Regulatory Update – Amendments to Personal Data Protection Act ("PDPA") Effective from 1 February 2021

The Personal Data Protection Commission ("PDPC") announced the much-anticipated updates to the PDPA on 29 January 2021. This is the first time the PDPC has updated the PDPA since it came into force on 1 July 2014. In this regulatory update we will address the three major changes made to the PDPA that came into effect from 1 February 2021, and we will outline the practical implications they may have on your business.

Mandatory Data Breach Notification Regime

Businesses are now required to notify the PDPC in 2 situations where a data breaches either has resulted in, or is likely to result in, significant harm to an affected individual or the data breach is of a significant nature (i.e., involves data of 500 or more individuals).

In addition, an individual that has been affected by a data breach must be notified if the breach is likely to significantly harm them. Examples of what constitutes significant harm in the context of the financial industry includes authenticating data relating to individuals' accounts, credit card details, bank account numbers, salary information, details of net worth or creditworthiness, personal identification and health information and details of deposits, loans, investments or insurance policies etc.. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 includes a full list of what personal data or types of data that could be deemed as significant.

The protection obligation has been extended to require firms to make security arrangements to prevent the loss of electronically stored data, but a mitigating factor has also been introduced. If the personal data has been protected by a technological measure (e.g. encryption), that means the lost data is unlikely to cause any significant harm, then the firm is not required to notify each affected individual.

Ideally the PDPC would like notifications to be made as soon as practicable but realistically have stated that notifications must be made to them no later than 3 calendar days after the business makes the assessment that a data breach warrants a notification. If you have identified a notifiable breach, you will be expected to provide the PDPC with a chronological account of the steps taken following the identification of the breach. This should include a detailed assessment of the breach, the number of individuals affected or the amount of potential harm that could be caused and the reasons why you felt it warranted a notification to the PDPC. In addition to this, you will be expected to outline any actions taken by the company before and after the identification of the breach.

The penalties for data breaches have also been increased. Firms that have an annual turnover in Singapore in excess of S$10 million can now be fined up to 10% of the firm's annual turnover in Singapore.

ComplianceAsia Consulting Pte Ltd. 137 Telok Ayer Street #03-06, Singapore 068602
Tel: (65) 6533 8834 www.complianceasia.com

Individual Criminal Offences for Mishandling of Personal Data

The PDPA has introduced three new criminal offences for individuals who have been found to have egregiously mishandled personal data. The offences include:

1. Knowing or reckless unauthorised disclosure of personal data;
2. Knowing or reckless unauthorised use of personal data for wrongful gain or wrongful loss to any person; and
3. Knowing or reckless unauthorised re-identification of anonymised data.

If found guilty of these offences an individual could face a fine not exceeding S$5,000 or imprisonment for a term not exceeding two years or both.

Consent Framework Expanded

Another substantial update is the inclusion of provisions to allow for deemed consent by contractual necessity to allow the firm to collect, use and disclose personal data to fulfill a contract with an individual and deemed consent by notification of a new purpose to allow organisations to collect, use and disclose personal data.

The following further expansions of deemed consent have been introduced:

- A legitimate interest exception where a firm may collect, use or disclose personal data without consent if that is in the legitimate interest of the firm and the resulting benefit to the public is greater than any adverse effect on an individual.
- A business improvement exception if that cannot be achieved without the use of the data and there is no adverse effect on an individual.

Data Portability

The amendments to the PDPA impose a data portability obligation on firms which allow an individual to submit a data porting request to one company (the porting organization) to transfer data to another company (the receiving organization). This obligation will come into effect at a later date when the data porting regulations are enacted.

How we can help

Our dedicated projects team can assist you with reviewing and updating your personal data protection policies to ensure that they address the updates that have been made to the PDPA. In addition, we can also assist with providing employee training on how to comply with the PDPA requirements.

ComplianceAsia Consulting Pte Ltd. 137 Telok Ayer Street #03-06, Singapore 068602
Tel: (65) 6533 8834 www.complianceasia.com

About ComplianceAsia

ComplianceAsia is the longest established compliance consulting firm in Asia Pacific established in 2003 with key offices in Hong Kong, Shanghai, Singapore, Tokyo and London. We have an unmatched track record of completing complex compliance consulting projects for financial firms in the APAC region.

With over 70 staff, including compliance experts with experience in dealing with the SFC, HKMA, MAS, CSRC, JFSA and Asian exchanges, we provide independent, unbiased advice on Asian financial industry legislation and regulations. Our international client base consists of asset managers, hedge funds, private equity funds, family offices, broker-dealers, insurers, wealth managers and investment banks.

Contact Us Today

SINGAPORE
137 Telok Ayer Street #03-06
Singapore
068602

T: +65 6533 8834

HONG KONG
Suite 1102
ChinaChem Tower
34-37 Connaught Road
Central

T: +852 2868 9070

MAINLAND CHINA
Room 132, Unit 1301-1308
13/F, Shanghai Tower
No.479 Lujiazui Ring Road
Pudong New Area Shanghai

T: +86 147 1431 1859

JAPAN
Level 2
Marunouchi Nijubashi Building
3-2-2 Marunouchi Chiyoda-ku
Tokyo 100-0005

T: +81 3 6837 5483

UNITED KINGDOM
1 St. Andrew's Hill
London
EC4V 5BY

T: +44 (0) 20 7213 0300
M: +44 (0) 7310 972435

Philippa Allen
CEO
E: philippa.allen@complianceasia.com

Alex Duperouzel
Managing Director
E: alex.duperouzel@complianceasia.com

Lachlan Chubb
Regional Head of Regulatory Advisory and Projects
E: lachlan.chubb@complianceasia.com

Geralt Owen
Regional Head of Client Relations
E: geralt.owen@complianceasia.com

Cherry Chan
Regional Head of Ongoing Support and Client Services
E: cherry.chan@complianceasia.com

Rachel Wu
Head of Mainland China Client Engagements
E: rachel.wu@complianceasia.com

Robert Lind
Senior Representative, UK and Europe
E: robert.lind@complianceasia.com

Hanae Kuroda
Compliance Consultant
E: hanae.kuroda@complianceasia.com

www.complianceasia.com
ComplianceAsia