Five Key Proposals to Amend Singapore's Data Protection Act

May 22, 2020

On May 14, 2020, Singapore's Ministry of Communications and the Personal Data Protection Commission (the "PDPC") launched an online public consultation on a new bill (the "Bill") proposing updates to the Personal Data Protection Act (the "Act"). Domestic corporations and multinationals alike will need to keep abreast of the changes to ensure ongoing compliance.

Reflecting feedback from three previous consultations, the proposed revisions aim to ensure the Act remains in step with technological advances and developments in global data protection legislation.

FIVE KEY AMENDMENTS

Five key amendments to the Act are:

New Mandatory Data Breach Notification Obligations

For the first time in Singapore, the Bill proposes mandatory data breach notification obligations. Notifications would be due to both the PDPC and the impacted individuals. Notification would be triggered by unauthorised access, collection, use, disclosure, disposal or loss of personal data which either (i) results, or is likely to result, in significant harm to the affected individual(s), or (ii) is of a significant scale (i.e., impacting 500 or more individuals). New regulations would also prescribe the categories of data likely to cause individuals significant harm. This would likely include national identification numbers, credit card details and other important identifying information. Organisations would not need to notify affected individuals, but would still need to notify the PDPC, where the compromised personal data was encrypted (or similarly protected) or where instructed by a Singaporean law enforcement agency or the PDPC. It is unclear at present whether requests made by non-Singaporean law enforcement agencies would be relevant for the exception.

Where an organisation has reason to believe that a data breach has occurred, the organisation would have to assess in a reasonable and expeditious manner whether the data breach triggers notification. Similar to under the GDPR, organisations would have to notify all affected individuals as soon as practicable and notify the PDPC no later than three calendar days after the day the organisation determines that notification is required.

While the Bill is inspired by notification obligations under global models like the GDPR, U.S. state breach laws and the Australia Data Privacy Act, companies handling cross-border cybersecurity incidents should remain mindful that subtle differences might result in different notification requirements arising in connection with the same incident.

Increased Cap on Penalties

Currently, the PDPC can impose fines up to S$1 million for violations of the Act. The Bill proposes increased maximum penalties of up to the greater of 1% of annual gross turnover in Singapore or S$1 million. The PDPC hopes that the higher cap would serve as a deterrent and provide it with increased flexibility to ensure fines reflect the seriousness of a breach. Notably, the cap remains significantly below the GDPR maximum fine of the higher of €20 million or 4% of annual *worldwide* turnover.

Amendments to Deemed Consent and Alternatives to Consent

At present, consent is the primary basis for the collection, use and disclosure of personal data. Consent is deemed valid if (i) the individual voluntarily provides the information, and (ii) it is reasonable that the individual would voluntarily provide the data. To align more closely with other global laws, the Bill proposes to expand deemed consent to include:

- Contractual Necessity: i.e., where it is reasonably necessary for contractual performance, consent may be deemed to have been given for the disclosure of personal data to third parties.

- Consent by Notification: i.e., where (i) the organisation notifies an individual of the purpose of the intended data processing, (ii) the organisation provides a reasonable time period for the individual to opt out and (iii) the individual does not opt out. Organisations would be able to rely on this deemed consent to send direct marketing material to individuals.

The Bill also proposes two new alternatives to consent:

- Legitimate Interests: With echoes of the GDPR, organisations would be able to process personal data where the public interest outweighs any adverse impact on the individual. Public interest may include the prevention and detection of illegal activities, identifying threats to safety and security or ensuring IT and network security. Organisations would need to complete a risk assessment and disclose information to support their reliance on legitimate interests. Organisations may not rely on this exception to send direct marketing materials to individuals.

- Business Improvement: Organisations would also be able to use personal data without consent for business improvement purposes. Namely, to: (i) improve operational efficiency and service, (ii) develop and improve products and services, and (iii) learn about an organisation. This exception is intended to apply to companies within the same corporate group.

Together, these new bases for processing personal data would give organisations greater flexibility in how they can use data and greater clarity to individuals as the new bases are likely to be more intuitively understood.

Introduction of the Accountability Principle and New Criminal Offence

The Bill would also introduce accountability as a key principle of the Act. Like under the GDPR's accountability principle, organisations would be required to demonstrate their compliance with the Act and would be held accountable to individuals for the proper handling and safekeeping of personal data. Organisations may therefore need to revisit their record-keeping practices surrounding their use of personal data and related compliance processes.

The Bill would also strengthen the accountability of individuals who handle or have access to personal data through their employment, introducing new criminal offences to hold individuals accountable for mishandling personal data, e.g. where an individual discloses personal information they obtain from their employer to another person without due authorisation. Nevertheless, organisations would still have primary responsibility for data protection compliance and organisations remain liable for the actions of their employees in the course of employment. The offence would be punishable by a fine not exceeding S$5,000 or imprisonment for a term not exceeding two years, or both.

Data Portability Right

Like under the GDPR, the Bill would introduce the right for individuals to request an organisation to transmit a copy of their personal data to another organisation. This

would, for example, help individuals switch between service providers. The data portability obligation would apply to requests from individuals who have an existing, direct relationship with organisations which have a presence in Singapore. This would include organisations that are registered or recognised under the law of Singapore or organisations that have a business presence there. The PDPC is still considering whether to extend the portability regime to organisations in jurisdictions with comparable protection and reciprocal arrangements.

If an organisation refuses a data porting request, the individuals would have to be notified within a reasonable time and provided with reasons for the refusal. The PDPC would have the power to review refusals and any fees charged for the porting of data.

Together, these changes would represent a significant shift in Singaporean data protection law, drawing inspiration from approaches taken in other major jurisdictions.

* * *

Please do not hesitate to contact us with any questions.

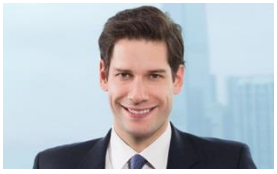
NEW YORK

Jeremy Feigelson
jfeigelson @debevoise.com

SHANGHAI

Philip Rohlik
prohlik@debevoise.com

HONG KONG



Ralph Sellar
rsellar@debevoise.com

LONDON

Christopher Garrett
cgarrett@debevoise.com

Nelson Goh
ngoh@debevoise.com

Robert Maddox
rmaddox@debevoise.com

Hilary Davidson
hdavidson@debevoise.com