Singapore Personal Data Protection Act – SPMI/ISOC

12 November 2013

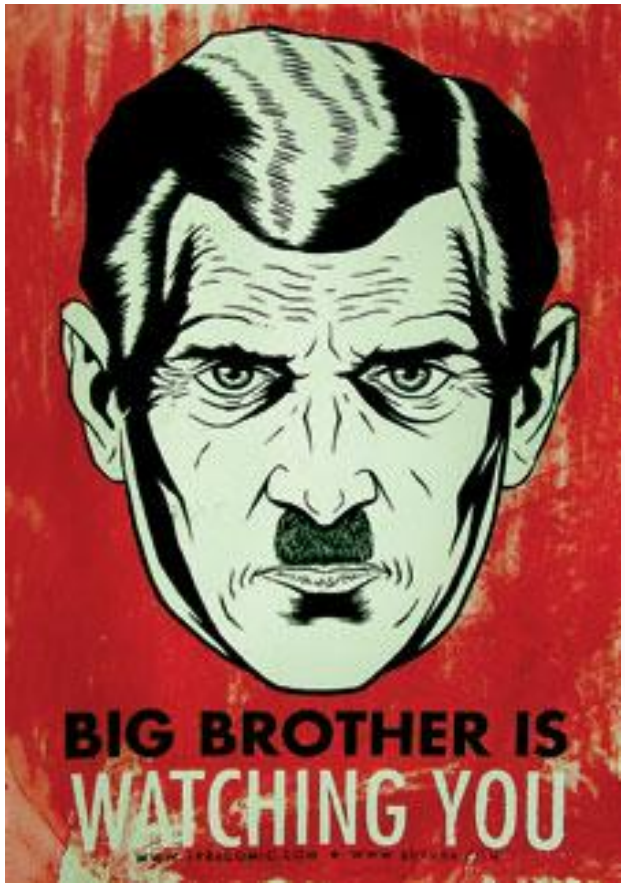
Bryan Tan

Partner, Pinsent Masons MPillay LLP

Pinsent Masons MPillay

Outline

- What is the PDPA all about?
- Specific obligations:
  - Consent
  - Notification
  - Retention
  - Data Protection Office
  - CCTV footages
  - DNC Regime
- Practical steps to achieving compliance
- Q&A



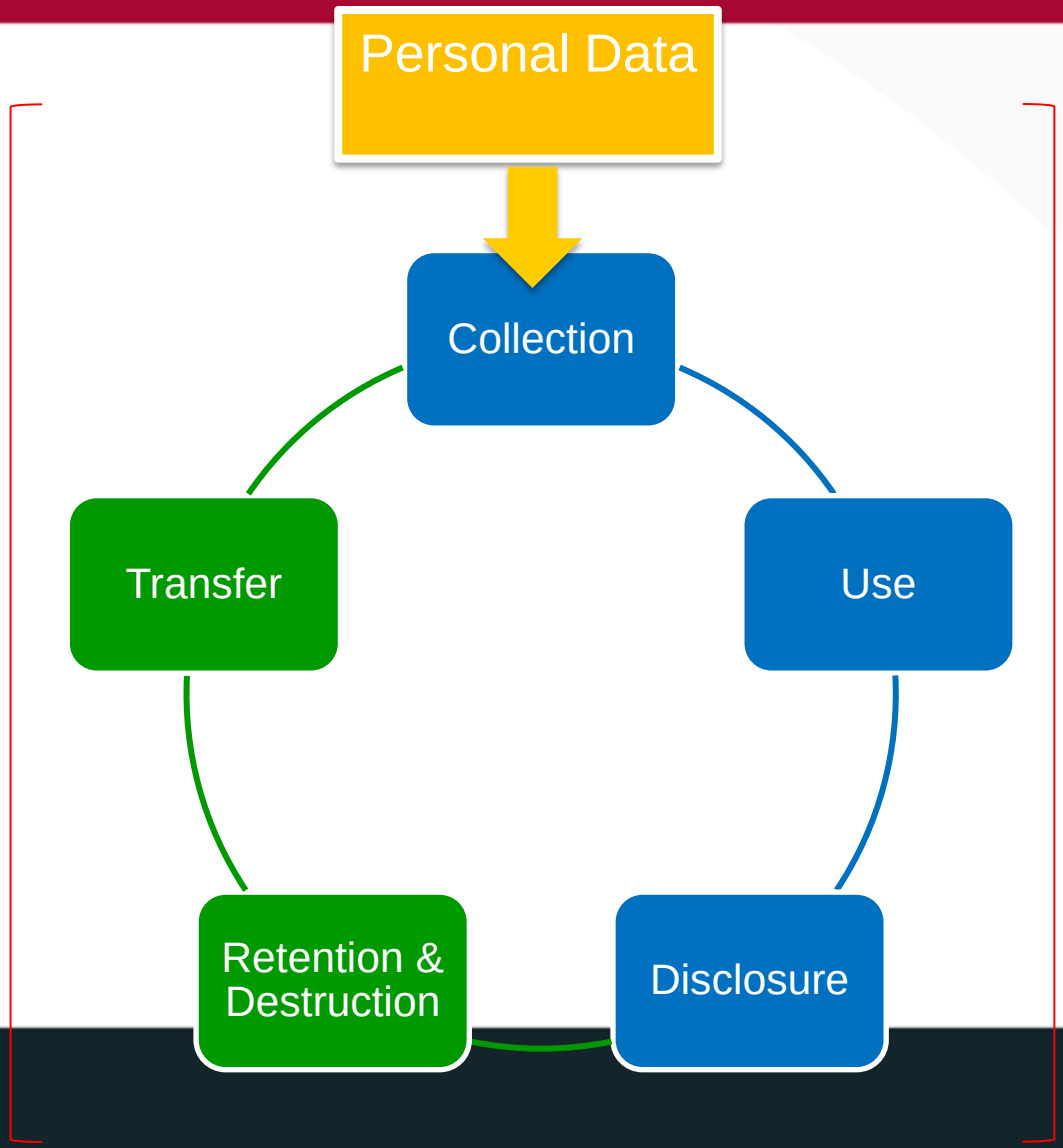
What is the PDPA all about?

"An Act to govern the collection, use and disclosure of personal data by obligations, and to establish the Personal Data Protection Commission and Do Not Call Register…"

Data Protection Regime

- Personal Data Protection Act 2012 ("**PDPA**") governs the collection, use, disclosure, transfer and security of personal data ("**PD**") by organisations
- Rationale:
  - Protect interests of consumers
  - Allowing organisations to obtain and process PD for legitimate and reasonable purposes
  - Strengthen Singapore's position as a business hub

Obligations imposed by the PDPA



Access and Correction

Accuracy

Security/ Protection

Openness

Pinsent Masons MPillay

Why is compliance important?

Negative Reasons

- Hefty fines imposed by the PDPA
- Fear of private action
- Reputational damages

Positive Reasons

- Targeted marketing activities
- Gain in the trust of internal and external stakeholders

What is the PDPC?

Singapore's main authority in matters relating to the PDPA

Key Functions

- Administer and enforce the PDPA
- Oversee the development and operation of the DNC Registry
- Issue guidelines and regulations
- Investigate complaints and resolve disputes

Investigative Powers

- To require documents/information
- To enter premises without warrant
- To enter and search premises with warrant

Compliance with the PDPA

Main PD provisions: Penalty of up to S$1m

Private action

Reputational damages

DNC Regime: Fine of up to S$10,000

Compliance with the PDPA

- An employer is responsible when an employee does not comply with the PDPA. However, it is a defence for the employer to prove that it ***took such steps as were practicable to prevent the employee from doing the act***.

*Both **employers** and **employees** are responsible for complying with the PDPA.*

Key issues in compliance

What are the standards required?

What is data protection anyway?

Compliance effort and costs

Conflict with existing practices

What is PD?

data, whether true or not, about an individual who can be identified —

(a) from that data; or

(b) *from that data and other information to which the organisation has or is likely to have access*

- Definition is broad
- Organisation is responsible for PD in its custody or under its control

Key timelines

7 November 2013

2 July 2014
Rest of the PDPA comes into force

< 2 months to go

< 8 months to go

2 January 2014

DNC provisions take effect

Pinsent Masons MPillay

The Advisory Guidelines (24 Sept 2013)

Issued on 24 September 2013 to provide guidance on how the PDPC will interpret the PDPA and the measures that will need to be taken in order to be compliant with the PDPA

Advisory Guidelines

- Advisory Guidelines on Key Concepts
- Advisory Guidelines on Selected Issues

Outstanding Issues

- Access and correction obligation
- Transfer limitation obligation
- Individuals who may act for others under the PDPA

What constitutes valid consent?

Express consent in writing is best. But what happens if such consent cannot be obtained?

Consent

- Consent is required for the collection, use or disclosure of PD
- Provision of consent:
  - Express
  - Deemed
  - Not needed (where collection is required by law)

Express Consent

- Notification of purpose of collection + “reasonableness”
- Express consent: in what form?
- Consent not validly given where:
  - an organisation’s collection, use and disclosure goes beyond what is reasonably required for the provision of goods/service
  - an organisation obtains or attempts to obtain consent by providing false/misleading information or using deceptive or misleading practices

Small print

6.2 Purpose: You agree that your Data may be used by us for:
(a) processing your registration for Membership Octopus;
(b) providing you with carefully selected offers, promotions and benefits by us, our subsidiaries, our affiliates (that is, our direct holding company and its subsidiaries), and/or Our Partners. We, our subsidiaries and/or our affiliates may need to carry out internal operational procedures to enable us:
(i) to better understand your characteristics and to provide other services better tailored to your needs (such as offering special promotions to you);
(ii) to assist us in selecting goods and services that are likely to be of interest to you;
(iii) to establish whether you already have a relationship with Our Partners; and
(iv) to arrange marketing offers;
(c) providing you with regular communications from us with details of the Programme and its Benefits;
(d) the management, operation and maintenance of the Programme, including audit and exercising our and your rights under these Terms and Conditions;
(e) designing new or improving existing services provided by us, our subsidiaries and/or our affiliates;
(f) investigation of complaints, suspected suspicious transactions and research for service improvement;
(g) prevention or detection of crime; and
(h) disclosure as required by law, rules, regulations, codes or guidelines.
6.3 Transfer: Data will be kept confidential by us, but you agree that for the purpose(s) set out in Clause 6.2, we may transfer or disclose such information to the following parties within Hong Kong (except that the parties set out in Clause 6.3(a) below may be located outside Hong Kong):

(a) our agents or contractors under a duty of confidentiality to us who provide administrative, telecommunications, computer, payment, data processing or other services to us in connection with the operation of our business (such as professional advisors, call centre service providers, gift redemption centres, or data entry companies);
(b) our subsidiaries and/or our affiliates which owe a duty of confidentiality to us; and
(c) any law enforcement agencies and/or regulatory bodies for compliance with applicable laws, rules, regulations, codes and/or guidelines and/or any person or entity to whom we, our subsidiaries and/or our affiliates are under a binding obligation to make disclosure under the requirements of any laws, rule, regulation, code and/or guideline and/or order of any competent court of law, law enforcement agencies and/or regulatory bodies, but such disclosure will only be made under proper authority.
6.4 Access: You have the right to:
(a) check whether we hold your Data and to have access to that Data;
(b) require us to correct any Data which is inaccurate;

Pinsent Masons MPillay

Deemed Consent

- Individual voluntarily provides PD; and
- Reasonable that individual would voluntarily provide PD

Withdrawal of Consent

- No prohibition on withdrawal: individuals can withdraw consent at any time
- On reasonable notice by the individual
- Individual to be informed of likely consequences of withdrawal
- No withdrawal where performance of a legal obligation would be frustrated

Previously Collected PD

What constitutes valid consent?

- **Verbal Consent –** ensure that consent is accessible for future reference by noting particulars of consent
- **Failure to Opt Out –** considerations
  - Was the failure to opt out due to reasons not related to a desire to consent?
  - E.g. did the person read the form?
- **Deemed consent –** two situations
  - Data is voluntarily provided by the individual for a specific purpose, and it is reasonable that he would do so
  - Data is provided by the individual for a purpose

What happens if the data is received from a third party?

Can the third party validly give consent on behalf of the individual, or has it obtained consent for the disclosure?

- Contractual undertaking
- Written or verbal confirmation
- Obtain a copy of the document evidencing the consent given by the individual to the third party to disclose the data

What happens if consent is withdrawn?

- Data does not need to be destroyed immediately
- An organisation can retain for as long as there are **legal** or **business reasons** to do so

Access to PD

- As soon as reasonably possible, on receipt of request
- Types of Information:
  - What PD is in the possession or under the control of the organisation
  - How the PD has been or may have been used or disclosed by the organisation within 1 year before the date of the request

Access to PD

- Where non-disclosure is permitted
  - Health of the individual is threatened
  - Individual will get harmed
  - PD or identity of another individual will be disclosed without his consent
  - National interest will be harmed

Correction of PD

- Requirements of correction
  - the individual requests correction
  - PD is in the custody or under the control of the organisation
- Organisation's responsibilities
  - correction as soon as practicable
  - send corrected PD to organisations that PD was disclosed to within 1 year before date of correction

What if you decide not to retain the data?

Destroy

- What happens if the data cannot be completely deleted? PDPC considers:
  - **Actions** taken in performing the destruction
  - **Intention** to use or access the data again
  - **Degree of effort and resources** required to retrieve the data

Anonymise

- Ensure minimal risk of re-identification through:
  - Robust techniques
  - Limiting disclosure
  - Limiting access
  - Imposing restrictions
  - Destruction

What constitutes valid notification?

Before obtaining an individual's consent, he must be notified of the purpose for which his data is being collected and handled. What should the individual be told?

- Purposes unexpected or of special concern
- Use of the organisation's privacy policy
- No "catch-all" phrases
- No need to mention all purposes

What are an organisation's obligations *vis-à-vis* the public?

Openness

Make available its DP policies and practices

Data Protection Officer

Ensure that the DPO office is accessible from Singapore and operational during Singapore business hours

Access/Correction Requests

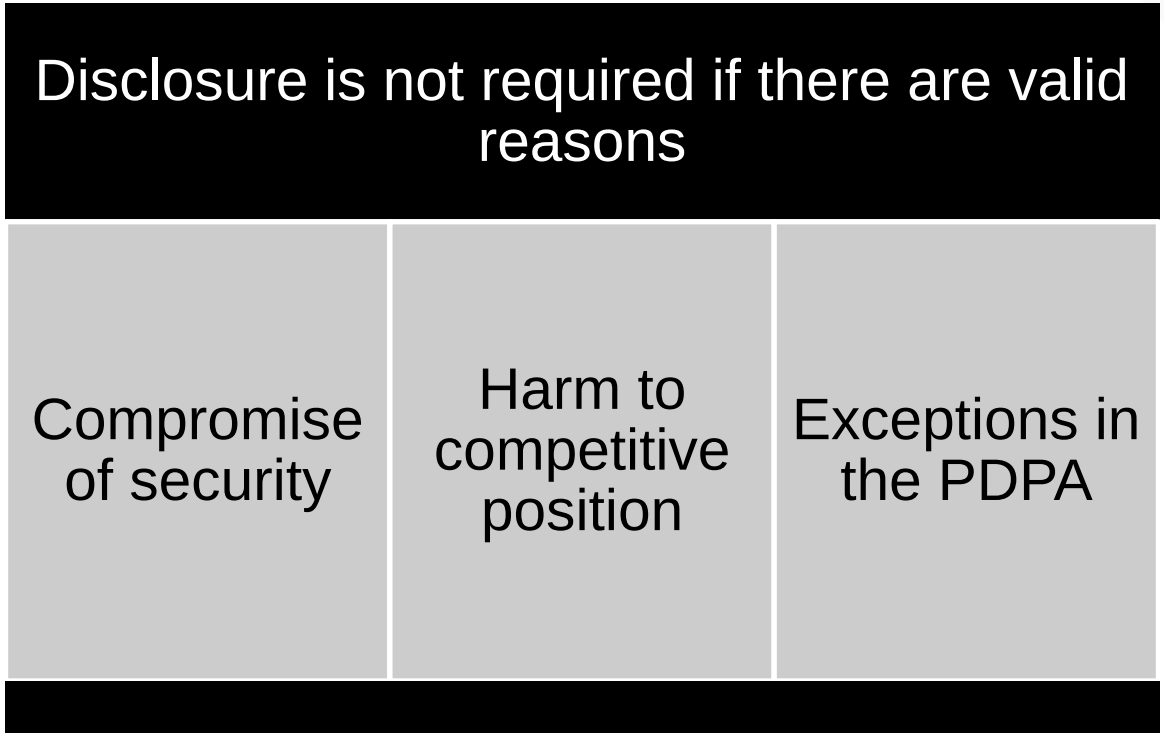
Respond to such requests within 30 days

Dealing with CCTV footages (notice)

- Images of an individual are personal data
- Notification obligation:
  - Written notice
  - Conspicuous location
  - Informing the individual that CCTVs have been deployed for a particular purpose
  - Need not reveal exact location of the CCTV

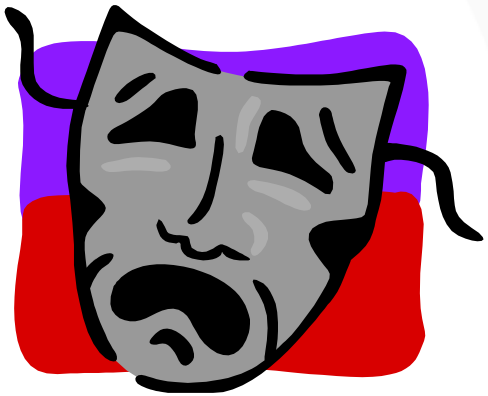
Dealing with CCTV footages (disclosure)

CCTV footages contain personal data and are subject to disclosure



Dealing with CCTV footages (disclosure)

- In the event that the footage needs to be disclosed, bear in mind that the footage will contain the personal data of other individuals.
- Unless the organisation has obtained consent from the relevant individual to disclose such personal data, the organisation should mask the personal data.



Care of PD

- Reasonable effort to ensure that PD collected is accurate and complete
- Protection – preventing unauthorised access, collection, use, disclosure, copying, modification, disposal
- Retention – when it is reasonable to assume that:
  - Purpose for collection has been fulfilled
  - Retention is no longer necessary for legal or business purposes
- Cessation of retention – destruction or anonymisation of PD

Care of PD – Practical Steps

Administrative measures

Robust policies and procedures; conduct regular training sessions

Physical measures

Locked cabinets; proper disposal of confidential documents

Technical measures

Ensure secure networks; implementing access controls; updating computer security

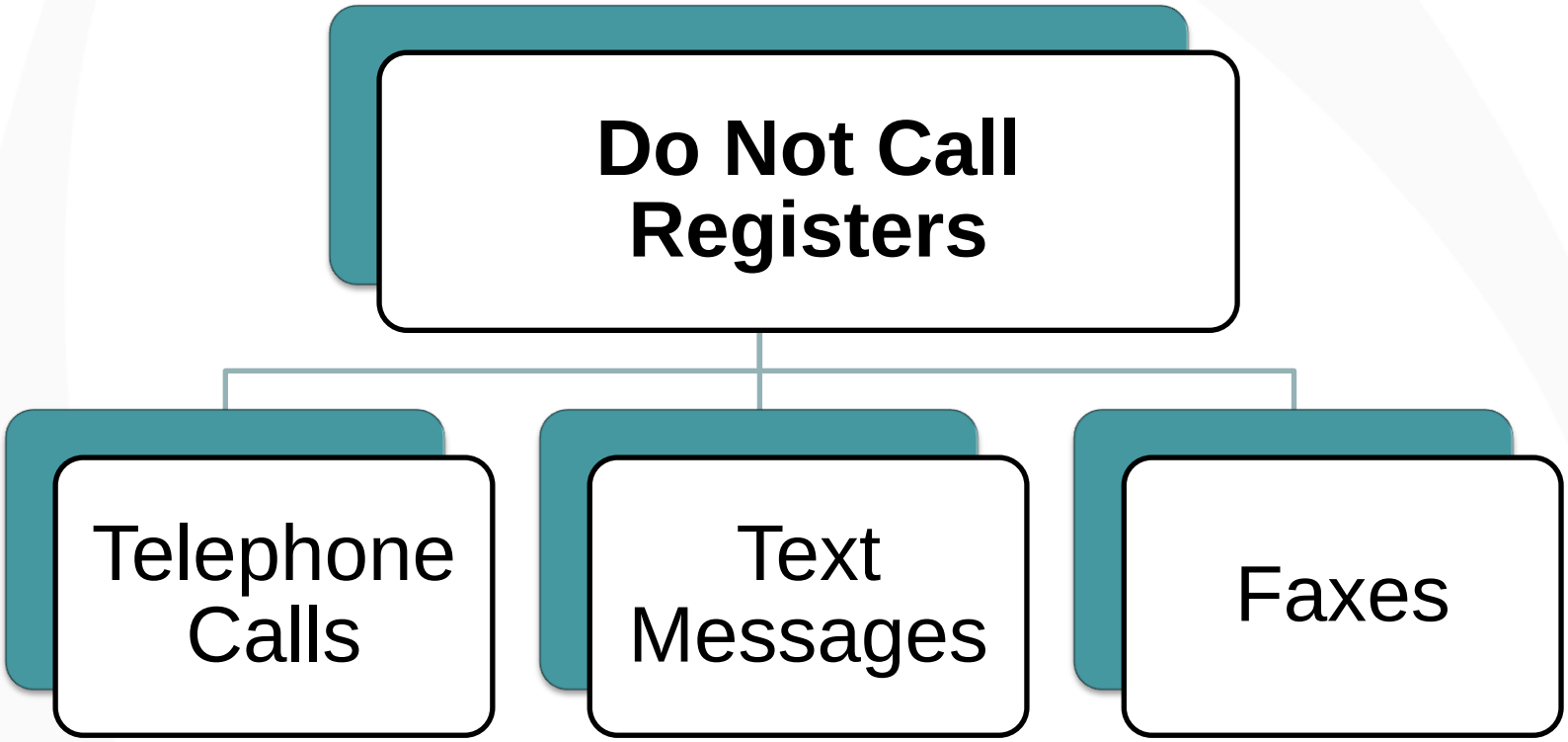
Transfer of PD

- PD can be transferred outside Singapore only if organisations ensure that the transferee provides a standard of protection that is comparable to that of the PDPA

DNC Regime


Hello! May I please interrupt your private time to sell you something you don't want?

DNC Regime - Scope



DNC Regime - Scope

What is a specified message?

- Message that advertises, promotes or offers:
  - to supply or provide goods/services
  - suppliers or providers of goods/services
  - land, interest in land, business/investment opportunity

DNC Regime – Obligations

- Key duties
  - **Check the DNC Register**
    - 2 Jan – 31 May 2014: 60 days
    - 1 June – 1 July 2014: 30/60 days
    - 2 July 2014 onwards: 30 days
  - **Identify the sender of message**
    - Providing information on sender
    - Not concealing or withholding the calling line identity of the sender

DNC Regime - Consent

- Clear and unambiguous consent required:
  - Have you notified the individual **clearly and specifically** that specified messages will be sent to his/her Singapore telephone number?
  - Has the individual given consent through some form of positive action?

DNC regime (consent)

- Clear and unambiguous consent:
  - Have you notified the individual **clearly and specifically** that specified messages will be sent to his/her Singapore telephone number?
  - Has the individual given consent through some form of positive action?

DNC regime (consent)

Marketing consent

To hear from us please tick the following:

☑ **Yes. I would like you to contact me about British Airways Group and Executive Club news, services, offers and BA Miles promotions.**

☑ **Yes. I would like you to contact me about news, services, offers and BA Miles promotions from our Executive Club Marketing Partners.**

We may communicate some news, offers and BA Miles Promotions **by email only.**

☑ **Yes. I would like to receive the above by email.**

☐ **Yes. I would like to receive the above by text message (SMS) where available.**

British Airways will not sell your data to any third party for direct marketing.

http://www.britishairways.com/travel/marketing-consent/public/en_gb

DNC regime (consent)

“you consent to receive information about special offers we may have from time to time, by SMS”

“you consent to the use of your personal data for marketing purposes”

Retailer A sends an individual an email stating that unless the individual replies, the individual is considered to have agreed to receiving information about special offers that Retailer A may have from time to time, via SMS.

Achieving compliance (practical steps)

Fact finding

- Checklist
- Questionnaire
- Mapping

Gap analysis

- Identification
- Documentation
- Reporting

Implementation

- Policies
- Manuals
- Appointments
- Processes
- Training

Establish the data protection office

- Establishing the data protection office
  - Who is the DPO?
  - Governance structure?
  - Who supports the DPO?
  - What are the roles of the DPO?
    - Pre-compliance
    - Compliance
    - Post-compliance

Adopt good practices

- Access controls
- Update IT security
- Confidentiality obligations
- Institute appropriate policies
- Employee training

On-going compliance

- Compliance is an on-going process
  - People change
  - Processes change
  - Standards change
  - Technology changes

Q&A

Pinsent Masons MPillay

Pinsent Masons MPillay LLP is a limited liability partnership registered in Singapore (UEN/Registration Number: T10LL1128C) and is a joint law venture between Pinsent Masons LLP and MPillay registered in Singapore under the Limited Liability Partnerships Act (chapter 163A). The word 'partner', used in relation to the LLP, refers to a partner of the LLP or an employee or consultant of the LLP of equivalent standing. A list of partners of the LLP, and of those non-partners who are designated as partners, is available at the LLP's registered office at 16 Collyer Quay, #22-00, Singapore 049318. We use 'Pinsent Masons MPillay' to refer to Pinsent Masons MPillay LLP.
© Pinsent Masons MPillay LLP 2013

For a full list of our locations around the globe please visit our websites:

www.pinsentmasonsmpillay.com

www.Out-Law.com