DREW & NAPIER

DATA PROTECTION QUARTERLY UPDATE

APRIL 2018

In this issue

This newsletter is intended to provide general information and may not be reproduced or transmitted in any form or by any means without the prior written approval of Drew & Napier LLC. It is not intended to be a comprehensive study of the subjects covered, nor is it intended to provide legal advice. Specific advice should be sought about your specific circumstances. Drew & Napier has made all reasonable efforts to ensure the information is accurate as of 3 April 2018.

WELCOME MESSAGE

The Drew & Napier Telecommunications, Media and Technology Practice Group is pleased to present the latest issue of our Data Protection Quarterly Update. In this Quarterly Update, we will provide an overview of important data protection law developments in Singapore as well as in jurisdictions around the world.

In this issue, we highlight key takeaways from the three most recent enforcement decisions issued by the Personal Data Protection Commission (***PDPC***), and examine several of the PDPC's latest publications, including its new Guide to Basic Data Anonymisation Techniques. Apart from that, we will also analyse the emergence of new regulatory instruments and frameworks in several jurisdictions including Australia, Canada, the United Kingdom as well as the European Union (***EU***).

We hope that this new publication will be useful to you, as your business navigates the increasingly complex regulatory landscape in data protection law. We welcome your feedback and questions on any of the data protection news and articles featured in this Quarterly Update, as well as any suggestions that you may have on topics to be covered in future publications.

For more details on the Drew & Napier Telecommunications, Media and Technology Practice Group, please visit: **http://www.drewnapier.com/Our-Expertise/Telecommunications-Media-Technology**.

IN THE NEWS

SINGAPORE

The PDPC issues three Grounds of Decisions

Between 30 December 2017 and 20 March 2018**,** the PDPC issued enforcement decisions against one individual and four organisations for breaching their data protection obligations under the Personal Data Protection Act 2012 (No. 26 of 2012) (***PDPA***). In addition, it issued a separate ground of decision explaining its decision to discontinue investigations against one

organisation, My Digital Lock Pte. Ltd. The three grounds of decision are as follows:

(a) Sharon Assya Qadriyah Tang (***Tang***) (issued 11 January 2018);

(b) Jiwon Hair Salon Pte Ltd, Next@Ion Pte. Ltd., Next Hairdressing Pte. Ltd. and Initia Pte Ltd (collectively, ***4 Hair Salons***) (issued 23 January 2018); and

(c) My Digital Lock Pte. Ltd. (***My Digital Lock***) (issued 12 February 2018).

Tang

Background

Tang was employed as a telemarketer from 2004 to 2014. Between 2012 and 2014, Tang started purchasing "leads" comprising personal data such as an individual's name, NRIC number, mobile number, and annual income range.

From late 2012 to 23 February 2017, Tang re-sold the leads in her possession for S$0.05 to S$0.20 per lead on 9 to 10 occasions via various websites on the Internet, making an estimated sum of S$5,000 in profit. Tang concealed her identity by using an alias and corresponding email address, her husband's bank account number, and a mobile phone number registered under her friend's name.

The PDPC's Decision

The PDPC found Tang to be in breach of sections 13 and 20 of the PDPA. Section 13 (***Consent Obligation***) requires an organisation to obtain consent from individuals with respect to the collection, use and disclosure of personal data, while section 20 (***Notification Obligation***) requires an organisation to inform individuals of the purposes for the collection, use and disclosure of personal data. The PDPC's reasons are set out below:

(a) Tang was an "organisation" subject to the Data Protection Provisions of PDPA

While the Data Protection Provisions in Parts III to VI of the PDPA (***Data Protection Provisions***) are only applicable to an "organisation" under the PDPA, individuals may be treated as an "organisation" for the purposes of the PDPA if they were not acting in a personal or domestic capacity.

On the facts, the PDPC found that Tang was clearly not acting in a personal or domestic capacity as the buying and selling of leads were not for her own personal use or purposes, but rather in a business capacity. In this regard, Tang was regarded as an "organisation" for the purposes of the PDPA, and subject to the Data Protection Provisions.

(b) Tang's sale and purchase of leads was in contravention of the Consent and Notification Obligations under the PDPA

The PDPC found that the Consent and Notification Obligations applied to Tang's purchase of leads (i.e., "collection" of personal data) and her sale of leads (i.e., a "disclosure" of personal data).

As the Data Protection Provisions of the PDPA only came into effect on 2 July 2014 (the ***Appointed Day***), Tang was not subject to or required to comply with the Data Protection Provisions of the PDPA in respect of the collection, use and disclosure of the personal data found in her database of 30,990 leads before the Appointed Day.

After the Appointed Day, however, Tang would have to provide notification to, and obtain consent from, the individuals involved pursuant to the Consent and Notification Obligations unless an exception applies. In this regard, the PDPC found no evidence that Tang had continued to purchase leads from other sellers after the Appointed Day. In respect of the sale of personal data, however, there was a question of whether Tang could rely on section 19 of the PDPA to continue to use or disclose (i.e., sell) such personal data to third parties after the Appointed Day, given that Tang had been selling personal data since 2012 and before the Appointed Day. The PDPC found that Tang could not rely on section 19 for the following reasons:

(i) section 19 only permits the continued "use" of personal data if such use falls within the purposes of collection, and does not extend to the "disclosure" of personal data unless the disclosure "is necessarily part of the organisation's use of such personal data";

(ii) in respect of personal data which was sold before the Appointed Day, Tang went beyond using the personal data for her own telemarketing purposes, as such disclosure (i.e. sale) was the main activity being carried out in this case and was not incidental to any of the organisation's own uses of the personal data; and

(iii) in respect of personal data that was not sold before the Appointed Day, there was never an existing practice of selling the personal data in the first place, and hence there was no "use" to be carried on.

During the course of the PDPC's investigations, Tang admitted that she had not obtained consent from the individuals for the sale of their personal data to third parties, nor had she checked or verified with the online sellers if they had obtained the individuals' consent for the same. The PDPC also verified with several individuals whose personal data had been found in Tang's database that they had not been informed of or consented to the sale of their personal data. Accordingly, Tang was found to be in breach of both the Consent and Notification Obligations under the PDPA.

The PDPC's Actions

In assessing the breach and the directions to be imposed on Tang, the PDPC considered the following factors:

(a) Tang's database of leads included personal data of a sensitive nature i.e. NRIC numbers and salary ranges of individuals;

(b) Tang's use of means to obscure her identity when selling the leads was indicative of a guilty conscience and of a premeditated and deliberate contravention of the PDPA;

(c) profiteering from the sales of personal data by organisations at the expense of consumers or individuals is the very kind of activity which the PDPA seeks to curb, and hence, must be severely dealt with;

(d) Tang's candid admission to the wrongdoing at the first instance, her rendering of full cooperation with the investigations and in providing evidence;

(e) the fact that Tang was not carrying out the sale and purchase of personal data on a large-scale basis but rather, opportunistically and on the side to supplement her income, and that based on a conservative estimate, the cumulative amount of income earned from the sale of the leads was unlikely to exceed S$5,000; and

(f) crucially, the special financial circumstances of Tang and her husband, such as the fact that they were of limited financial means and were earning modest salaries, and that they had a child and family to support, were taken into consideration as imposing a high financial penalty would likely place a crushing burden on Tang and her family in the circumstances and cause undue hardship.

Based on the above factors, the PDPC directed Tang to pay a financial penalty of S$6,000 within 30 days from the date of the PDPC's decision. The PDPC expressly noted that the lower financial penalty in this case is exceptional and should not be taken as setting any precedent for the extension of the same leniency or indulgences in any other cases, as the PDPC takes a serious view towards any unauthorised sale of personal data.

Key Takeaway

The PDPC takes a serious view of breaches under the PDPA involving the unauthorised sale of personal data, as they may constitute cases of potential misuse or abuse of personal data by organisations at the individual's expense, and/or result in harm to the individual through facilitating identity theft or nuisance calls.

4 Hair Salons

Background

The complaint had emanated from Jiwon Hair Salon Pte Ltd (***Jiwon***), which alleged that a former employee (***Employee***) had misappropriated its customers' names and contact numbers (***Personal Data***) by accessing its customer management system (***CMS***).

To ascertain whether the Employee was indeed using the Personal Data from Jiwon's CMS, the PDPC investigated Jiwon and three other hair salons (collectively, ***4 Hair Salons***) at which the Employee had worked after leaving Jiwon. The three salons were Next@Ion Pte. Ltd., Next Hairdressing Pte. Ltd. and Initia Pte Ltd.

In the course of investigations, it was revealed that the 4 Hair Salons had no data protection policies or practices in place. This was admitted by the 4 Hair Salons.

The PDPC's Decision

Upon the conclusion of the PDPC's investigations, the 4 Hair Salons were found to have breached section 12(a) of the PDPA, which requires organisations to develop and implement policies

and practices that are necessary to meet their obligations under the PDPA.

In quoting the decision in *M Star Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15, the PDPC reiterated the need for organisations to implement data protection policies and practices. It explained that an overarching data protection will ensure a consistent minimum data protection standard across an organisation's business practices, procedures and activities.

The PDPC's Actions

In assessing the breach and the directions to be imposed on the 4 Hair Salons, the PDPC took into consideration that fact that the personal data collected by them was limited to their customers' names and contact numbers.

Accordingly, the PDPC's directions to the 4 Hair Salons were the following:

(a) to implement data protection policies to comply with the provisions of the PDPA within 60 days from the date of the PDPC's directions; and

(b) to inform the office of the Commissioner of the completion of the above direction within 1 week of implementation.

Key Takeaway

To ensure compliance with the PDPA, it is important that organisations implement data protection policies and practices in place, even when the personal data collected by them is limited, such as to customers' names and contact numbers, as in the present case.

My Digital Lock

Background

The complainant had purchased a digital lock from My Digital Lock Pte. Ltd. (***MDL***) for his home. Thereafter, the complainant was involved in a dispute with the director of MDL (***Sole Director***) concerning alleged defects in the Organisation's product. The Sole Director posted screenshots of WhatsApp messages, as well as photographs, on his personal Facebook page (***Facebook Page***) regarding the dispute with the complainant. The personal data in the WhatsApp messages comprised the complainant's contact details, namely his mobile phone number and residential address.

The complainant lodged a total of three complaints to the PDPC, the third of which is the focus of the present case. In the third complaint, the complainant referred the PDPC to a Facebook post where MDL had posted a copy of a police report that MDL's staff had made about being harassed by the complainant.

The PDPC's Findings

In the present case, the complainant's identity was disclosed because MDL had, in a Facebook post, posted a copy of a police report that MDL's staff had made against the complainant, for harassing conduct. Nonetheless, the PDPC decided to exercise its discretion under section 50(3) of the PDPA to discontinue investigations. According to the PDPC, it arrived at this decision based on the distinction drawn between the applicable common law principles that protected privacy and the operations of the PDPA. The PDPC acknowledged that although the common law does not explicitly recognise a general right to privacy, an individual's privacy is collectively protected by an existing framework of common law and statutory torts. Therefore, the PDPC held that the complainant should have sought recourse under this framework, rather than the PDPA.

Right to seclusion

In its decision, the PDPC recognised that the common law tort of privacy based on the right to seclusion has been recognised in other countries such as New Zealand (e.g. in the High Court case of *C v Holland* [2013] 3 LRC 78). According to the PDPC, intrusion upon seclusion or solitude involves an invasion of a victim's private space or affairs.

Furthermore, the PDPC noted that in Singapore, the tort of harassment is enshrined in sections 3 and 4 of the Protection from Harassment Act (Cap. 256A) (***POHA***), which abolishes the common law tort of intentional harassment and establishes that no civil proceedings shall be brought for the tort of harassment except as a statutory tort under section 14 of POHA.

In this regard, the PDPC stated that the protection offered by these statutory torts no doubt covers physical intrusions, but may extend to online activities where the communication content amounts to harassment or stalking conduct. In *Benber Dayao Yu v. Jacter Singh* [2017] 5 SLR 316 at [25], it was held that "harassing conduct on the Internet, such as those in the Web post in the

present case would be covered by sections 3 and 4 of the POHA".

Ultimately, the PDPC decided that where the true mischief is an intrusion upon one's seclusion, a civil claim before the courts is more likely to yield an effective set of relief than a complaint to the PDPC.

Furthermore, upon examining the interaction between the PDPA and (i) the right to prevent publication of private communications, and (ii) personality rights (including the right to prevent false publicity), the PDPC concluded that the Complainant's claim was for the protection of his privacy which extends beyond protection of his personal data (which involved no more than the disclosure of his name). According to the PDPC, the PDPC was not the appropriate office to investigate the Complainant's claims.

The PDPC noted that the crux of the Complainant's claim was based on the publication of alleged defamatory remarks in a police report. Accordingly, the PDPC stated that a resolution of the underlying dispute relied on the framework of laws protecting privacy rights rather than the manner in which personal data was managed by MDL. Therefore, the legal issues that raised concerned the Complainant's expectations of privacy which is protected by a framework of common law and statutory torts.

The PDPC concluded by citing Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts (as he then was) in the parliamentary debates leading to the enactment of the PDPA, that "the Bill is concerned with regulating the management and the protection of personal data. It does not govern other actions of individuals online. This would be more appropriately addressed by others laws." Thus, the PDPC was of the view that the Complainant's recourse laid in sections 3 and 4 of the POHA.

The PDPC's publications on the PDPA

Between 30 December 2017 and 20 March 2018, the PDPC released two publications on the PDPA. These are the following:

(a) Guide to Basic Data Anonymisation Techniques (published 25 January 2018); and

(b) Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy (published 1 February 2018).

Guide to Basic Data Anonymisation Techniques

On 25 January 2018, the PDPC issued a new guide entitled "Guide to Basic Data Anonymisation Techniques" (***Data Anonymisation Guide***). The Data Anonymisation Guide provides organisations with information and examples on the techniques that can be implemented to anonymise personal data.

The pararaphs below provide a non-exhaustive summary of the Data Anonymisation Guide.

Factors and Concepts to consider when carrying out Data Anonymisation

First, the Data Anonymisation Guide sets out factors that organisations can consider when selecting which anonymisation technique to use. The factors are the nature and type of personal data, the level of risk management undertaken by the organisation to protect anonymised data, and the amount of utility required from the anonymised data. In addition to these factors, the Data Anonymisation guide further sets out concepts that organisations should have in mind when deciding which anonymisation technique to use. These include the following:

(a) Purpose of anonymisation and utility: anonymisation should be carried out specifically to the purpose at hand. As the utility of the dataset reduces with anonymisation, organisations should conduct a balancing exercise to decide on the degree of the trade-off between acceptable (or expected) utility and trying to reduce the risk of any re-identification.

(b) Characteristics of anonymisation techniques: organisations should implement anonymisation techniques according to the type of dataset, as certain techniques may be more suitable for a situation than others. For instance, techniques like data perturbation work better for continuous values compared to discrete values.

(c) Inferred information: as it is possible for certain information to be inferred even after the data is anonymised, organisations should take the necessary safeguards to prevent this from happening, such as reshuffling the entire dataset.

(d) Expertise with the subject matter: organisations should engage a person with expertise in the subject matter of the data to conduct an "identifiability" assessment before and after anonymisation techniques are applied. For instance, an expert with sufficient healthcare knowledge should be engaged to assess healthcare data.

(e) Competency in anonymisation process and techniques: organisations should ensure that the anonymisation process is undertaken by persons well-versed in anonymisation techniques and principles, and engage external help if necessary.

(f) The recipient: organisations should bear in mind the recipients' expertise with the subject matter, the controls implemented to prevent the data from being shared with unauthorised parties, and the expected use of the anonymised data by the recipient.

(g) Tools: organisations should be aware of the software tools available to aid in executing anonymisation techniques, and ensure that there is human oversight and familiarity when using such tools.

Types of Data Anonymisation Techniques

Second, the Data Anonymisation Guide sets out the various anonymisation techniques that organisations can use in order to anonymise personal data. These are the following:

(a) attribute suppression: removing an entire part of data in a dataset;

(b) record suppression: removing an entire record in a dataset;

(c) character masking: changing the characters of a data value, for instance, by using a constant symbol such as "x";

(d) pseudonymisation: replacing identifying data with made up values, also known as coding;

(e) generalisation: reducing the precision of data, for instance, converting a person's age into an age range, or a precise location into a less precise location;

(f) swapping: rearranging the data in the dataset such that the individual attribute values are still represented in the dataset, but generally, do not correspond to the original records;

(g) data perturbation: modifying the values from the original dataset to ones that are slightly different;

(h) synthetic data: generating synthetic datasets directly and separately from the original data, instead of modifying the original dataset; and

(i) data aggregation: converting a dataset from a list of records to summarised values.

Proposed Methodology

Lastly, the Data Anonymisation Guide also sets out a suggested methodology that organisations could consider following when performing anonymisation. The methodology can be broadly summarised into the following steps:

(a) determine how the anonymised dataset will be released, for instance, whether public or non-public;

(b) determine the acceptable re-identification risk threshold as well as the expected utility and risk threshold intended or required;

(c) classify data attributes and remove unused data attributes;

(d) anonymise direct and indirect identifiers;

(e) determine actual risk and compare against threshold;

(f) perform more anonymisation, where necessary;

(g) evaluate the situation to determine if the utility of the anonymised dataset meets the target;

(h) determine the technical and non-technical controls required; and

(i) document the anonymisation process.

Response to Feedback on Public Consultation on Approaches to Managing Personal Data in the Digital Economy

On 1 February 2018, the PDPC published its Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy (***Response***). The Response summarised the concerns raised by respondents and set out the PDPC's position in respect of two key areas for upcoming amendments to the PDPA, namely:

(a) a Proposed Enhanced Framework for Collection, Use and Disclosure of Personal Data with new bases for organisations to collect, use and disclose personal data, namely, a '*Notification of Purpose*' Approach and a '*Legal and Business Purpose*' Approach (the latter of which will be re-named as the '*Legitimate Interests*' Approach going forward); and

(b) a Proposed Mandatory Data Breach Notification Regime.

We briefly summarise each of the above points as follows:

'Notification of Purpose' Approach

The PDPC considered that '*Notification of Purpose*' can be an appropriate basis for an organisation to collect, use and disclose personal data where it is impractical for organisations to obtain consent, and the collection, use or disclosure of personal data is not expected to have any adverse impact on individuals. Organisations that wish to rely on this basis must provide:

(a) appropriate notification of the purpose;

(b) information about how individuals may opt out, where applicable; and

(c) where feasible, organisations must allow individuals to opt out.

While the PDPC will not specify how organisations are to notify individuals, the PDPC will provide further guidance in guidelines on how organisations may allow individuals to opt out in circumstances where large volumes of personal data are instantaneously and seamlessly collected (e.g., by sensors). The PDPC will also issue guidelines to provide clarity as to what would be considered "not likely to have any adverse impact".

'Legitimate Interests' Approach

During the public consultation, the PDPC proposed organisations may collect, use or disclose personal data regardless of consent where it is necessary for a '*Legal or Business Purpose*', subject to the following conditions:

(a) it is not desirable or appropriate to obtain consent from the individual for the purpose; and

(b) the benefits to the public (or a section thereof) clearly outweighs any adverse impact or risks to the individuals.

In its Response, the PDPC stated its intention to provide for '*Legitimate Interests*' as a basis instead going forward, and will provide clarification in guidelines on the legal or business purposes which are consistent with the intent of this exception, such as prevention of fraud.

Under this proposed approach, the PDPC also intends to provide for an openness requirement as an additional safeguard to this approach, in which an organisation relying on this approach will need to disclose a document justifying its reliance, and the business contact information of a person to answer individuals' questions about such collection, use or disclosure by the organisation.

In addition, the PDPC proposed that all organisations that wish to rely on either of the approaches must:

(a) implement accountability measures, which will require a risk and impact assessment (such as a Data Protection Impact Assessment) to be conducted to determine whether benefits outweigh any foreseeable adverse impact to the individual; and

(b) put in place measures to identify and mitigate the risks when relying on such approaches to collect, use or disclose personal data.

While such accountability measures, in particular risk and impact assessments, should be documented, organisations need not make available such assessments to the public on request given their potential commercial sensitivity. That said, in the event of complaints, the PDPC reserves the right to have organisations disclose such assessments for the PDPC's consideration.

Mandatory Data Breach Notification Regime

During the public consultation, the PDPC highlighted a proposed mandatory data breach notification regime to enable the PDPC to better oversee the level of incidences and management of data breaches at the national level. The PDPC's Response is as follows:

(a) the PDPC proposed that organisations notify:

  (i) both affected individuals and the PDPC where there is a breach which is "likely to

result in significant harm or impact to the individuals to whom the information relates"; or

(ii) the PDPC only, where the breach does not pose any risk of impact or harm to affected individuals, but is of a significant scale (e.g., 500 affected individuals). In this, the PDPC will issue further guidance on assessing whether a data breach is likely to result in significant impact or harm, and its scale.

(b) the PDPC intends to retain the propose time frames for notification to individuals (i.e., "*as soon as practicable*") and to the PDPC (i.e., "*as soon as practicable, no later than 72 hours*" once the breach is assessed to be eligible for notification):

(i) in relation to the data breach notification time frame, the PDPC intends to provide for an assessment period of up to 30 days from the day the organisation first becomes aware of a suspected breach, to assess its eligibility for notification; and

(ii) where an organisation is unable to complete the assessment within 30 days, it should document the justificatory reasons for the delay as unreasonable delays without justification will be considered a breach of the mandatory notification obligation.

(c) the proposed exceptions to the requirement to notify affected individuals will be extended as follows:

(i) the law enforcement exception (i.e., if notification is likely to impede law enforcement investigations) will be extended to include investigations carried out by other government agencies authorised under the respective laws;

(ii) the technological protection exception (i.e., if the personal data was encrypted to a reasonable standard) will be broadened beyond encryption to become technology neutral. This means that organisations do not need to notify these affected individuals if they are able to demonstrate that the breach is not likely to have any significant impact or harm as a result of remedial actions taken; and

(d) where organisations need to comply with reporting requirements under other applicable laws and regulations, they must do both in accordance with the respective requirements under such applicable law and under the PDPA. However, the same format of notification required for reporting to the other sectoral regulator may be adopted for the breach notification to the PDPC. The PDPC will provide advisory guidelines on breach notifications to affected individuals in due course.

The PDPC's Response may be accessed **here**.

Call for Assessment Bodies for DP Trustmark Certification

The PDPC has called for interested companies to act as assessment bodies for its Data Protection (***DP***) Trustmark Certification scheme. To do so, companies must be located and incorporated in Singapore, must be accredited by the Singapore Accreditation Council as being in compliance with ISO/IEC 17021-1 (Conformity Assessment – requirements for bodies providing audit and certification of management systems), and must not be debarred by statutory boards and government agencies. The PDPC had earlier announced on 27 July 2017 its plans to introduce the scheme by end 2018.

The DP Trustmark Certification Scheme is intended to assist organisations in verifying their conformity to personal data protection standards and best practices. The scheme forms part of the government's efforts in furthering its digital economy strategy. This includes establishing Singapore as a trusted data hub with a strong data ecosystem that supports competition, innovation and cross-border data flows.

The key objectives of the scheme are as follows:

(a) to assist organisations in demonstrating their compliance with the PDPA and accountability;

(b) to enhance and promoting consistency in data protection standards across all sectors;

(c) to provide businesses certified under the scheme with a competitive advantage, both locally and internationally; and

(d) to improve consumer confidence in organisations' personal data management.

The PDPC's media release may be accessed **here**.

Singapore joins APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems

On 20 February 2018, with the approval of the Asia-Pacific Economic Cooperation (***APEC***) Joint Oversight Panel, Singapore became the sixth APEC economy to participate in the APEC Cross-Border Privacy Rules (***CBPR***) system (along with the USA, Mexico, Canada, Japan and the Republic of Korea). Singapore also became the second APEC economy to participate in the APEC Privacy Recognition for Processors (***PRP***) system (with the first being the USA). Singapore had submitted her Notice of Intent to participate in both systems on 26 July 2017.

The CBPR and PRP systems are multilateral certification mechanisms which ensure that certified organisations implement data protection policies in accordance with the APEC Privacy Framework. The CBPR system covers data controllers, including organisations which control data collection, holding, processing or use. The PRP system covers data processors, including organisations which process data on behalf of other organisations.

Collectively, the CBPR and PRP systems allow for a much smoother exchange of personal data amongst certified organisations in participating economies, and seek to ensure that data protection standards are maintained for consumers in the Asia-Pacific region.

The PDPC is currently developing the certification scheme for the CBPR and PRP systems. Once this scheme is implemented, organisations may start applying for certification under the relevant systems.

The factsheet released by the Ministry of Communications and Information can be accessed **here**.

Parliament passes the Cybersecurity Act

On 5 February 2018, the Cybersecurity Act 2018 (No. 9 of 2018) (***Cybersecurity Act***) was passed by Parliament. The Cybersecurity Act was first introduced in Parliament on 8 January 2018 and had its second reading on 5 February 2018. It subsequently received President's Assent on 2 March 2018. The date of commencement of the Cybersecurity Act has not been announced yet.

The Cybersecurity Act is a dedicated cybersecurity law which supports Singapore's cybercrime and cybersecurity strategy to ensure that computers, systems and data are better protected.

The paragraphs below set out a non-exhaustive summary of the Cybersecurity Act.

Key aspects

The chief executive of the Cyber Security Agency of Singapore (***CSA***) will be appointed as the Commissioner of Cybersecurity (***Cybersecurity Commissioner***) to administer and enforce the Cybersecurity Act. Amongst other things, the Cybersecurity Commissioner will have the duty to oversee the cybersecurity of computers and computer systems in Singapore, as well as establish codes of practice for implementation by owners of critical information infrastructure (***CII***).

The Cybersecurity Act includes provisions that:

(a) create a framework for the protection of designated CII against cybersecurity threats;

(b) regulate owners of CII and providers of licensable cybersecurity services in Singapore, specifically, managed security operations centre monitoring services, and penetration testing services; and

(c) authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore.

Protection of critical information infrastructure

The Cybersecurity Act establishes a framework for the protection of CII against cybersecurity threats. CII refers to a computer or computer system located wholly or partly in Singapore, that is necessary for the continuous delivery of an essential service, the loss or compromise of which will lead to a debilitating effect on the availability of the essential service in Singapore.

Under the Cybersecurity Act, essential services have been identified in the following 11 critical sectors: (a) government; (b) security and emergency; (c) healthcare; (d) telecommunications; (e) banking and finance; (f) energy; (g) water; (h) media; (i) land transport; (j) air transport; and (k) maritime.

CII are designated as such by written notice from the Cybersecurity Commissioner. Therefore, there is no need for organisations to make self-assessments as to whether their computer or computer systems fall within the criteria of a CII. CII owners are charged with various duties to ensure the cybersecurity of the CII that they own, as set out in the Cybersecurity Act. These duties include the following:

(a) a duty to provide information, i.e. to provide the Cybersecurity Commissioner with information on the technical architecture of the CII;

(b) a duty to comply with codes of practice, standards of performance or written directions in relation to the CII as may be issued by the Cybersecurity Commissioner;

(c) a duty to notify the Cybersecurity Commissioner of any change in ownership of the CII;

(d) a duty to report incidents, i.e. to notify the Cybersecurity Commissioner of any prescribed cybersecurity incidents relating to the CII;

(e) a duty to conduct audits, i.e. to cause regular audits of the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance, which are to be carried out by an auditor approved or appointed by the Cybersecurity Commissioner;

(f) a duty to conduct risk assessments, i.e. to regularly conduct risk assessments of the CII as required by the Cybersecurity Commissioner; and

(g) a duty to participate in cybersecurity exercises as required by the Cybersecurity Commissioner.

Non-compliance with the relevant provisions under the Cybersecurity Act may constitute an offence, for which a fine or a term of imprisonment may be imposed.

Regulation of providers of licensable cybersecurity services

Under the Cybersecurity Act, no person may engage in the business of providing any licensable cybersecurity services to other persons, except under and in accordance with a licence granted or renewed. Currently, two categories of services i.e. penetration testing services and managed security operations centre monitoring services, have been identified as licensable cybersecurity services.

An application for the grant or renewal of a license must be made in the prescribed form and manner as set out in the Cybersecurity Act. If satisfied that the service provider is no longer fit and proper, among other factors, the Cybersecurity Commissioner may revoke or suspend a license that has been granted. The service provider will be required to keep records on the cybersecurity services it has provided to its clients, including details of the employee providing the service, for not less than 3 years.

Powers of the Cybersecurity Commissioner to respond to cybersecurity threats and incidents

In response to a cybersecurity threat or incident, the Cybersecurity Commissioner and appointed officers may exercise investigatory powers and authorise the taking of emergency cybersecurity measures. With respect to investigations, the powers which can be exercised against persons affected by the cybersecurity threat or incident include the following:

(a) requiring the person to attend at a specified place and time to answer questions or to provide a signed statement concerning the cybersecurity threat or incident;

(b) requiring the person to produce any record or document, or provide any relevant information to the incident response officer;

(c) inspect, copy or take extracts from such records or documents; and

(d) examining orally the person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident.

For 'serious' cybersecurity threats or incidents, i.e., those which satisfy the severity threshold specified in section 20(3) of the Cybersecurity Act, an additional set of more extensive powers can be taken. This includes entering premises where the affected computer or computer system is reasonably suspected to be located.

Lastly, the Cybersecurity Act confers on the Minister for Communications and Information (***Minister***) the power to take certain action in response to cybersecurity incidents that threaten

the national security, defence, economy, foreign relations, public health, order or safety, or any of the essential services of Singapore.

The Minister may, by issuing a certificate, authorise any person or organisation to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service, or any class of computers or computer services. The Cybersecurity Act will apply concurrently with other laws and regulations enacted in Singapore, including existing sectoral laws.

AUSTRALIA

Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 comes into effect

On 22 February 2018, Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 came into effect, establishing the Notifiable Data Breaches (***NDB***) scheme under Part IIIC of the Privacy Act 1988 (***Privacy Act***).

Under the NDB scheme, the Australian Government agencies and various organisations have to notify the Office of the Australian Information Commissioner (***OAIC***), as well as affected individuals, of data breaches occurring after 22 February 2018 that are likely to result in serious harm.

If an organisation suspects that it may have experienced an eligible data breach, it must quickly assess the situation to decide whether or not there has been an eligible data breach. The requirement for an assessment is triggered if an organisation is aware that there are reasonable grounds to suspect that there may have been a serious breach. An organisation must take all reasonable steps to complete the assessment within 30 calendar days after the day the organisation became aware of the grounds (or information) that caused it to suspect an eligible data breach.

In addition, in order to provide guidance to organisations, the OAIC has published the "Data Breach Preparation and Response" guide (***Data Breach Guide***). The Data Breach Guide sets out, amongst other things, the steps which organisations should take in responding to data breaches, a non-exhaustive list of 'relevant matters' which may assist organisations to assess the likelihood of serious harm, and a framework for a data response plan.

On 16 March 2018, it was reported that Australian shipping company, Svizter Australia Pty Ltd (***Svizter***) had notified the OAIC of a data breach under the NDB scheme. According to reports, this was the first publicised data breach notification under the NDB scheme.

In its notification to the OAIC, Svizter revealed that approximately 60,000 emails from email accounts in its finance, payroll and operations divisions were auto-forwarded to two external email accounts, resulting in unauthorised disclosure of information. The auto-forwarded emails contained employee information such as personal tax file numbers, details of next of kin, and superannuation account information.

According to reports, the OAIC has received over 30 data breach notifications brought under the NDB scheme since it came into effect.

The media release on the NDB scheme can be accessed **here**, and the Data Breach Guide can be accessed **here**.

HONG KONG

Hong Kong Privacy Commissioner for Personal Data issues revised Guidance Note on Election Activities

In December 2017, the Hong Kong Privacy Commissioner for Personal Data (***PCPD***) issued the Guidance on Election Activities for Candidates, Government Departments, Public Opinion Research Organisations and Members of the Public (***Election Activities Guidance***).

The Election Activities Guidance supersedes the previous Guidance on Electioneering Activities issued in August 2015. While the latter only provided guidance to election candidates, the former is of a significantly wider scope that extends to the other eponymous stakeholders. The issuance of additional guidance was a response to the substantial amount of electoral complaints received by the PCPD in 2017, which numbered around 2,000.

The Election Activities Guidance provides practical guidance to electoral stakeholders, and it contains case studies discussing past complaints and/or contraventions, and the remedial action taken.

The media statement released by the PCPD on 11 January 2018 can be assessed **here**. The Election Activities Guidance, and the accompanying infographic, can be accessed **here** and **here** respectively.

CANADA

Parliamentary committee releases report on the review of the Personal Information Protection and Electronic Documents Act

On 28 February 2018, a report entitled "*Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act*" was tabled in the Canadian House of Commons by the Standing Committee on Access to Information, Privacy and Ethics (***Committee***).

The Committee's report sets out 19 recommendations to the Government of Canada in respect of updates which should be made to the Canadian Personal Information Protection and Electronic Documents Act (***PIPEDA***) and measures which should be taken to improve the protection of Canadian's privacy with regard to their relation with private sector organisations. A non-exhaustive list of the recommendations is as follows:

(a) consent should remain the core element of the privacy regime, but when possible or necessary, it should be enhanced and clarified by additional means;

(b) PIPEDA should be amended to explicitly provide for opt-in consent as the default for any use of personal information for secondary purposes, with a view to also implementing a default opt-in system regardless of purpose;

(c) the implementation of measures to improve algorithmic transparency should be considered;

(d) the issue of revocation of consent should be studied further in order to clarify the form of revocation required and its legal and practical implications;

(e) the Regulations Specifying Publicly Available Information should be modernised in order to take into account situations in which individuals post personal information on a public website and in order to make the Regulations technology-neutral;

(f) amendments to PIPEDA in respect of clarifying the terms under which personal information can be used to satisfy legitimate business interests should be considered;

(g) the best ways of protecting depersonalised data should be examined further;

(h) the term "fraud" in paragraph 7(3)(d.2) of PIPEDA should be replaced with "financial crime" (and a definition should be proposed accordingly);

(i) specific rules of consent for minors, as well as regulations governing the collection, use and disclosure of minors' personal information, should be considered for implementation;

(j) PIPEDA should be amended to provide for a right to data portability;

(k) a framework for the right to erasure based on the model developed by the EU should be considered for implementation in PIPEDA;

(l) a framework for the right to de-indexing should be considered for implementation in PIPEDA;

(m) amendments to PIPEDA to strengthen and clarify organisations' obligations with respect to the destruction of personal information should be considered;

(n) privacy by design (including its seven foundational principles, where possible) should be a central tenet of PIPEDA;

(o) PIPEDA should be amended to provide the Privacy Commissioner with enforcement powers such as the power to make orders and impose fines for non-compliance, and other broad audit powers such as the ability to choose which complaints to investigate;

(p) the Government of Canada should work with its EU counterparts to determine what would constitute adequacy status for PIPEDA in the context of the new General Data Protection Regulation (***GDPR***);

(q) the Government of Canada should determine what, if any, changes to PIPEDA will be required in order to maintain its adequacy status under the GDPR, and if it is determined that the changes required to maintain adequacy status are not in the Canadian interest, mechanisms to allow for the

seamless transfer of data between Canada and the EU should be created; and

(r) the Government of Canada should work with the provinces and territories to make sure that all relevant jurisdictions are aware of what would be required for adequacy status to be granted by the EU.

A response from the Government of Canada has been requested by the Committee. Presently, no other information is available as at the time of writing.

Office of the Information and Privacy Commissioner for British Columbia releases guidance on GDPR

In March 2018, the British Columbia (***BC***) Information & Privacy Commissioner (***IPC***) published a guidance document to help organisations in BC determine whether they are subject to the EU GDPR and how to comply with both the Personal Information Protection Act (***PIPA***) and GDPR (***Guidance Document***). The PIPA applies to all private sector organisations in British Columbia and sets out how those organisations may collect, use and disclose personal information.

According to the Guidance Document, the extensive reach of the GDPR presents global compliance challenges for organisations in BC. The GDPR requires private sector organisations to comply with data protection requirements when they process the personal information of individuals located in the EU. Therefore, organisations covered by the PIPA will also need to comply with the GDPR if:

(a) they have an established presence in the EU;

(b) they offer goods and services to individuals in the EU; or

(c) they monitor the behaviour of individuals in the EU.

Although largely similar, there are some aspects of the GDPR that have no equivalent in the PIPA, and hence additional compliance effort will be required in those areas. The Guidance Document provides an overview of how the following areas are dealt with by the GDPR and PIPA:

(a) Personal Information;

(b) Consent;

(c) Individual Rights;

(d) Mandatory Breach Notification;

(e) Cross-Border Transfers of Personal Information; and

(f) Data Governance Obligations.

(a) Personal Information

Both the GDPR and PIPA recognise personal information as information about an identifiable individual. However, the GDPR goes a step further to set out special categories of particularly sensitive personal data that is subject to additional protections i.e. data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. The GDPR provides specific restrictions for processing special personal data. Processing is only allowed under certain circumstances, such as if the data subject has given explicit consent for specified purposes.

(b) Consent

The GDPR imposes more onerous consent requirements for information processing than the PIPA. Under the GDPR, the concept of "opt-out consent" is prohibited, and specific consent is required for any new data processing, unless the subsequent processing is so similar to those already consented to that it would be expected by the data subject. In addition, the GDPR requires explicit consent for the processing of special categories of data, for automated individual decision-making, including profiling, and for international data transfers. Furthermore, the GDPR has more specific protections for children. For e.g. the processing of personal data of any child under the age of 16 requires parental consent, and member states can opt to reduce the age to 13, 14 or 15.

In contrast, under the PIPA, both "opt-out consent" and "implicit consent" are recognised. There is a further requirement under the PIPA that any collection, use or disclosure of personal information must be reasonable. This means that a reasonable person, knowing the purpose for collection and the surrounding circumstances, would consider the purpose to be appropriate. What is reasonable depends on the sensitivity and volume of personal information being collected, the purpose and circumstances of collection, how the organization handles the information, and how

an organization plans to use and disclose the information. With regard to children, the PIPA does not specify a minimum age for consent, and a minor may consent if they are capable of understanding what they are consenting to.

(c) Individual Rights

Both the GDPR and PIPA grant individuals the right to be informed, the right to access one's personal data and the right to rectification of personal information. However, the GDPR grants individuals additional rights that are not provided by the PIPA, which include:

(i) the right to erasure;

(ii) the right to restriction of processing;

(iii) the right to data portability;

(iv) the right to information about the logic involved in automated decision-making;

(v) the right not to be subject to automated decision making; and

(vi) the right to object to data processing activities.

Thus, organisations in BC that are subjected to the GDPR need to take heed of these additional rights.

(d) Mandatory Breach Notification

Unlike the GDPR, the PIPA does not require a mandatory breach notification. Thus, organisations in BC who are subjected to the GDPR must be aware of the GDPR's mandatory breach notification requirement, which requires individuals affected by a data breach to be notified by the controller within 72 hours of discovering the breach. Breaches affecting the rights and freedoms of individuals require immediate notification, without undue delay. The notification must include full details of the breach, the approximate number of individuals affected, potential consequences, and ways to mitigate any harm.

(e) Cross-Border Transfers of Personal Information

The GDPR aims to facilitate the cross-border transfers of personal data in limited circumstances which include:

(i) to countries, territories, or sectors of a country providing an adequate level of data protection;

(ii) where standard data protection clauses or binding corporate rules apply; or

(iii) where approved codes of conduct or certification are in place.

In contrast, the PIPA does not explicitly address cross-border transfers of personal information. Currently, the PIPA applies the same requirement of "reasonable security measures" to be taken against unauthorised access or disclosure both within and outside of BC. Thus, organisations in BC that are subjected to the GDPR need to ensure that they adhere to the GDPR's more specific requirements for cross-border transfers.

(f) Data Governance Obligations

The GDPR requires all organisations to install a number of accountability measures (Privacy by Design) and show that they take data governance seriously, including privacy impact assessments (***PIAs***), audits, policy reviews, activity reports, and in some cases appointing a Data Protection Officer. The PIPA does not require private sector organisations in BC to complete PIAs. Nonetheless, the IPC has nonetheless encouraged them to do so. The IPC has also recommended private sector organisations to put in place a privacy management programme.

The Guidance Document can be accessed **here**.

UNITED KINGDOM

ICO: WhatsApp signs public commitment not to share personal data with Facebook until data protection concerns are addressed

On 14 March 2018, the UK Information Commissioner's Office (***ICO***) announced that WhatsApp has signed an 'undertaking' wherein they provided a voluntary public commitment (***Commitment***) not to share personal data with companies in the Facebook group (collectively, ***Facebook***) until WhatsApp can satisfy the requirements of the upcoming GDPR.

This follows the completion of the ICO's investigation on whether WhatsApp could legally share users' data with Facebook pursuant to its updated Terms and Conditions and Privacy

Policy, to the extent that Facebook may use such data to help operate, provide, improve, understand, customise, support, and market WhatsApp's services and Facebook's own offerings, including improving users' experiences within Facebook's services such as making product suggestions and showing relevant advertisements and offers.

The ICO's investigation found that:

(a) WhatsApp had not identified a lawful basis of processing for any such sharing of personal data;

(b) WhatsApp failed to provide adequate fair processing information to users in relation to any such sharing of personal data;

(c) in relation to existing users, such sharing would involve the processing of personal data for a purpose that is incompatible with the purpose for which such data was obtained; and

(d) if WhatsApp had shared the data, it would have been in contravention of the UK Data Protection Act 1998.

For avoidance of doubt, WhatsApp stated that it did not share any UK user data with Facebook, other than in Facebook's capacity as a data processor of WhatsApp.

WhatsApp's Commitment provides that it will not transfer any EU user data to any Facebook company on a controller-to-controller basis for any purpose prior to the GDPR coming into force. After the GDPR comes into force, WhatsApp shall commence the sharing of such user data for safety and security purposes or any other purposes (including the purposes of using such data to improve Facebook's products and advertising) in accordance with the GDPR's requirements.

Information Commissioner's Office publishes detailed Guidance on Documentation

On 30 January 2018, the ICO published a new guidance document (***Documentation Guidance***) to assist UK organisations in understanding the importance of documenting their processing activities, and how to document these activities effectively in line with the GDPR. Under the GDPR, records must be kept on processing purposes, data sharing, and retention. Documenting this information is linked to the principle of accountability and helps organisations

The following paragraphs provide a non-exhaustive summary of the Documentation Guidance.

Why is documentation important?
The Documentation Guidance explains that documentation helps organisations to comply with the GDPR in the following aspects:

(a) drafting of the organisation's privacy notice;

(b) responding to access requests from individuals;

(c) taking stock of the organisation's processing activities;

(d) improving data governance by assuring data quality, completeness and provenance; and

(e) increasing business efficiency by developing more effective and streamlined business processes.

Who needs to document their processing activities?

The Documentation Guidance states that while both controllers and processors have their own documentation obligations, controllers need to keep more extensive records than processors. Furthermore, organisations with 250 or more employees must document all their processing activities.

The Documentation Guidance further highlights that the GDPR provides a limited exemption for small and medium-sized organisations. These organisations only need to document processing activities that:

(a) are not occasional (for e.g. are more than just a one-off occurrence or something you do rarely); or

(b) are likely to result in a risk to the rights and freedoms of individuals; or

(c) involve special category data or criminal conviction and offences data.

What needs to be documented under the GDPR?

The Documentation Guidance states that organisations that are controllers need to document the following:

(a) the organisation's name and contact details;

(b) if applicable, the name and contact details of:

(i) the data protection officer;

(ii) any joint controllers;

(iii) the representative;

(c) the purposes of the processing;

(d) the categories of personal data processed;

(e) the categories of recipients of personal data;

(f) if applicable, the name of any third countries or international organisations that personal data is transferred to;

(g) if applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations;

(h) if possible, the retention schedules for the different categories of personal data; and

(i) if possible, a general description of technical and organisational security measures undertaken.

The Documentation Guidance further states that organisations that are processors need to document the following:

(a) the organisation's name and contact details;

(b) if applicable, the name and contact details of:

(i) the data protection officer;

(ii) each controller on whose behalf the processor is acting for;

(iii) the representative;

(iv) each controller's representative;

(c) the categories of processing carried out on behalf of each controller;

(d) if applicable, the name of any third countries or international organisations that personal data is transferred to;

(e) if applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations; and

(f) if applicable, a general description of technical and organisational security measures undertaken.

In addition, the Documentation Guidance explains that documenting information will be helpful in the following areas:

(a) controller-processor contracts – if a controller uses a processor to carry out a particular processing activity, a written contract must be in place. Both controllers and processors can use their record of processing activities to link to the relevant contract documents;

(b) the location where personal data is stored – this helps organisations to locate information more easily when an individual exercises the right of access to their personal data (e.g. manual records held in HR files, electronic records held on cloud servers or electronic records held by data processors); and

(c) data protection impact assessments – a data protection impact assessment (***DPIA***) is needed where there is a high risk to individuals' rights and freedoms, particularly when new technologies are involved. A record of processing activities will help to identify when a DPIA is required.

How should processing activities be documented?

The Documentation Guidance suggests that organisations conduct an information audit or data-mapping exercise to clarify what personal data the organisation holds, and where these are located. Engaging personnel across the organisation is crucial to ensure that nothing is left out during the mapping process. Buy-in from senior management is equally important to ensure that the documentation exercise is supported and well resourced. There are several methods to document processing activities:

(a) devise a questionnaire;

(b) meet directly with key business functions; and

(c) locate and review policies, procedures, contract and agreements.

EUROPEAN UNION

European Commission publishes guidance on direct application of the GDPR

On 24 January 2018, the European Commission published a new set of guidance on the direct application of the GDPR, titled "Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018" (***GDPR Guidance***).

The GDPR Guidance outlines what the European Commission, national data protection authorities and national administrations should do to facilitate a direct and smooth application of the GDPR across the EU. More specifically, the GDPR Guidance seeks to:

(a) recap the main innovations and opportunities opened up by the new EU data protection legislation;

(b) take stock of the preparatory work undertaken so far at EU level;

(c) outline the responsibilities of the European Commission, national data protection authorities and national administrations in bringing the preparation to a successful completion; and

(d) set out measures that the European Commission intended to take in the coming months.

The following paragraphs provide a non-exhaustive summary of the GDPR Guidance.

National Data Protection Authorities

According to the GDPR Guidance, full commitment of the national data protection authorities is crucial in ensuring the successful implementation of the GDPR. In particular, the GDPR Guidance highlights that it is contrary to the Treaties for Member States to have national measures which create obstacles to the direct applicability of the GDPR, and jeopardise the simultaneous and uniform application of the GDPR across the EU.

In addition, Member States are encouraged to fulfil their legal obligation to provide their national data protection authority with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of their powers. Member States are to provide the above support systems to their respective national data protection authorities to ensure the establishment of fully independent and competent supervisory authorities in each Member State.

The GDPR codifies the requirement of any data protection authority to act completely independently. It strengthens the national data protection authorities' independence and provides them with uniform powers across the EU to deal effectively with complaints, carry out effective investigations, take binding decisions and impose effective and dissuasive sanctions.

Businesses and Organisations that Process Personal Data

The GDPR Guidance further explains that operators whose core business is data processing and/or dealing with sensitive data need to be acutely aware of any new obligations that arise under the GDPR. These operators will most probably have to appoint a data protection officer, conduct a data protection impact assessment and notify data breaches if there is a risk to the rights and freedoms of individuals. Businesses and other organisations processing data will also be able to take advantage of the new tools provided for in the GDPR as an element to demonstrate compliance, such as codes of conduct and certification mechanisms.

Educating Stakeholders

According to the GDPR Guidance, the success of the GDPR rests on proper awareness of all those affected by the new rules (the business community and other organisations processing data, the public sector and citizens). Data protection authorities have started informing stakeholders in line with the specific national approach. For example, local and regional seminars are held with public administrations; workshops are carried out with different business sectors; and specific training programmes are conducted for data protection officers.

Next Steps

As stated in the GDPR Guidance, the European Commission will aim to make available practical guidance materials to help businesses, in particular SMEs and public authorities and the public to comply with the new data protection rules. The guidance takes the form of a practical

online tool available in all EU languages. It comprises questions and answers selected based on feedback received from stakeholders with practical examples and links to various sources of information.

The GDPR Guidance can be accessed **here**.

The Drew & Napier Telecommunications, Media and Technology Team

For more information on the TMT Practice Group, please click **here**.

Lim Chong Kin • Director and Head of TMT Practice Group

Chong Kin practices corporate and commercial law with strong emphasis in the specialist areas of TMT law and competition law. He regularly advises on regulatory, licensing, competition and market access issues. Apart from his expertise in drafting "first-of-its-kind" competition legislation, Chong Kin also has broad experience in corporate and commercial transactions including mergers and acquisitions. He is widely regarded as a pioneer in competition practice in Singapore and the leading practitioner on TMT and regulatory work. Chong Kin has won plaudits for his '*good knowledge of the telecommunications industry and consistently excellent service*' (***Asia Pacific Legal 500***), and '*thoroughly [understanding] the requirements of an international company seeking to do business in Singapore and provides excellent practical, pithy and timely advice,*' (***Chambers Asia 2018***: Band 1 for TMT); and has been endorsed for his excellence in regulatory work and competition matters: ***Practical Law Company's Which Lawyer Survey 2011/2012; Who's Who Legal Data: Telecoms & Media 2017*** and ***Who's Who Legal: Competition 2017***. ***Asialaw Profiles 2018*** lists Chong Kin as a market-leading lawyer in IT, Telco & Media.

Tel: +65 6531 4110 • Fax: +65 6535 4864 • Email: **chongkin.lim@drewnapier.com**

Charmian Aw • Director

Charmian is a Director in Drew & Napier's TMT Practice Group. She is frequently involved in advising companies on a wide range of corporate, commercial and regulatory issues in Singapore. Charmian has also been actively involved in assisting companies on Singapore data protection law compliance, including reviewing contractual agreements and policies, conducting trainings and audits, as well as advising on enforcement issues relating to security, access, monitoring, and data breaches. Charmian is "recommended for corporate-related TMT and data privacy work" by ***The Asia Pacific Legal 500 2016***, and she is recognised by ***Who's Who Legal 2017*** as an expert in Data: Telecoms & Media. ***Asialaw Profiles 2018*** notes, "Charmian Aw is 'equipped, proactive and approachable'". In 2015, she was listed as one of 40 bright legal minds and influential lawyers under the age of 40 by ***Asian Legal Business*** and ***Singapore Business Review*** respectively. Charmian is a Certified Information Privacy Professional for Europe, the United States, and Asia (CIPP/E, CIPP/US, CIPP/A). She is also a co-chair of the International Association of Privacy Professionals (IAPP) KnowledgeNet chapter in Singapore.

Tel: +65 6531 2235 • Fax: +65 6535 4864 • Email: **charmian.aw@drewnapier.com**

Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval. Drew & Napier LLC accepts no liability for, and does not guarantee the accuracy of information or opinion contained in this publication. This publication covers a wide range of topics and is not intended to be a comprehensive study of the subjects covered nor is it intended to provide legal advice. It should not be treated as a substitute for specific advice on specific situations.