The Privacy, Data Protection and Cybersecurity Law Review

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 1
(published in November 2014 – editor Alan Charles Raul).

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

Law Business Research Ltd

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 9

HONG KONG

Yuet Ming Tham and Joanne Mok[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 (known as '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 will discuss the recent data privacy developments, including new legislation and guidelines, and major enforcement actions in Hong Kong in 2014. 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

In 2014, the Privacy Commissioner has continued to advocate the importance of data privacy protection by launching a Privacy Management Programme, which encourages organisations to embrace data protection as part of their corporate governance responsibilities.

In relation to new legislation, the Privacy Commissioner has raised concerns over certain data privacy issues to the Bills Committee on the Electronic Health Records

1 Yuet Ming Tham is a partner and Joanne Mok is an associate at Sidley Austin LLP.

Sharing System Bill, which if passed, would enable a platform for access to, and sharing of patients' health data by authorised healthcare providers.

As regards major enforcement actions, the Privacy Commissioner has served 48 enforcement notices on organisations that have placed 'blind' recruitment advertisement whereby job ads were placed without disclosing the identities of the hiring organisations.

i From compliance to accountability – Privacy Management Programme

On 18 February 2014, the PCPD issued the Privacy Management Programme: A Best Practice Guide as part of its campaign to encourage organisations to develop and improve their own privacy programmes. Although the Privacy Management Programme is not a legal requirement, organisations are encouraged to voluntarily take part in this programme. Various companies including companies in the insurance and telecommunication sectors have made a pledge to implement the Privacy Management Programme.

In a media statement on 23 January 2014, the Privacy Commissioner said that the Privacy Management Programme marked a strategic shift in the focus from compliance to accountability and organisations are now expected to embrace data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business requirement throughout the organisations.

ii Electronic Health Record Sharing System Bill

On 17 April 2014, the Food and Health Bureau submitted the Electronic Health Record Sharing System Bill (eHR Bill) to the Legislative Council. If passed, this legislation would enable a platform for the access to and sharing of patients' health data by authorised health-care providers.

In view of the sensitive and private nature of health data, the Privacy Commissioner expressed the view that there should be enhanced protection under the new legislation. The Privacy Commissioner expressed concerns about the eHR Bill in his submission to the Bills Committee on 21 May 2014. The major concerns raised in the submissions are as follows:[2]

a the accessibility of a patient's health records should be on a strictly 'need-to-know' basis;

b the system should provide a 'safe deposit box' to allow separate storage of certain data with enhanced access control;

c the discretion of the Electronic Health Record Commissioner in allowing bodies 'who directly or indirectly provide health care' and government bodies that are 'involved in providing health care' to register under the system is too wide; and

d in line with the provision in the Bill to create a specific offence for unauthorised access to health data held in the system through the use of computer, offences should be introduced for unauthorised access to the data in the system by any means and also for unauthorised use of the data.

2 PCPD media statement, 'Privacy Commissioner raised concern on Electronic Health Record Sharing System Bill', published on 21 May 2014.

iii Use of social networks

In April 2014, the PCPD published an information leaflet entitled Privacy Implications for Organisational Use of Social Networks advising on best practices for organisations to adopt. In particular, the information leaflet gives specific guidance on what should be considered when social networks are used in marketing, customer services, human resource management and network analytics.

On 14 May 2014, the PCPD invited the Deputy Chief Privacy Officer of Facebook to address and exchange views on privacy issues with individuals in Hong Kong during Privacy Awareness Week. The PCPD invited Facebook to commit to Hong Kong Facebook users that its privacy safeguards (such as to obtain express consent from users before overriding their privacy settings and to honour requests for deletion within 30 days) that are applicable to US and EU-resident users would also apply to Hong Kong Facebook users. With 4.3 million local users and almost 60 per cent of its population on Facebook, Hong Kong is one of the highest concentrations of Facebook users in the world.[3]

iv Blind recruitment advertisements

On 29 May 2014, the PCPD served 48 enforcement notices on organisations that had placed 'blind' recruitment advertisements whereby their identities were not disclosed (blind ads). These organisations were found to be in breach of the fairness principle for the collection of personal data. The enforcement notices were issued as a result of a random investigation initiated by the PCPD where 71 blind ads were selected. The PCPD stated that such practice constituted an unfair collection of the job applicants' data and could be exploited as a dishonest means to acquire personal data for direct marketing and even for fraudulent activities.[4]

In May 2014, after the enforcement notices were issued, the PCPD published an information leaflet entitled Understanding the Code of Practice on Human Resource Management – Frequently Asked Questions About Recruitment Advertisements, which provides guidance for employers about identity disclosure in advertisements. The Privacy Commissioner stated that where there is a genuine need to conceal identity, employers may resort to blind ads to solicit job applicants' enquiries rather than personal data.

III REGULATORY FRAMEWORK

i The PDPO and the six DPPs

The PDPO came into force on 20 December 1996 and it was recently amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance). The

3 PCPD media statement, 'PCPD's dialogue with Facebook on Personal Data Protection', published on 14 May 2014, quoting from the *South China Morning Post*, 9 September 2013.

4 PCPD media statement, 'Privacy Commissioner Condemned 48 Blind Recruitment Advertisements for Unfair Collection of Job Applicants' Personal Data', published on 29 May 2014.

majority of the provisions of the Amendment Ordinance came into force on 1 October 2012 and the provisions relating to direct marketing and legal assistance came 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 request.

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 a 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 is accurate and up-to date and is not kept longer than necessary for the fulfillment 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 of Hong Kong, the data users 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 is no longer required for the purpose for which it was 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 the offenders are liable for a fine.

Implications for organisations

The PCPD published a Guidance on Personal Data Erasure and Anonymisation (revised on 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 those 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 case, 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 of 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, dated 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, DVDs etc. Given 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 date protection policy 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 such 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 amount of disputes under the PDPO are in relation 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 of the data access request.

ii Direct marketing

New direct marketing provisions under the PDPO

The new direct marketing provisions under the Amendment Ordinance came 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 response) 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 is 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 is collected, for example, whether the personal data concerned is 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.[5] 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 made 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

In view of the technological advancements in recent years, the PCPD has published various guidelines and information leaflets to facilitate data users in protecting individuals' personal data and complying with the relevant data privacy laws.

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

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

the contents of the cookies whenever appropriate and not to 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 Cloud Computing Information Leaflet 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. Also, 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.

Employee monitoring

The PCPD published the 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. The guidelines are applicable to monitoring by telecommunications equipment (e.g., telephones, computers, mobile phones), company e-mail services, internet browsing, video recording and closed-circuit TV systems.

Employers must ensure that they do not contravene the DPPs of the PDPO while monitoring employees' activities. In particular, employers must ensure that:

a monitoring is only carried out to the extent necessary to deal with their legitimate business purpose;

b the personal data collected in the course of monitoring is kept to an absolute minimum and by means that are fair in the circumstances; and

c a written privacy policy on employee monitoring has been implemented and practicable steps have been taken to communicate that policy to employees.

IV INTERNATIONAL DATA TRANSFER

Section 33 of the PDPO deals with the transfer of data outside of 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 according to the Privacy Commissioner's recent media statement on 23 January 2014, the government currently has no timetable for its implementation in the future. One of the strategic focus of the PCPD for 2014 is to assist the government in reviewing the regulatory issues concerning cross-border flows of personal data.

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, among other things, 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:

a accuracy and retention of personal data;
b security of personal data; and
c access to and correction of personal data.

The Best Practice Guide also emphasised 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 by reason that 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 enforcement notices served by the PCPD have 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 where the foreign organisations have offices or operation 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 which it controls and it must ensure the personal data are handled in accordance with the PDPO, no matter whether the data is 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,[6] the Crimes Ordinance[7] and the Theft Ordinance[8] expanded the scope of existing criminal offences to include computer-related criminal offences. These include unauthorised access to any computer; damage or misuse of property (computer program or data); making false entries in banks' books of accounts by electronic means; obtaining access to a computer with intent to commit an offence or with a dishonest intent; and 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:

6 Sections 24 and 27 of the Telecommunications Ordinance.

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

8 Sections 11 and 19 of the Theft Ordinance.

a the affected data subjects;
b the law enforcement agencies;
c the Privacy Commissioner (a data breach notification form is available from 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 (for example, internet companies such as Google and Yahoo may assist in removing the relevant cached link from their search engines).

X OUTLOOK

The recent trend in Hong Kong clearly shows a stricter privacy regulatory regime in Hong Kong with closer scrutiny and increased enforcement actions by the Privacy Commissioner. There is also a growing public concern over privacy and data protection and a raising public expectation that organisations should adopt policies and procedures to protect their personal information.

It is therefore crucial for organisations doing business in Hong Kong to ensure that they put in place robust data privacy compliance programmes to meet the growing requirements and to conduct regular reviews and audits of their data privacy policies to keep pace with the legislative and technological developments.

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin LLP

Yuet Ming Tham is a partner in Sidley Austin's Hong Kong office. 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 Japan, China, Australia, Korea, India, Indonesia, Thailand, Taiwan, Hong Kong, Malaysia, Singapore and the Philippines.

Yuet is named as a leading lawyer in *Chambers Asia Pacific* in four categories, as well as being recognised in *IFLR 1000* and *Asia Pacific Legal 500*. In 2014, she was the only lawyer awarded the 'Client Choice' award by International Law Office for white-collar crime practice in Hong Kong.

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

JOANNE MOK

Sidley Austin LLP

Joanne Mok is an associate in the litigation team of the firm's Hong Kong office. Her practice focuses on data privacy law, complex commercial dispute resolution, and financial services regulatory matters. She advises clients on data privacy issues, including data protection and compliance, cybersecurity, cloud computing, direct marketing and electronic surveillance. Ms Mok speaks fluent English, Mandarin and Cantonese.

SIDLEY AUSTIN LLP
39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7888
Fax: +852 2509 3110
yuetming.tham@sidley.com
jmok@sidley.com

www.sidley.com