government administration to amend the UEMO to expand the do-not-call registers to include person-to-person calls. In support of the amendment, the Privacy Commissioner conducted a public opinion survey, which revealed that there had been a growing incidence of person-to-person calls, with more people responding negatively to the calls and fewer people reporting any gains from the calls. Although there had been long-standing discussions regarding the regulation of person-to-person calls in the past, it remains to be seen whether any changes will be made to the legislation.

iii Technological innovation and privacy law

Cookies, online tracking and behavioural advertising

While there are no specific requirements in Hong Kong regarding the use of cookies, online tracking or behavioural advertising, organisations that deploy online tracking that involves the collection of personal data of website users must observe the requirements under the PDPO, including the six DPPs.

The PCPD published an information leaflet entitled 'Online Behavioural Tracking' (revised in April 2014), which provides the recommended practice for organisations that deploy online tracking on their websites. In particular, organisations are recommended to inform users what types of information are being tracked by them, whether any third party is tracking their behavioural information and to offer users a way to opt out of the tracking.

In cases where cookies are used to collect behavioural information, it is recommended that organisations preset a reasonable expiry date for the cookies, encrypt the contents of the cookies whenever appropriate, and do not deploy techniques that ignore browser settings on cookies unless they can offer an option to website users to disable or reject such cookies.

The PCPD also published the Guidance for Data Users on the Collection and Use of Personal Data through the Internet (revised in April 2014), which advises organisations on compliance with the PDPO while engaging in the collection, display or transmission of personal data through the internet.

Cloud computing

The PCPD published the information leaflet 'Cloud Computing' in November 2012, which provides advice to organisations on the factors they should consider before engaging in cloud computing. For example, organisations should consider whether the cloud provider has subcontracting arrangements with other contractors, and what measures are in place to ensure compliance with the PDPO by these subcontractors and their employees. In addition, when dealing with cloud providers that offer only standard services and contracts, the data user must evaluate whether the services and contracts meet all security and personal data privacy protection standards they require.

20 Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance (April 2011).

On 30 July 2015, the PCPD published the revised information leaflet 'Cloud Computing' to advise cloud users on privacy, the importance of fully assessing the benefits and risks of cloud services and the implications for safeguarding personal data privacy. The new leaflet includes advice to organisations on what types of assurances or support they should obtain from cloud service providers to protect the personal data entrusted to them.

Employee monitoring

In April 2016, the PCPD published the revised Privacy Guidelines: Monitoring and Personal Data Privacy at Work to aid employers in understanding steps they can take to assess the appropriateness of employee monitoring for their business, and how they can develop privacy-compliant practices in the management of personal data obtained from employee monitoring. The guidelines are applicable to employee monitoring activities whereby personal data of employees are collected in recorded form using the following means: telephone, e-mail, internet and video.

Employers must ensure that they do not contravene the DPPs of the PDPO while monitoring employees' activities. The PDPO has provided some additional guidelines on monitoring employees' activities and has recommended employers to:

a Evaluate the need for employee monitoring and its impact upon personal data privacy. Employers are recommended to undertake a systematic three-step assessment process:
- 'assessment' of the risks that employee monitoring is intended to manage and weigh that against the benefits to be gained;
- 'alternatives' to employee monitoring and other options available to the employer that may be equally cost effective and practical but less intrusive on an employee's privacy; and
- 'accountability' of the employer who is monitoring employees, and whether the employer is accountable and liable for failure to be compliant with the PDPO in the monitoring and collection of personal data of employees.

b Monitor personal data obtained from employee monitoring. In designing monitoring policies and data management procedures, employers are recommended to adopt a three-step systematic process:
- 'clarify' in the development and implementation of employee monitoring policies the purposes of the employee monitoring; the circumstances in which the employee monitoring may take place; and the purpose for which the personal data obtained from monitoring records may be used;
- 'communication' with employees to disclose to them the nature of, and reasons for, the employee monitoring prior to implementing the employee monitoring; and
- 'control' over the retention, processing and the use of employee monitoring data to protect the employees' personal data.

IV INTERNATIONAL DATA TRANSFER

Section 33 of the PDPO deals with the transfer of data outside Hong Kong, and it prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances, such as where the data protection laws of the foreign country are similar to the PDPO or the data subject has consented to the transfer in writing.

Section 33 of the PDPO has not been brought into force since its enactment in 1995, and the government currently has no timetable for its implementation. However, given the increased level of activity by the PCPD, it is foreseeable that Section 33 will be implemented eventually.

V COMPANY POLICIES AND PRACTICES

Organisations that handle personal data are required to provide their PPS to the public in an easily accessible manner. In addition, prior to collecting personal data from individuals, organisations must provide a PICS setting out, *inter alia*, the purpose of collecting the personal data and the classes of transferees of the data. As mentioned above, the PCPD has published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement (see Section III.i, *supra*), which provides guidance for organisations when preparing their PPS and PICS.

The Privacy Management Programme: A Best Practice Guide (see Section II.i, *supra*) also provides guidance for organisations to develop their own privacy policies and practices. In particular, it is recommended that organisations should appoint a data protection officer to oversee the organisation's compliance with the PDPO. In terms of company policies, apart from the PPS and PICS, the Best Practice Guide recommends that organisations develop key policies on the following areas: accuracy and retention of personal data; security of personal data; and access to and correction of personal data.

The Best Practice Guide also emphasises the importance of ongoing oversight and review of the organisation's privacy policies and practices to ensure they remain effective and up to date.

VI DISCOVERY AND DISCLOSURE

i Discovery

The use of personal data in connection with any legal proceedings in Hong Kong is exempted from the requirements of DPP3, which requires organisations to obtain prescribed consent (see Section III.i, *supra*) from individuals before using their personal data for a new purpose. Accordingly, the parties in legal proceedings are not required to obtain consent from the individuals concerned before disclosing documents containing their personal data for discovery purposes during legal proceedings.

ii Disclosure

Regulatory bodies in Hong Kong, such as the Hong Kong Police Force, the Independent Commission Against Corruption and the Securities and Futures Commission, are obliged to comply with the requirements of the PDPO during their investigations. For example, regulatory bodies in Hong Kong are required to provide a PICS to the individuals prior to collecting information or documents containing their personal data during investigations.

Nevertheless, in certain circumstances, organisations and regulatory bodies are not required to comply with DPP3 to obtain prescribed consent from the individuals concerned. This includes cases where the personal data is to be used for the prevention or detection of crime, and the apprehension, prosecution or detention of offenders, and where the compliance with DPP3 would likely prejudice the aforesaid purposes.

Another exemption from DPP3 is where the personal data is required by or authorised under any enactment, rule of law or court order in Hong Kong. For example, the Securities and Futures Commission may issue a notice to an organisation under the Securities and Futures Ordinance requesting the organisation to produce certain documents that contain its customers' personal data. In such a case, the disclosure of the personal data by the organisation would be exempted from DPP3 because it is authorised under the Securities and Futures Ordinance.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Public enforcement

An individual may make a complaint to the PCPD about an act or practice of a data user relating to his or her personal data. If the PCPD has reasonable grounds to believe that a data user may have breached the PDPO, the PCPD must investigate the relevant data user. As mentioned above, although a contravention of the DPPs does not constitute an offence in itself, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

Prior to the amendment of the PDPO in 2012, the PCPD was only empowered to issue an enforcement notice where, following an investigation, it is of the opinion that a data user is contravening or is likely to continue contravening the PDPO. Accordingly, in previous cases where the contraventions had ceased and the data users had given the PCPD written undertakings to remedy the contravention and to ensure that the contravention would not continue or recur, the PCPD could not serve an enforcement notice on them as continued or repeated contraventions were unlikely.

Since the entry into force of the Amendment Ordinance, the PCPD has been empowered to issue an enforcement notice where a data user is contravening, or has contravened, the PDPO, regardless of whether the contravention has ceased or is likely to be repeated. According to the PCPD's 2013 review, the number of enforcement notices served by the PCPD has more than doubled compared with 2012, and this could be attributed to the enhanced power of the PCPD to take such enforcement actions under the Amendment Ordinance.

The enforcement notice served by the PCPD may direct the data user to remedy and prevent any recurrence of the contraventions. A data user who contravenes an enforcement notice commits an offence and is liable on first conviction for a fine of up to HK$50,000 and two years' imprisonment and, in the case of a continuing offence, a penalty of HK$1,000 for each day on which the offence continues. On second or subsequent conviction, the data user would be liable for a fine of up to HK$100,000 and imprisonment for two years, with a daily penalty of HK$2,000.

ii Private enforcement

Section 66 of the PDPO provides for civil compensation. Individuals who suffer loss as a result of a data user's use of their personal data in contravention of the PDPO are entitled to compensation by that data user. It is a defence for data users to show that they took reasonable steps to avoid such a breach.

After the Amendment Ordinance came into force, affected individuals seeking compensation under Section 66 of the PDPO may apply to the Privacy Commissioner for assistance and the Privacy Commissioner has discretion whether to approve it. Assistance

by the Privacy Commissioner may include giving advice, arranging assistance by a qualified lawyer, arranging legal representation or other forms of assistance that the Privacy Commissioner may consider appropriate. According to the PCPD's 2013 review, the PCPD received 16 applications in 2013. Of these applications, one was granted assistance, five were rejected and two were withdrawn by the applicants.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Although the PDPO does not confer extraterritorial application, it applies to foreign organisations to the extent that the foreign organisations have offices or operations in Hong Kong. For example, if a foreign company has a subsidiary in Hong Kong, the Hong Kong subsidiary will be responsible for the personal data that it controls, and it must ensure the personal data are handled in accordance with the PDPO no matter whether the data are transferred back to the foreign parent company for processing.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

Legislative enactments relating to cybersecurity in Hong Kong are dealt with by both the PDPO and the criminal law.

The Computer Crimes Ordinance was enacted in 1993, and it has, through the amendment of the Telecommunications Ordinance,[21] the Crimes Ordinance[22] and the Theft Ordinance,[23] expanded the scope of existing criminal offences to include computer-related criminal offences. These include:

a unauthorised access to any computer; damage or misuse of property (computer program or data);
b making false entries in banks' books of accounts by electronic means;
c obtaining access to a computer with the intent to commit an offence or with dishonest intent; and
d unlawfully altering, adding or erasing the function or records of a computer.

ii Data breaches

There is currently no mandatory data breach notification requirement in Hong Kong. The PCPD published Guidance on Data Breach Handling and the Giving of Breach Notifications in June 2010, which provides data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the individuals involved. In particular, after assessing the situation and the impact of the data breach, the data users should consider whether the following persons should be notified as soon as practicable:

a the affected data subjects;
b the law enforcement agencies;

21 Sections 24 and 27 of the Telecommunications Ordinance.

22 Sections 59, 60, 85 and 161 of the Crimes Ordinance.

23 Sections 11 and 19 of the Theft Ordinance.

c the Privacy Commissioner (a data breach notification form is available on the PCPD's website);

d any relevant regulators; or

e other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the data subjects affected (e.g., internet companies such as Google and Yahoo may assist in removing the relevant cached link from their search engines).

X OUTLOOK

Recent trends clearly indicate the development of a stricter privacy regulatory regime in Hong Kong, with closer scrutiny and an increase in the number of enforcement actions by the Privacy Commissioner. As previously mentioned, although Section 33 has yet to enter into force, the introduction of the Guidance Note may itself signal that Section 33 could soon be implemented. Due to the significant penalties for breach of Section 33, IT organisations doing business in Hong Kong should ensure that they commence a review of their business and international data transfer processes to meet the standards set out in the PDPO and DPPs. A robust data privacy compliance programme will also be required to meet the growing requirements of company data privacy policies and to keep pace with legislative and technological developments.

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin

Yuet Ming Tham is a partner in Sidley Austin's Hong Kong and Singapore offices. She advises international corporations on their legal risks, such as those relating to privacy, data protection and cybersecurity law issues, as well as cross-border compliance and investigations, anti-bribery laws (including FCPA), international trade controls, sanctions, anti-money laundering and dispute resolution.

Prior to joining Sidley, Yuet was the Asia head of the regulatory, compliance and investigations group, and also head of the Asia life sciences group at another international law firm. She has also held roles as a deputy public prosecutor in Singapore and was the Asia Pacific regional compliance director for Pfizer. During that time, she was responsible for compliance and investigations in Singapore, Japan, China, Australia, Korea, India, Indonesia, Thailand, Taiwan, Hong Kong, Malaysia and the Philippines.

Yuet is named as a leading lawyer in *Chambers Asia Pacific* in four categories, as well as being recognised in *IFLR1000* and *The Legal 500 – Asia Pacific*. In 2014, she was the only lawyer awarded the Client Choice award by International Law Office for white-collar crime practice in Hong Kong. The leading legal directory, *Chambers Asia Pacific*, noted that industry players appreciate Yuet's 'wealth of knowledge of the latest trends across the region', as well as her having a 'tough, no-nonsense approach in tackling tricky compliance questions'. In the global edition of the book, she is described by clients as 'a marvelous and gifted attorney', and a client observed that 'two things stand out about her: she is extraordinarily responsive, but is also very good at getting answers to your questions from a practical perspective. In that respect, she really is a gem of a lawyer'. Yuet has up-to-the-minute knowledge on the rapidly changing issues surrounding privacy, data protection and cybersecurity matters related to Hong Kong, Singapore and the rest of Asia. She has written several articles and is a frequent speaker at industry conferences on these subjects.

She speaks English, Mandarin, Cantonese and Malay, and is admitted to practise in Hong Kong, Singapore, New York, and England and Wales.

SIDLEY AUSTIN LLP
Sidley Austin
39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645
Fax: +852 2509 3110
yuetming.tham@sidley.com