An Overview of Hong Kong's Personal Data (Privacy) Ordinance:
Key Questions for Businesses

Background to the PDPO

Hong Kong is one of Asia's earliest adopters of comprehensive data privacy regulation. The Personal Data (Privacy) Ordinance (the ***PDPO***) came into force in 1996.

Enforcement activity had been marginal for a number of years, but recent data privacy incidents, including a direct marketing scandal that became front page news in the summer of 2010, led to an overhaul of the regulatory regime in 2012 and a subsequent stepping up of enforcement action. Reforms brought into force in 2013 have made Hong Kong's regulation of direct marketing amongst the most stringent in the world.

Hong Kong's Privacy Commissioner for Personal Data (the ***Commissioner***) is now very active and regularly publishes official guidance on a wide range of topics.

Guidance issued in February, 2014 calls for businesses to adopt comprehensive Privacy Management Programmes directed at achieving compliance in all aspects of business.

With increased fines, an activist regulator, a policy of "naming and shaming" those who fail to comply and a growing public interest in data privacy issues, it is clear that PDPO compliance has to be a priority for Hong Kong businesses.

The Commissioner and his powers

The Commissioner can investigate complaints of breaches of the PDPO, as well as initiate investigations. The approach to enforcement is generally administrative and consultative in nature, but the scope for criminal enforcement has recently been broadened and the penalties for non-compliance have been increased.

At the conclusion of an investigation, the Commissioner can issue an enforcement notice against the "data user" (ie the business controlling the data processing), requiring it to take remedial action.

The Commissioner can institute civil or criminal proceedings against any data user that fails to comply with an enforcement notice, depending on the nature of the breach. Maximum penalties for breaches under the PDPO are fines of up to HK$1m (US$130,000) and imprisonment for up to five years.

Quite apart from the criminal sanctions, there are reputational risks for an organisation that is subject to an investigation. The Commissioner has the right to publish the results of any investigation, name the organisation involved and give details of the breaches committed.

What is personal data?

The PDPO draws from the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the guidelines which are the cornerstone for Europe's *Data Protection Directive EC95/46*.

The PDPO defines "personal data" very broadly and includes any data relating directly or indirectly to a living individual from which it is practicable for the identity of the individual to be directly or indirectly ascertained.

Does the PDPO have extraterritorial effect?	The PDPO does not include any express limitation on its territorial scope. However, some limitation may be implied from the discretion the Commissioner has to refuse to investigate a complaint which does not meet one of the following requirements: (i) the investigation relates to the personal data of Hong Kong residents or persons who were in Hong Kong at the relevant time; or (ii) the investigation relates to data users that are able to control the collection, holding, processing or use of the relevant personal data from Hong Kong.
On what basis can personal data be processed?	"Processing," in relation to personal data, is defined to include amending, augmenting, deleting or rearranging data, by automated or other means. Subject to specific exemptions, personal data can only be processed for the purposes notified to the data subject on or before the collection of the data and any directly related purpose. Data subjects must consent to any new or additional purpose. The PDPO contains a number of exemptions to these requirements, including an exemption for national security interests and exemptions for matters such as disclosures to law enforcement officials and processing in connection with legal proceedings.
Do data owners need to register with or notify any authorities, or appoint an official compliance officer?	There is no need to register with or notify any authorities of data processing, nor is there any requirement to appoint an official compliance officer. However, data users must provide data subjects with the name or job title and address of the individual who will be responsible for handling data access requests. In practical terms, it is becoming increasingly important to have senior internal roles that include responsibility for PDPO compliance. The Commissioner's February, 2014 guidance dealing with Privacy Management Programmes makes clear that significant organisational measures are the expected standard for compliance.
What rights do data subjects have to access and correct their data?	Data subjects have the right to know whether or not a business holds personal data about them. They have the right to access and make corrections to that data. Data users may refuse to comply with a request for access or a correction, but must be prepared to give reasons for doing so within 40 days of receipt of a proper request. They may charge a fee for producing the personal data.
Are there any restrictions on transfers of personal data to third parties? Or within a group of companies?	Personal data cannot be transferred to another data user without the data subject's consent. Where transfers are made for direct marketing purposes, the special requirements set out in the section below entitled "How is direct marketing regulated?" apply. The PDPO draws no distinction between related and unrelated entities, meaning that transfers within groups of companies are in principle regulated to the same standards. There is no requirement under the PDPO to obtain a data subject's consent to transfer personal data to a data processor (i.e., a person or entity which processes personal data on behalf of a data user). As a matter of practice, however, data users often notify data subjects that third party processing will be taking place.
How is external data processing regulated?	The PDPO stipulates that data users remain responsible for compliance in relation to any third party data processing arrangements. The Commissioner has issued specific guidance dealing with processing carried out by outsourced service providers and by cloud service providers. Banks, insurers and licensed securities businesses should take note that the Hong Kong Monetary Authority, the Hong Kong Commissioner of Insurance and the Hong Kong Securities and Futures Commission have all issued material outsourcing guidelines which address data privacy issues in relation to outsourced service arrangements.

Can data be exported to other countries?	The PDPO contains a data export restriction that has not yet been brought into force. The inoperative provision would make exports subject to data users meeting one of a number of conditions, including data subjects' written consent or situations in which the data user has reasonable grounds to believe that the personal data will be transferred to a jurisdiction that provides a similar degree of protection as Hong Kong. The Commissioner has been outspoken in his support for implementing the export restrictions in the near future and recently concluded a survey of 50 jurisdictions to produce a white list of places which have in force a data protection law which is substantially similar to, or serves the same purpose as, the PDPO. That list has now been submitted to the Hong Kong Government.
How is direct marketing regulated?	Hong Kong has one of the world's most complex direct marketing regulatory regimes. Much of the complexity relates to requirements that direct marketing notifications be sufficiently detailed. Data users are required to inform data subjects of the kinds of personal data they will be using for direct marketing purposes and the classes of goods or services that will be marketed. General language such as references to the marketing of "selected products and services" or "products and services we think you might be interested in" do not meet the new requirements. The PDPO provides that an `indication of no objection' will represent adequate consent for direct marketing purposes. On its face, this means that an "opt out" standard of consent applies rather than an "opt in" standard. However, the "opt out" standard adopted by Hong Kong requires that data subjects affirmatively indicate that they have opted out, for example, by signing and returning an application form without ticking the "opt out" box. Silence is not sufficient. If consent has been given orally, the data user must send a confirmation in writing to the data subject within 14 days confirming the scope of the consent obtained. In addition, the first time that the data user uses the personal data in direct marketing it must notify the data subject of its right to require the data user to stop the direct marketing. The data subject can subsequently require that marketing stop at any time. Grandfathering provisions apply to personal data collected and used for direct marketing purposes in compliance with the PDPO prior to 1 April, 2013. 'Cross-marketing' arrangements under which one business transfers personal data to another business for the second business's marketing purposes are subject to even more stringent controls. Oral consent is not possible, and data users must disclose whether or not personal data has been transferred for gain. No grandfathering applies. It should also be noted that Hong Kong maintains "do not call" registries for commercial electronic messages communicated within Hong Kong or to Hong Kong recipients by email, fax, SMS, MMS or by pre-recorded voice message. These registries are separately provided for under the 2007 Unsolicited Electronic Messages Ordinance.
What rules apply to employee monitoring?	The Commissioner has published guidance on the monitoring of employees in the workplace. Employers are obliged to carry out a privacy impact assessment and evaluate less intrusive approaches to achieving the objectives of the monitoring. Employers must then draft and communicate a written policy on employee monitoring to affected employees explaining the business purposes of the monitoring, the circumstances under which monitoring takes place and the kinds of personal data collected as part of the monitoring.
Is there an obligation to notify of data security breaches?	The PDPO does not specifically require data users to notify affected data subjects, the Commissioner or any other person of data security breaches. However, the Commissioner has published guidance strongly encouraging data users to make notification when a real risk of harm is reasonably foreseeable if no notification is made.

What is the current enforcement environment and are there any expected legislative developments?

The Hong Kong government's Bureau of Constitutional and Mainland Affairs comprehensively reviewed the PDPO in 2009-10, a process that resulted in significant reforms.

The fact that the PDPO was so recently reviewed may suggest that additional reforms are some time off. However, it is clear that the Commissioner's appetite for further development to the law continues, with data export controls being top of his list.

The consequences of not complying with the PDPO are becoming far more serious, particularly in light of policies of "naming and shaming" businesses found to not be complying with the law.

In January 2014, the Commissioner announced that Hong Kong had seen a 48% increase in privacy complaints in 2013, with roughly a third of total complaints relating to the new direct marketing controls. Public awareness of data privacy issues is clearly growing.

The Commissioner also reported that his referral of cases to Hong Kong police for criminal investigation was also up a third from 2012, suggesting a more aggressive approach to enforcement.

It is clear that the Commissioner will carry forward an activist approach to regulation and in the "Big Data" age of enhanced public awareness of data privacy issues, compliance with the law matters now more than it ever did before.

In February, 2014, the Commissioner published guidance calling for businesses to adopt comprehensive Privacy Management Programmes directed at achieving compliance in all aspects of their business. This "best practice" standard of compliance will likely be looked at in adjudicating future rounds of enforcement action. Businesses need to act now to ensure they are prepared.

March 2014

If you would like further information please contact a person mentioned below or the person with whom you usually deal.

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Peter Colegate
Associate, Hong Kong
T +852 2840 5961
peter.colegate@hoganlovells.com