DREW & NAPIER

DATA PROTECTION QUARTERLY UPDATE

JANUARY 2018

In this issue

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 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 six most recent enforcement decisions issued by the Personal Data Protection Commission (***PDPC***) at the time of writing, and examine several of the PDPC's latest publications, including its General Data Protection Regulation (***GDPR***) Factsheet for Organisations. We have also prepared a write-up that provides a snapshot of the GDPR and its key provisions, with a focus on how it might impact your business in Singapore. Please refer to the **Annex** of this Quarterly Update for more details.

Additionally, we also examine the Cybersecurity Bill and the draft Healthcare Services Bill. The Cybersecurity Bill was introduced in Parliament on 8 January 2018. The draft Healthcare Services Bill was released by the Ministry of Health on 5 January 2018, together with a public consultation paper seeking comments on the same.

On the global front, we also analyse the emergence of new regulatory instruments and frameworks in several jurisdictions including Australia, the United Kingdom as well as the European Union.

We hope that this new publication will be useful for 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

PDPC issues six grounds of decisions

Between 11 October 2017 and 8 January 2018, the PDPC issued enforcement decisions against six organisations in relation to the data protection obligations under the Personal Data Protection Act 2012 (No. 26 of 2012) (***PDPA***). These organisations are as follows:

(a) Aviva Ltd (***Aviva***) (issued 11 October 2017).

(b) M Stars Movers & Logistics Specialist Pte. Ltd. (***M Stars Movers***) (issued 15 November 2017).

(c) BHG (Singapore) Pte. Ltd. (***BHG***) (issued 15 November 2017).

(d) Social Metric Pte. Ltd. (***Social Metric***) (issued 27 November 2017).

(e) ComGateway (S) Pte. Ltd. (***ComGateway***) (issued 29 December 2017).

(f) Credit Counselling Singapore (***Credit Counselling SG***) (issued 29 December 2017).

Aviva

Background

The PDPC was notified that Aviva had mistakenly mailed to one of its policyholders (***First Policyholder***) documents meant for another policyholder (***Second Policyholder***). The First Policyholder had received two different envelopes from Aviva. In each of the envelopes, apart from the First Policyholder's documents, there was another document meant for the Second Policyholder. The document disclosed various personal details such as the Second Policyholder's full name, NRIC number and CPF account number, as well as the Second Policyholder's dependent's full name and relationship to the Second Policyholder (***Personal Data***). As a result, a family member of the First Policyholder lodged a complaint with the PDPC on 8 November 2016.

The PDPC's Decision

Upon conclusion of the PDPC's investigations, Aviva was found to be in breach of its obligations under section 24 of the PDPA to take reasonable security arrangements to protect the personal data in its possession or under its control, for the reasons set out below:

(a) Personal data of a sensitive nature should be safeguarded by a higher level of protection

The PDPC found that sensitive personal data of the Second Policyholder and the Second Policyholder's dependent, such as the CPF account number of the former and the FIN of the latter, had been disclosed to the First Policyholder. The PDPC also observed that if information such as the Second Policyholder's medical information and credit card details had been pre-filled into one of the documents, these would also have been inadvertently disclosed to the First Policyholder.

Such sensitive personal data required a higher standard of protection, or particular care in its processing and mailing, which Aviva had not met.

(b) The unauthorised disclosure of the Personal Data was the result of Aviva's failure to make reasonable security agreements

The PDPC found that the incident was not caused by an isolated case of human error. Rather, Aviva had failed to make reasonable security arrangements to protect the sensitive personal data it handled, since it had extremely weak internal work process controls.

First, Aviva faced the systemic problem of having Standard Operating Procedures (***SOPs***) that were ineffective in protecting personal data. There were no second-level checks by the team leader on the follow-up letters prepared by the processing staff. The team leader would only conduct a full audit on a staff member for one week when alerted to any errors of that particular staff. While it is not mandatory for organisations to do additional checks in all cases, the PDPC took the view that Aviva should have done so because it is a well-established multinational insurance organisation which handles large amounts of sensitive client personal data on a daily basis. The fact that this error was made by a staff with ten years of experience in enveloping work also indicated that a lack of additional checks would not be reasonable, since a less experienced staff would have a greater chance of making a similar mistake.

Second, while Aviva had a general data protection policy, the PDPC noted that the policy did not provide specific and practical guidance for the processing staff with regard to their specific duties. While it indicated basic dos and don'ts, this was insufficient in light of the fact that data protection policies could also serve as an administrative security measure to protect personal data.

The PDPC's Actions

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

(a) The Personal Data disclosed was of a sensitive nature, such as the Second Policyholder's NRIC number.

(b) Aviva is in the business of handling large volumes of personal data, the disclosure of which may cause exceptional damage, injury or hardship to the affected individuals.

(c) Aviva had cooperated fully with the PDPC's investigation and was forthcoming in admitting its mistake.

(d) Aviva had notified, apologised and provided shopping vouchers to the affected victim (i.e. the Second Policyholder), and had also retrieved the wrongly delivered documents from the First Policyholder.

(e) The unauthorised disclosure of Personal Data was limited to possibly three individuals (the First Policyholder and the First Policyholder's nuclear family).

(f) There was no evidence indicating that the Second Policyholder had suffered any actual loss or damage from this incident.

Based on the above factors, the PDPC directed Aviva to pay a financial penalty of S$6,000 within 30 days from the date of the PDPC's direction. The PDPC also noted that Aviva had taken various remedial actions. For example, it had updated the SOPs to include various steps such as requiring each team leader to check around 10% of envelopes each day. While the PDPC did not provide any opinion on the revised SOPs, it stated that Aviva could consider a graduated approach to sample checking, under which the work of more senior staff members with relatively few records of mistakes could be subject to more moderate checks.

Key takeaway

Organisations should be aware of the sensitivity and amount of personal data which they handle when formulating security arrangements to ensure compliance with section 24 of the PDPA. To facilitate compliance with data protection obligations, organisations should also implement adequate checks and provide practical guidance for employees.

M Stars Movers

Background

In December 2016, the complainant engaged M Stars Movers' professional moving services. To do so, she voluntarily provided her name, mobile number and residential addresses for the pick-up and delivery of the items. She was dissatisfied with the service and left a negative review in a public post on M Stars Movers' Facebook page. In its public reply to her, M Stars Movers identified the Complainant by her English name, surname and residential address (***Personal Data***). It also informed her that she would receive her S$100 deposit—which she had complained about—once she returned the carton boxes that M Stars Movers had provided for the moving service. In response to the complainant's private Facebook message requesting the immediate removal of her residential address from the public page, M Stars Movers refused to do so until it was advised to do so by the PDPC.

The PDPC's Decision

Upon conclusion of the PDPC's investigations, M Stars Movers was found to have disclosed the complainant's personal data without consent or authorisation, and failed to comply with its obligations under sections 11 and 12 of the PDPA.

(a) <u>Whether M Stars Movers had disclosed the complainant's personal data without consent or authorisation</u>

The PDPC noted that the complainant had provided the Personal Data to M Stars Movers for the purpose of moving her belongings to her new home. She had not consented to, nor could she be deemed to have consented to, the disclosure of such data on M Stars Movers' public Facebook page. It was not within her reasonable contemplation that the Personal Data would be publicly disclosed on the Facebook page.

While M Stars Movers claimed the disclosure was done to confirm the Complainant's identity, this was not accepted by the PDPC as a legitimate reason for disclosing the Personal Data to third parties. The PDPC also found that it would not be objectively reasonable for M Stars Movers to disclose personal data in response to the Complainant's allegations, since there was no link between the disclosure of the Personal Data and the Complainant's allegations or M Stars Movers' explanations. Given this, the PDPC regarded the disclosure as objectively disproportionate. It further observed that while a civil dispute clearly existed, the disclosure was not made in the context of an investigation of such a dispute, which would constitute an exception to consent. Rather, it was most likely made for convenience alone, making it unreasonable.

M Stars Movers also admitted its lack of awareness of the PDPA, but the PDPC stated that ignorance of the law was no excuse and observed that the PDPA had been in effect since 2 July 2014.

(b) Whether M Stars Movers had complied with its obligations under sections 11 and 12 of the PDPA

M Stars Movers admitted that as a result of its lack of awareness of the PDPA, it had not implemented any data protection policies or appointed a Data Protection Officer (***DPO***) at the material time. Hence, it was in breach of sections 11 and 12 of the PDPA.

The PDPC's Actions

In assessing the breach and the directions to be imposed on M Stars Movers, the PDPC took the following factors into consideration:

(a) The Personal Data only consisted of the Complainant's name and residential address.

(b) M Stars Movers had breached the PDPA due to its lack of awareness of its obligations under the PDPA.

Based on the above factors, the PDPC's directions to M Stars Movers were to:

(a) Put in place a data protection policy and internal guidelines to comply with the PDPA within 60 days from the date of the PDPC's directions.

(b) Appoint a data protection officer *(**DPO**)* within 30 days from the date of the PDPC's directions.

(c) Inform the PDPC of the completion of each of the above directions within 1 week of implementation.

Key takeaway

Each organisation should have a designated DPO, as well as a data protection policy that has both general principles and specific procedures. For organisations with a social media or online presence, the policies and procedures that the organisations put in place must deal with the risks of disclosing personal data in an online environment.

BHG

Background

On 26 December 2016, the complainant and another customer (***Customer V***) both registered for a BHG loyalty card account at the same BHG store. This involved the usage of an electronic registration form on tablets which had technical issues. The complainant had first keyed in her details into one of the tablets, but used a physical registration form after this proved unsuccessful. However, the complainant's mobile phone number and email address continued to be displayed in the online form, which Customer V then filled in. Hence, Customer V's account was linked to the complainant's mobile phone number and email address.

Since the default login ID for a BHG loyalty card account was a customer's phone number, the Complainant was unable to log into her account on the first try. After obtaining a password reset, the Complainant managed to log into what she thought was her account, but realised that the account contained the personal data of Customer V, such as his income group and residential address (***Personal Data***). The only data that belonged to her were the mobile phone number and email address. The complainant alerted BHG and the PDPC about the incident.

The PDPC's Decision

Upon conclusion of the PDPC's investigations, BHG found to be not in breach of its obligations under section 24 of the PDPA to take reasonable security arrangements to protect the personal data

in its possession or under its control, for the reasons set out below:

(a) BHG had implemented security arrangements to prevent unauthorised access to the Personal Data

First, BHG had implemented security arrangements to prevent unauthorised access to the Personal Data during the registration process. For example, the screen on the electronic tablet was programmed to automatically "refresh" once the electronic registration form was successfully submitted. BHG employees were also supposed to manually "refresh" the system before allowing another customer to use the form. Additionally, if the form experienced 30 seconds of inactivity, all personal data keyed in would be deleted.

Second, BHG had implemented security arrangements to prevent unauthorised access to the Personal Data when customers accessed their online accounts. The login credentials were set as a customer's mobile phone number (user ID) and membership card account number (password). Furthermore, a customer would only be able to obtain a password reset upon providing the customer's mobile phone number and email address.

(b) The unauthorised access was caused by a confluence of events and circumstances that would have been difficult to foresee

The PDPC found that the unauthorised access occurred as a result of the following events:

(i) The complainant's electronic registration could not be completed, meaning that the Complainant's data was not automatically cleared from the electronic registration form.

(ii) The employee in charge of performing a manual "refresh" was not successful in doing so. The assistant retail manager had not performed a check on this occasion as the employee had done it properly when the assistant retail manager had checked earlier that day, and the service counter was very busy.

(iii) Customer V did not alert the BHG employees but left the Complainant's contact details in the form he was filling up.

(iv) Only the complainant's email address and mobile telephone number were included in Customer V's registration form, but not the rest of her personal data. However, these were the only details required for the complainant's access to the personal data.

The PDPC observed that various arrangements such as the aforementioned automatic "refresh", the manual "refresh" and the supervisory checks by the assistant retail manager would have individually prevented the unauthorised access. However, each of these arrangements had failed individually. There was no systemic problem that caused this incident.

The PDPC also noted that BHG had undertaken various remedial actions, such as creating new accounts for both the complainant and Customer V, scheduling all refresher data protection training for all customer service counter staff and scheduling its IT personnel to carry out extensive checks on all electronic tablets used.

The PDPC's Actions

The PDPC did not issue any directions, since it found that BHG had already implemented security arrangements of a reasonable standard to protect the personal data in its possession and under its control. In addition, the remedial actions which BHG had undertaken sufficiently addressed the residual harm caused by the incident.

Key takeaway

The PDPA does not require an organisation to provide failproof methods for the protection of personal data in its possession or under its control. In other words, if the organisation can prove that it had taken reasonable steps to protect the data, the PDPA is not automatically breached upon the occurrence of a data leak.

Social Metric

Background

Social Metric had produced nine webpages (***Webpages***) for social media contests that it conducted for and on behalf of its clients, which could be accessed from its website (***Website***). The Webpages contained tables listing out the personal particulars of various individuals, such as email addresses and employment details. This was done for internal administrative and client use. Approximately 155 of these individuals were children. The individuals had sent such data to Social Metric using Facebook's private messaging function.

Except for the data of two individuals, the personal data had been disclosed on the Webpages before the PDPA came into force on 2 July 2014 (***Appointed Day***). The Complainant and the PDPC had informed Social Metric about the disclosure in April and May 2016 respectively. However, at the time of the PDPC's investigation, six of the nine Webpages were still publicly accessible, and contained the personal data of approximately 558 individuals. Hence, approximately two months had passed between the time Social Metric was informed about the personal data and the time when the data was completely removed (around 11 July 2016). By this time, some of the personal data had been left on the Webpages for more than two years after the respective events.

The PDPC's Decision

Upon conclusion of the PDPC's investigations, Social Metric was found to be in breach of its obligations under sections 24 and 25 of the PDPA. It failed to show that it had a purpose for retaining personal data, or that it had made reasonable security arrangements to protect the personal data in its possession or under its control, for the reasons set out below:

(a) Social Metric's obligations under the PDPA

The PDPC held that it was incumbent on Social Metric to take proactive steps to comply with the PDPA obligations in relation to both the existing personal data it had, as well as new personal data which it collected.

The PDPC also analysed whether Social Metric was an "organisation" or a "data intermediary" under the PDPA. It found that while Social Metric was a data intermediary when it collected the personal data and posted this on the Webpages, this was not the case when the marketing campaigns ended. This was because both Social Metric and its clients had no further purpose in retaining the personal data on the Website. Since Social Metric had held on to the personal data for a longer period than was reasonable, it was acting on its own accord in relation to the personal data. Furthermore, Social Metric had a standard operating procedure to dispose of the personal data after the marketing campaigns had ended, and the PDPC was of the view that it would not be reasonable to impose a continuing obligation on Social Metric's clients to protect the personal data. Therefore, Social Metric became an "organisation" under the PDPA after the end of the marketing campaigns.

(b) Social Metric's failure to comply with its Retention Limitation and Protection Obligations

The PDPC held that Social Metric would be considered as an "organisation" for the entire duration after the end of a reasonable period justifiable for legal or business purposes. It would not be meaningful to consider it as a data intermediary for part of the duration and an organisation for the rest of the duration, since the same obligations (the Retention Limitation and Protection Obligations) were breached in both cases.

It was found that Social Metric had breached section 25 of the PDPA since the purpose for which the personal data was collected was no longer being served by retention of the data, and Social Metric had no other legal or business purposes in retaining the data.

It was also found that Social Metric had breached section 24 of the PDPA as the personal data could be accessed by any member of the public well after the Appointed Day. In addition, it had uploaded the personal data of two individuals after the Appointed Day onto the Webpages. While it claimed that its prolonged failure to implement the necessary protection measures was due to oversight or forgetfulness, the PDPC was of the view that these were not valid reasons.

The PDPC's Actions

In assessing the breach and the directions to be imposed on Social Metric, the PDPC took the following factors into consideration:

(a) The fact that the personal data (names and ages) of about 155 children were disclosed.

(b) Social Metric failed to take prompt remedial actions after being informed of the data breach by the PDPC.

(c) Social Metric had, more than once, informed the PDPC that the personal data in question had been deleted when this was untrue.

(d) Social Metric generally failed to cooperate with the PDPC's investigations. For example, it made unsubstantiated claims, including that it had engaged freelance developers in the Philippines to create and maintain the Website without adducing any evidence of this. It also caused multiple delays in the

investigation process when it repeatedly missed the PDPC's deadlines to reply.

Based on the above factors, the PDPC's directions to Social Metric were the following:

(a) To scan and confirm that its Website no longer store publicly accessible personal data that was not supposed to be disclosed to the public.

(b) To pay a financial penalty of S$18,000 within 30 days from the date of the PDPC's directions.

Key takeaway

A "data intermediary" might be considered an "organisation" for the purposes of the PDPA if it holds onto to data after a period that is justifiable for legal or business purposes. Organisations must also be aware of their PDPA obligations in relation to the publishing of personal data on publicly accessible webpages.

ComGateway

Background

ComGateway operates an online shopping portal that provides logistics, shopping and shipping services to its customers. Shipping and transaction orders from customers are processed, tracked and managed by an electronic system and application through and on its website (***Website***).

On 28 November 2016, a customer discovered that when she accessed a shipping details webpage (***Shipping Webpage***), it displayed another customer's shipping details (***First Data Breach***). This was the first time that such an error had been reported to ComGateway, and it could not reproduce the error nor determine its root cause.

The PDPC was further notified that the URL of one customer's Shipping Webpage could be easily manipulated to enable access to shipping details of other customers through trial and error, by systematically changing the last character until a workable link was derived (***Second Data Breach***). This was because shipment identification numbers ***(IDs)*** were not encrypted, but merely encoded using Base64, a common and simple encoding scheme.

The shipping details included personal data such as the customer's name, contact number and address.

The PDPC's Decision

Upon the conclusion of the PDPC's investigations, ComGateway was found not to have breached its obligations under section 24 of the PDPA in respect of the First Data Breach, as its IT security measures were adequate. However, ComGateway was found to have breached the same in respect of the Second Data Breach, as it had failed to implement reasonable security measures to protect personal data in its possession or under its control.

(a) <u>First Data Breach</u>

The PDPC held that the mere fact that personal data had been rendered accessible to an unauthorised party by an error or flaw in an organisation's systems and processes did not automatically mean that the organisation was in breach of section 24 of the PDPA. Conversely, the fact that the cause of a data breach could be a rare computer glitch or could not be determined did not absolve the organisation from liability under section 24 of the PDPA.

On the facts, the PDPC found that ComGateway was not in breach of section 24 of the PDPA as its IT security measures were adequate. Before the occurrence of the First Data Breach, ComGateway's IT system had passed regular and rigorous IT security tests and scans, which took the form of quarterly "Trustwave" vulnerability scans and annual penetration tests for external and internal networks, and automated code checks to detect any "OWASP" top 10 application security risks on its Website. There was also no evidence of any issues with the functions or services of the Website that would affect the protection of the personal data that it held. Rather, the data breach appeared to be anomalous.

The PDPC further commented that ComGateway's removal of all personal data from its Shipping Webpages in the aftermath of the First Data Breach would have been excessive and unnecessary if it had been done purely as a risk avoidance measure and had affected the Website's usability, especially if there had been reasonable technical or operational alternatives.

(b) Second Data Breach

The PDPC found that the URL manipulation vulnerability (as described above), taken together with the fact that ComGateway did not restrict access to the URLs of the Shipping Webpages, meant that any person, such as another customer or even an outsider, could accidentally or intentionally access the URLs and the personal data contained within them, without needing to authenticate or furnish information to verify his identity.

ComGateway admitted that its IT security measures (as described above) were targeted at protecting personal data on its Website and did not address the URL manipulation vulnerability, which it had not considered. Since there were no security measures to protect its customers' personal data from unauthorised access, the PDPC found that ComGateway was in breach of section 24 of the PDPA.

The PDPC's Actions

In assessing the breach and the directions to be imposed on ComGateway, the PDPC took the following factors into consideration:

(a) ComGateway handled a substantial volume of shipping transactions for individual customers in Singapore and thus a substantial amount of personal data.

(b) ComGateway had fully cooperated with PDPC's investigations, including carrying out technical and security testing to ascertain the cause of the breaches.

(c) Upon the PDPC's notification, ComGateway took prompt action to address the Second Data Breach by adding another unique variable to the URLs of the Shipping Webpages to prevent manipulation.

(d) ComGateway had been conducting regular penetration tests, vulnerability scans and code checks as security safeguards.

Based on the above factors, the PDPC directed ComGateway to pay a financial penalty of S$10,000 within 30 days of its direction.

Key takeaway

As this case demonstrates, compliance with section 24 of the PDPA does not preclude organisations from storing customers' personal data on their websites. Rather, they should consider other reasonable technical or operational means of protecting such data, such as securing the configuration of hardware and software components, and conducting regular security testing, among others. For further guidance on the protection of personal data stored on websites, please refer to the PDPC's brochure on Building Websites, which can be accessed **here**.

Additionally, it is important that organisations implement security measures to protect URLs from being easily manipulated, hence gaining unauthorised access to personal data. For instance, organisations may consider adding another unique variable to the URLs of the relevant webpages, as was done in the present case.

Credit Counselling SG

Background

Credit Counselling SG is a registered charity under the National Council of Social Services which helps individuals with debt problems. Its services include the Debt Management Programme (***DMP***), a voluntary debt repayment scheme under which Credit Counselling SG assists individuals who have difficulties repaying unsecured consumer debts in working out a repayment arrangement with their creditors.

On one occasion, Credit Counselling SG sent questionnaires via post to 810 DMP clients requesting for a status update on the debts to be repaid to their creditors under the DMP. When 297 clients did not respond by the deadline, Credit Counselling SG sent three batches of follow-up emails to them.

In sending out one batch of follow-up emails on 30 September 2016 (***Follow-up Email***), an administrative staff of Credit Counselling SG mistakenly pasted the email addresses of 96 DMP clients in the "To" field instead of the "Bcc" field. As such, these 96 email addresses (and associated names for some individuals) were visible to all recipients of the Follow-up Email.

Four DMP clients conveyed to Credit Counselling SG their concerns that their identities had been disclosed to all recipients. Furthermore, 2 DMP clients had clicked the "Reply All" button in submitting their completed questionnaires to Credit Counselling SG, which meant that additional personal data contained in the questionnaires were exposed to all recipients.

The PDPC's Decision

Upon conclusion of PDPC's investigations, Credit Counselling SG was found to have breached its obligations under section 24 of the PDPA to implement reasonable security measures to protect personal data in its possession or under its control.

Not only did the Follow-up Email disclose the 96 individuals' email addresses, which were personal data, it also indirectly disclosed those individuals' financial information, which were *sensitive* personal data and necessitated the implementation of stronger security measures for compliance with the PDPA. However, Credit Counselling SG did not have any checks or controls in place.

(a) <u>The 96 individuals' email addresses were personal data</u>

Under section 2(1) of the PDPA, "personal data" is defined as data, whether true or not, about an individual who can be identified from (a) that data, or (b) from that data and other information to which the organisation has or is likely to have access.

The PDPC observed that since Credit Counselling SG had "other information" in the form of the names of the individuals to whom the 96 email addresses belonged, it would be able to identify them from their email addresses. As such, the 96 email addresses were personal data.

The PDPC further noted that even if the fact that Credit Counselling SG had the names of the individuals to whom the 96 email addresses belonged were disregarded, a number of the email addresses would still constitute personal data.

First, email addresses which contain the individual's full name (e.g. "tan.ah.kow980@gmail .com") or the individual's partial name (e.g. "ylt.rachel@hotmail.com") would allow even an outsider to identify the individual, and would thus be personal data. Secondly, investigations showed that 16 of the 96 individuals could be identified on online social media platforms by searching their email addresses. As such, these 16 email addresses would also constitute personal data.

(b) <u>The disclosure of the 96 individuals' email addresses led to the indirect disclosure of their financial information, which was sensitive personal data</u>

The Follow-up Email contained a "DMP Status Update Form" in which individuals were to select one of several available options as to their state of indebtedness. Consequently, the fact that an individual's email address was included in the list of email addresses in the Follow-up Email would indicate that he was then or had previously been in debt, and was obtaining or had obtained assistance under the DMP.

The PDPC found that financial information about an individual's indebtedness amounts to sensitive personal data, as it could harm the individual by causing social stigma or discrimination, or by tarnishing his reputation. This is notwithstanding that specific details of the debt were not disclosed.

(c) <u>Credit Counselling SG had failed to implement reasonable security measures</u>

The PDPC stated that compliance with section 24 of the PDPA requires the implementation of security measures which correspond to the sensitivity of the data in question. Given that the present case involved sensitive personal data, stronger security measures were warranted, as serious harm may befall an individual from the misuse or unauthorised use of sensitive data.

At the time the Follow-up Email was sent, Credit Counselling SG did not have any checks or controls in place to prevent the pasting of recipient email addresses in the "To" field instead of the "Bcc" field, a mistake which could be easily made and repeated. The PDPC thus found that Credit Counselling SG was in breach of section 24 of the PDPA.

The PDPC helpfully expounded on the checks or controls which Credit Counselling SG could have implemented. Operational measures include sending the emails individually, such as by using the mail merge function of Outlook, and having an additional layer of supervision or oversight before emails are sent. Technical measures include having a technical control that would ensure that email addresses were correctly pasted in the "Bcc" field and not the "To" field.

The PDPC's Actions

In assessing the breach and the directions to be imposed on Credit Counselling SG, the PDPC took the following aggravating factors into consideration:

(a) Information about an individual's adverse financial condition and/or state of indebtedness is sensitive personal data, and the disclosure of such information could cause the individual to suffer harm, injury or hardship, including serious reputational damage and embarrassment.

(b) Credit Counselling SG had no excuse for not having a system of checks for sensitive personal data, given the nature of its business of handling large volumes of such data.

(c) The present incident might cause the public to lose trust in credit counselling organisations in protecting their personal data, which might thwart larger national credit management efforts.

However, the PDPC also took the following mitigating factors into consideration:

(a) Credit Counselling SG had fully cooperated with the PDPC's investigations and had readily and promptly admitted its mistake.

(b) Credit Counselling SG had promptly notified all affected recipients of the present incident, apologised, and requested that the Follow-up Email be deleted.

(c) Credit Counselling SG had counselled the administrative staff who had made the mistake, and had implemented further steps to prevent future data breaches, including plans to conduct an organisation-wide refresher course on compliance with the PDPA, and deploying "mail-merge" software within two months.

(d) No other data breach incidents had been reported.

Based on the above factors, the PDPC directed that Credit Counselling SG pay a financial penalty of S$10,000 within 30 days of its direction.

Key takeaway

To ensure compliance with the PDPA, it is important that organisations implement security measures that correspond to the sensitivity of the personal data concerned. When handling sensitive personal data, organisations may consider taking precautions such as good email procedures and encryption technology. As a matter of good practice, organisations may also consider carrying out data protection risk assessments to help identify and address specific risks of disclosure.

PDPC Updates

Between 4 October 2017 and 8 January 2018, the PDPC released several publications relating to data protection. These are the following:

(a) EU General Data Protection Regulation (***GDPR***) Factsheet for Organisations (issued 4 October 2017).

(b) Data Protection Starter Kit (issued 17 October 2017).

(c) Guide to Developing a Data Protection Management Programme (***DPMP Guide***) (issued 1 November 2017).

(d) Guide to Data Protection Impact Assessments (***DPIA Guide***) (issued 1 November 2017).

(e) Public Consultation on Proposed Revision of NRIC Advisory Guidelines (issued 7 November 2017).

(f) E-Learning Modules on Securing Electronic Personal Data (issued 21 November 2017) and Disposal of Personal Data in Physical and Electronic Medium (issued 21 November 2017).

(g) Summary Reports of the Consumer Survey on the PDPA (issued 4 Dec 2017) and Industry Survey on the PDPA (issued 4 Dec 2017).

EU GDPR Factsheet for Organisations

On 4 October 2017, the PDPC published the EU GDPR Factsheet for Organisations, which highlights important aspects of the GDPR to organisations in Singapore. The GDPR is slated to come into force from 25 May 2018.

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

Application of the GDPR

The GDPR will apply to any organisation which processes the personal data of individuals in the EU, where the processing relates to offers of goods or services to individuals in the EU, or the monitoring of their behaviour.

Where the GDPR applies to an organisation established outside of the EU, the organisation may be required to appoint a representative in an EU Member State, but not where the processing by the organisation is only occasional and does not include processing of certain special categories of personal data (including racial or ethnic origin, political opinions and religious or philosophical beliefs) on a large scale.

Basis of processing

Processing of personal data is lawful under the GDPR in certain situations, including where the individual gives consent for the processing for one or more specific purposes, where it is necessary to perform a contract, and where it is necessary for the organisation's compliance with a legal obligation.

Rights of individuals

Under the GDPR, organisations will have to provide certain rights to individuals, including the right to access and obtain a copy of the individual's personal data, the right to rectification of inaccurate personal data concerning the individual, and the right to erasure of personal data concerning the individual in some circumstances.

Accountability and governance

Organisations will have certain responsiblities, including putting in place appropriate measures to ensure that by default, only personal data that is necessary for the specific purpose is processed.

Data breach notification

Where there is a personal data breach, the organisation must notify the supervisory authority without undue delay, but not later than 72 hours where feasible, and notify the individual without undue delay, if the breach is likely to result in a high risk to the individual's rights and freedoms.

Upon becoming aware of a breach, a data processor must also notify the organisation without undue delay.

Administrative fines

Depending on which provision is infringed upon, the administrative fines that may be imposed are either up to 10 million EUR or 2% of worldwide annual turnover of the preceding financial year (whichever is higher), or up to 20 million EUR or 4% of worldwide annual turnover of the preceding financial year (whichever is higher).

The Factsheet can be accessed **here**.

Data Protection Starter Kit

On 17 October 2017, the PDPC published the Data Protection Starter Kit, which serves as a basic guide for SMEs to comply with their obligations under the PDPA.

The Starter Kit contains helpful information relating to the Data Protection and Do Not Call provisions. It also contains useful advice, including suggestions as to how SMEs may protect electronic personal data, and dispose of personal data that is no longer needed.

Additionally, the Starter Kit also provides sample forms, clauses and communication material which are easily implemented. These include a sample consent clause for sending marketing materials, and a sample consent clause for job applicants.

To supplement the Starter Kit, the PDPC has published two new resources, namely "Sample Clauses and Template for Employees and Job Applicants" and "Sample Clauses and Template for Customers".

The Starter Kit can be accessed **here**.

DPMP Guide

On 1 November 2017, the PDPC published the DPMP Guide, which seeks to help organisations improve their personal data protection policies and practices by implementing a DPMP. A DPMP is a systematic framework to help organisations establish a robust data protection infrastructure. It has three main facets: policy, people and process.

Policy

First, the DPMP Guide explains the importance of having a personal data protection policy and provides guidance as to what should be included in such a policy, among other things.

People

Secondly, the DPMP Guide describes the key responsibilities of a ***DPO***, whose appointment is mandated under the PDPA. It also suggests how the DPO should be appointed.

The DPMP Guide further explains the roles of senior management, other staff and service vendors in personal data protection, and discusses the various training and communication initiatives that may be conducted to help staff understand their responsibilities.

It also discusses potential personal data protection initiatives that organisations may implement to demonstrate accountability to customers.

Process

Thirdly, the DPMP Guide sets out in detail the process of implementing a personal data protection policy, namely the documentation of personal data flows in the organisation, the identification of weaknesses with respect to data protection, the incorporation of good practices into business processes, systems, products or services, and the establishment of a risk reporting structure.

Maintenance

Lastly, the DPMP Guide explains why it is important that organisations review their data protection policies, and suggests how organisations may keep them relevant.

The DPMP Guide can be accessed **here**.

DPIA Guide

On 1 November 2017, the PDPC published the DPIA Guide, which provides organisations with guidance as to how they may conduct a DPIA. A DPIA involves identifying, assessing and addressing personal data protection risks specific to the organisation, so that the organisation may then better assess if it is in compliance with the PDPA, and put in place the appropriate operational or technical safeguards.

The DPIA Guide discusses when a DPIA should be conducted, who should be involved, and the six phases of the DPIA lifecycle, namely:

(a) Assess need for DPIA.

(b) Plan DPIA.

(c) Identify personal data, and personal data flows.

(d) Identify and assess data protection risks.

(e) Create an action plan.

(f) Implement action plan and monitor outcomes.

Throughout the DPIA Guide, case examples are provided to illustrate how an organisation may decide to implement each phase.

Assess need for DPIA

For projects involving personal data, the DPIA Guide sets out threshold questions to be asked in assessing the need for a DPIA, namely:

(a) Is a new system or process being introduced, developed or implemented?

(b) Is an existing system or process being reviewed, or substantially redesigned?

If the answer to either is yes, the DPIA Guide recommends that a DPIA be conducted.

Plan DPIA

The DPIA Guide describes the key aspects to be covered when planning a DPIA. These are:

(a) Providing an overview of the project and key considerations surrounding the DPIA.

(b) Defining the scope of the DPIA, such as the specific system or process that the DPIA needs to be carried out on.

(c) Defining the risk assessment framework or methodology.

(d) Identifying the parties whose inputs or views would have to be sought during consultation or interview sessions.

(e) Providing an estimate of time required for key tasks and overall timeline for conducting the DPIA.

Identify Personal Data, and Personal Data Flows

The DPIA Guide discusses how the DPIA lead (i.e. the person leading the DPIA) should take steps to identify personal data, and personal data flows. This comprises the following steps:

(a) Identifying all the various types of personal data handled in relation to the specific project, and determining the organisation's purposes for collecting, using or disclosing them.

(b) Mapping the way that personal data flows through various stages or touchpoints of the project across its lifecycle i.e. from collection to storage and/or disposal.

Identify and Assess Data Protection Risks

The DPIA Guide explains how the DPIA lead may identify and assess personal data protection risks, and discusses some relevant considerations in doing so, such as the applicable PDPA obligations, and whether the staff are aware of their roles and responsibilties.

At this stage, the steps that should be taken are:

(a) Completing a DPIA questionnaire to assess the project against PDPA requirements and/or data protection best practices.

(b) Identifying areas in the personal data flow which could lead to a breach of the PDPA (e.g. loss of personal data) or are gaps compared to industry best practices.

(c) Analysing the potential impact and likelihood of identified gaps and risks based on the pre-defined risk framework. .

Create an Action Plan

The DPIA Guide discusses what should be included in an action plan, and the approach an organisation should adopt in developing one.

The action plan should include the following information:

(a) The action owner(s) responsible for the implementation of specific recommendations (such as technical or organisational measures).

(b) Monitoring of implementation outcomes.

(c) Timelines for implementation.

(d) A contact point for responding to queries regarding the DPIA process or arising from implementing the action plan.

Implement action plan and monitor outcomes

The DPIA Guide describes, among other things, what should be done before and upon the implementation of the action plan.

Before implementation, the following steps should be taken:

(a) Prepare a DPIA report which documents the whole DPIA process.

(b) Get the DPIA report reviewed by the organisation's Data Protection Officer.

(c) Submit the DPIA report to the project steering committee and seek approval to implement the plan.

Upon implementation, the following steps should be taken:

(a) Monitor the outcomes of the action plan.

(b) Review and update the DPIA where there is a change in risks associated with the personal data handling of the project.

The DPIA Guide can be accessed **here**.

Public Consultation on Proposed Revision of NRIC Advisory Guidelines

On 7 November 2017, the PDPC released a public consultation paper seeking comments on its proposed revision of the chapter on NRIC numbers in the Advisory Guidelines on the PDPA for Selected Topics, which it had earlier issued in September 2013.

Concurrently, the PDPC also released for public consultation a proposed technical guide to complement the revised NRIC Advisory guidelines.

The public consultation closed on 18 December 2017.

Proposed advisory guidelines on the PDPA for NRIC numbers

NRIC numbers are personal data as individuals may be identified from their unique sequences of numbers and letters. As such, organisations which collect NRIC numbers, copies of NRICs or physical NRICs must comply with the PDPA.

Since NRIC numbers are permanent and irreplaceable identifiers that can be used to access huge amounts of information relating to the individuals, the indiscriminate collection and use of NRIC numbers are undesirable, as they increase the risk of the NRIC numbers being obtained and used for illegal activities including identity theft and

fraud. The collection of individuals' NRIC numbers or copies of their NRICs are of even greater concern, as they contain additional personal data, such as the individual's full name, photograph, thumbprint and residential address.

Consequently, the PDPC has proposed that organisations should not collect, use or disclose individuals' NRIC numbers or copies of the NRIC, nor retain individuals' physical NRICs, except in two circumstances:

(a) It is required under the law.

(b) It is necessary to accurately establish and verify the individual's identity.

As to (a), the PDPC provides examples of situations where the collection, use or disclosure of NRIC numbers or copies of the NRIC may be required under the law.

As to (b), the PDPC provides examples of situations where the collection, use or disclosure of NRIC numbers or copies of the NRIC is necessary to accurately establish and verify the individual's identity. These include situations or transactions where verification is necessary to prevent a risk of significant harm or impact to the individual and/or the organisation, such as where the individual enters into high value contracts like property transactions. In these situations, the PDPC proposes that it may be considered reasonable to require consent to collect, use or disclose the individual's NRIC number to accurately establish and verify the identity of the individual, unless the exceptions under the Second, Third or Fourth Schedule of the PDPA apply such that consent is not required.

In relation to the retention of physical NRICs, the PDPC proposes that even if the organisation does not record any personal data contained in an NRIC, in most circumstances, it is to be regarded as having done so for the duration that it is in possession of or has control of the NRIC.

While the PDPC does not prescribe the alternatives that organisations should use in place of NRIC numbers or copies of the NRIC, it sets out some alternatives, which include organisation/user-generated IDs or passwords, tracking numbers, organisation-issued QR codes, or monetary deposits.

In light of the above, the PDPC proposes that organisations will be given up to one year from the issuance of the advisory guidelines to review and implement the necessary changes to their practices and processes involving the collection of NRIC numbers, copies of NRICs or physical NRICs.

Proposed Technical Guide to NRIC Advisory Guidelines

The proposed Technical Guide seeks to provide guidance to organisations as to alternatives that may be used to replace the NRIC number as a unique identifier used in websites and other public facing computer systems.

It suggests the following five alternatives:

(a) User selected identifier.

(b) Organisation selected identifer.

(c) Email address.

(d) Mobile number.

(e) Combination of identifiers.

The Technical Guide also provides advice on how these alternatives may be implemented in both new systems and existing systems, with an emphasis on the latter. It divides the process of replacing the NRIC number in existing systems into three phases: preparation, implementation and post-implementation, and suggests steps to be taken during each phase.

The Technical Guide further highlights various resources which organisations may refer to for more guidance, including Advisory Guidelines and other guides.

E-Learning Modules on Securing Electronic Personal Data and Disposal of Personal Data in Physical and Electronic Medium

On 21 November 2017, the PDPC announced the addition of two E-Learning Modules:

(a) E-Learning Module on Securing Electronic Personal Data.

(b) E-Learning Module on Disposal of Personal Data in Physical and Electronic Medium.

The E-Learning Modules are an interactive learning tool developed by the PDPC, and can be accessed **here**.

Summary Reports of the Consumer and Industry Surveys on the PDPA

On 4 December 2017, the PDPC announced the release of the summary reports of the 2017 Consumer Survey on the PDPA and the 2017 Industry Survey on the PDPA, which are conducted annually to assess the awareness and perceptions of consumers and organisations in relation to the PDPA.

The summary report of the 2017 Consumer Survey on the PDPA shows that 53% of survey respondents have heard of the PDPA, 14% are registered under the Do Not Call registry, and 73% are willing to share personal data in exchange for benefits such as freebies and lucky draws, among others.

The summary report of the 2017 Industry Survey on the PDPA shows that 86% of survey respondents have heard of the PDPA, 92% are aware of their obligations under the Data Protection provisions and 78% are aware of their obligations under the Do Not Call provisions, among others.

The summary report of the 2017 Consumer Survey on the PDPA can be accessed **here**.

The summary report of the 2017 Industry Survey on the PDPA can be accessed **here**.

Cybersecurity Bill

The Cybersecurity Bill (***CS Bill***) was introduced in Parliament on 8 January 2018. At the time of writing, the CS Bill has yet to undergo its Second Reading in Parliament.

The CS Bill seeks to achieve the following purposes:

(a) Create a framework for the protection of critical information infrastructure (***CII***) against cybersecurity threats.

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

(c) Regulate owners of CII and providers of cybersecurity services in Singapore.

The CS Bill consists of the following parts:

(a) Part 1 introduces the fundamental concepts used in the CS Bill and provides for the application of the CS Bill.

(b) Part 2 provides for the administration of the CS Bill and the appointment of a Commissioner of Cybersecurity and other officers for the purposes of the CS Bill.

(c) Part 3 provides for the designation of CII and the regulation of owners of CII with regard to the cybersecurity of CII.

(d) Part 4 provides for the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore.

(e) Part 5 provides for the licensing of providers of licensable cybersecurity services.

(f) Part 6 contains general provisions.

The following key points can be noted in relation to the CS Bill:

(a) A "cybersecurity threat" is defined as an activity carried out on or through a computer system that may imminently jeopardise or affect adversely the cybersecurity of a computer system. On the other hand, a "cybersecurity incident" is a cybersecurity threat that has been realised. An example of a cybersecurity incident is the unauthorised hacking of a computer by a hacker.

(b) The Minister will appoint a Commissioner who will be responsible for the administration of the CS Bill.

(c) If the Commissioner is satisfied that a computer or computer system falls within the definition of a CII, he may designate it as such via written notice. The definition of a CII is as follows:

- the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of which will have a debilitating effect on the availability of the essential service in Singapore; and
- the computer or computer system is located wholly or partly in Singapore.

(d) The Commissioner may issue codes of practice to regulate the owners of CII, and

conduct cybersecurity exercises in order to ensure the cybersecurity of the CII.

(e) In response to a cybersecurity threat or incident, the Commissioner can exercise investigatory powers and authorise the taking of emergency cybersecurity measures.

(f) Certain cybersecurity services are prescribed as licensable cybersecurity services. These are (i) managed security operations centre monitoring services, and (ii) penetration testing services. In relation to licensable cybersecurity services, the CS Bill creates the following offences:

- It is an offence for a person to engage in the business of providing a licensable cybersecurity service without a licence.
- It is an offence for a person to advertise or otherwise hold out that the person provides a licensable cybersecurity service, unless the person holds a licence.

Healthcare Services Bill

On 5 January 2018, the Ministry of Health (***MOH***) released the draft Healthcare Services Bill (***Draft HCS Bill***). It also released a public consultation paper seeking comments on the Draft HCS Bill. The public consultation opened on 5 January 2018, and will close on 15 February 2018.

The Draft HCS Bill is intended to replace the Private Hospitals and Medical Clinics Act (***PHMCA***), under which healthcare providers are currently licensed and regulated.

If passed, the Draft HCS Bill will have data protection implications. Prescibed licensees would be required to contribute core patient data containing critical patient health information to the National Electronic Health Record (***NEHR***), so as to facilitate coordination across healthcare providers, continuity of care and patient safety. This data would include the patient's profile, diagnosis, procedures or treatments and medications, among others. The PDPA would not apply to restrict the access, use and contribution of such data to the NEHR. Further, the Draft HCS Bill proposes that a patient's data may be retained on the NEHR for a period of 10 years after his death.

Even so, the Draft HCS Bill proposes several safeguards to ensure that patients' NEHR records are kept confidential. These records may only be accessed for the sole purpose of patient care, and not other purposes such as employment and insurance assessments. Other proposed measures include providing access logs to patients, conducting regular audits on NEHR access and imposing penalties for unauthorised access.

Under the Draft HCS Bill, a patient may choose to opt out of the NEHR, with the implication that while his data will still be uploaded to the NEHR, healthcare providers will not be able to access it, except in situations of emergency. Where patients do not wish to have their data uploaded to the NEHR, such requests will considered on a case-by-case basis.

More broadly, the Draft HCS Bill also proposes enhancing existing powers under the PHMCA. This would allow MOH to obtain data from healthcare providers in the interest of patient safety, care and welfare, and public health.

The Draft HCS Bill and the public consultation paper can be accessed **here**.

AUSTRALIA

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

On 22 February 2018, Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 (***PA Act***) is slated to come into effect, establishing the Notifiable Data Breaches (***NDB***) scheme under Part IIIC of the Privacy Act 1988 (***Privacy Act).*** The PA Act requires organisations subject to the Privacy Act to notify the Australian Information Commissioner (***AIC***) and the affected individuals if the entity experiences a data breach of a certain severity as specified in the PA Act. The NDB scheme will only apply to eligible data breaches that occur on or after 22 February 2018.

For further details on the NDB scheme and what it entails, please see our **Data Protection Quarterly Update published in January 2017**.

HONG KONG

Statements issued by the Hong Kong Privacy Commissioner for Personal Data

The Hong Kong Privacy Commissioner for

Personal Data (***PCPD***) has issued two statements in relation to recent enforcement decisions. They are the following:

(a) Statement on Complying with Opt-out Requests of Direct Marketing, which can be accessed **here** (issued 11 December 2017).

(b) Statement on Personal Data Obtained from Public Domains, which can be accessed **here** (issued 17 November 2017).

Statement on Complying with Opt-out Requests of Direct Marketing

In relation to the conviction of Physical Health Centre Hong Kong Limited under section 35G(3) of the Personal Data (Privacy) Ordinance, the PCPD stated that regardless of whether a customer's opt out request in direct marketing is made verbally or in writing, the company must immediately cease to use the personal data concerned for direct marketing upon receipt of such notification, without any charge to the customer.

Statement on personal data obtained from public domains

In relation to the conviction of a financial consultant under sections 35C and 35F of the Personal Data (Privacy) Ordinance, the PCPD commented that under the Ordinance, a data user may only use an individual's personal data in direct marketing with that individual's consent. To obtain valid consent, the data user must notify the individual of the types of personal data that will be used, the classes of goods or services that will be marketed, and a response channel through which the individual can communicate his consent to the intended use. Further, when using the individual's data in direct marketing for the first time, the data user is required to inform him of his right to request to opt out without charge. It is crucial to note that such an obligation applies regardless of whether the personal data is collected directly or indirectly from the individual.

CANADA

Draft Guidelines issued on 28 September 2017 by the Office of the Privacy Commissioner of Canada

On 28 September 2017, the Office of the Privacy Commissioner of Canada (***OPC***) issued two sets of Draft Guidelines on the Personal Information Protection and Electronic Documents Act (***PIPEDA***). The PIPEDA is the federal privacy law for private-sector organisations and sets out the rules for how businesses must handle personal information in the course of commercial activity. The two sets of draft guidelines issued are the following:

(a) Draft guidelines on obtaining meaningful online consent (***Consent Guidelines***), which can be accessed **here**.

(b) Draft guidelines on inappropriate data practices, regarding the interpretation and application of subsection 5(3) of the PIPEDA (***Data Practices Guidelines***), which can be accessed **here**.

The Consent Guidelines sets out practical guidance regarding what organisations should do to ensure that they obtain meaningful consent in the online environment. The Data Practices Guidelines sets out guiding principles for interpreting subsection 5(3) of the PIPEDA, which allows organisations to collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

The two sets of draft guidelines are closed for comment, and the OPC is currently reviewing the feedback received. At the time of writing, the finalised guidelines have not been issued yet.

Report on Privacy-Enhancing Tools Issued by the OPC

On 15 November 2017, the OPC released a report on Privacy-Enhancing Tools (***PETs***). PETs are a category of technology that allows users to protect their (informational) privacy by allowing them to decide, among others, the following:

(a) The information they are willing to share with third parties, such as online service providers.

(b) The circumstances under which that information will be shared.

(c) The purposes for which the third parties can use that information.

The report provides a summary of privacy-enhancing technologies used by online users and organisations legal in nature to protect their data, and discusses their efficacy and prominence as research interests. The report can be accessed **here**.

UNITED KINGDOM

Data Protection Bill introduced and debated in the UK Parliament

The Data Protection Bill (***DP Bill***) was introduced in the UK Parliament on 13 September 2017. The DP Bill will amend the Data Protection Act 1998 (***DP Act***), which is the main legislation for data protection in the UK. The four main matters provided for in the DP Bill are as follows:

(a) General data processing.

(b) Law enforcement data processing.

(c) Data processing for national security purposes including processing by the intelligence services.

(d) Regulatory oversight and enforcement.

In the impact assessment that was released alongside the DP Bill, the UK Government stated the following objectives of the DP Bill:

(a) To provide a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice.

(b) To set new standards for protecting general data in accordance with the GDPR, give people more control over the use of their data, and provide new rights to move or delete personal data.

(c) To preserve existing exemptions that have worked well in the DP Act and carry them over to the new law to ensure that UK businesses and organisations can continue to support world leading research, financial services, journalism and legal services.

(d) To provide a framework tailored to the needs of criminal justice agencies and national security organisations, including the intelligence agencies, and to protect the rights of victims, witnesses and suspects in light of the changing nature of the global threats the UK faces.

The latest text of the DP Bill can be accessed on the Parliament website **here**.

EUROPEAN UNION

General Data Protection Regulation to come into force on 25 May 2018

On 25 May 2018, the General Data Protection Regulation (***GDPR***) is slated to come into force and be directly applicable in all EU Member States. In light of this, we have prepared a write-up on the GDPR in the Annex of this Quarterly Update. The write-up provides a brief overview of the GDPR and its key provisions, with a focus on how it might impact your business in Singapore.

The write-up can be found **here**.

Additional Sets of GDPR Guidelines and Working Documents issued by the Article 29 Working Party

Six sets of GDPR guidelines and three sets of working documents have been issued by the Article 29 Working Party.

The GDPR guidelines issued are the following:

(a) Guidelines on automated individual decision-making and profiling, which can be accessed **here** (issued 3 October 2017).

(b) Guidelines on personal data breach notification, which can be accessed **here** (issued 3 October 2017).

(c) Guidelines on the application and setting of administrative fines, which can be accessed **here** (issued 3 October 2017).

(d) Guidelines on data protection impact assessment, which can be accessed **here** (issued 4 October 2017).

(e) Guidelines on consent, which can be accessed **here** (issued 28 November 2017).

(f) Guidelines on transparency, which can be accessed **here** (issued end 2017).

The working documents issued are the following:

(a) Working document on adequacy referential, which can be accessed **here** (issued 28 November 2017).

(b) Working document setting up a table with the elements and principles to be found in binding corporate rules (***BCRs***), which can

be accessed **here** (issued 29 November 2017).

(c) Working document setting up a table with the elements and principles to be found in processor BCRs, which can be accessed **here** (issued 29 November 2017).

Guidelines on Automated Individual Decision-Making and Profiling

These guidelines seek to clarify the new provisions introduced by the GDPR relating to the risks arising from profiling and automated decision-making, in particular privacy risks. It covers the following:

(a) Definitions of profiling and automated decision-making, and the GDPR approach to these generally.

(b) Specific provisions on automated decision-making as defined under Article 22 GDPR.

(c) General provisions on profiling and automated decision-making.

(d) Children and profiling.

(e) Data protection impact assessments.

Best practice recommendations are provided in the **Annexes**.

Guidelines on Personal Data Breach Notification

These guidelines clarify the mandatory breach notification and communication requirements under the GDPR, and explain how controllers and processors may meet these new requirements. They also provide examples of different types of breaches, and who is to be notified in different circumstances.

Guidelines on the Application and Setting of Administrative Fines

These guidelines are intended for use by supervisory authorities to allow for a more consistent application and enforcement of the GDPR, and reflects their common understanding of Article 83 GDPR, its relationship with Articles 58 and 70 GDPR, and their corresponding recitals. A significant portion of the guidelines is dedicated to explaining how supervisory authorities should interpret and apply the assessment criteria set out in Article 83(2) GDPR as to whether a fine should be imposed and if so, the amount of the fine.

Guidelines on Data Protection Impact Assessment

The guidelines aim to clarify Data Protection Impact Assessment (***DPIA***) requirements under the GDPR, so as to assist controllers in complying with the law, and provide controllers required to carry out a DPIA with legal certainty. In particular, the guidelines seek to clarify when a processing operation is "likely to result in a high risk to the rights and freedoms of natural persons" under Article 35(1) GDPR, such that carrying out a DPIA is mandatory.

Guidelines on Consent

These guidelines contain a detailed analysis of the concept of consent under the GDPR, so as to facilitate compliance with it. Given that the concept of consent remains similar to that under the repealed Data Protection Directive (Directive 95/46/EC), the guidelines expand upon and complete earlier Article 29 working party opinions, such as Opinion 15/2011 on the definition of consent.

Guidelines on Transparency

These guidelines provide guidance as to how to interpret and comply with the new obligation of transparency in relation to the processing of personal data under the GDPR. In particular, it discusses the various elements of transparency under the GDPR, and the information that is to be provided to the data subject under Articles 13 and 14 GDPR.

Working Document on Adequacy Referential

This working document seeks to provide guidance to the European Commission and the Working Party of EU Data Protection Authorities under the GDPR in assessing the level of data protection in a third country, a territory or one or more specified sectors within that third country, or in an international organisation. It establishes the core data protection principles that must be present in a third country legal framework or an international organisation to ensure essential equivalence with the EU framework, which is required under Article 45 GDPR before data transfers to them may take place.

Working Document setting up a table with the elements and principles to be found in BCRs

The table seeks to facilitate the use of BCRs by a corporate group for its international transfers from the EU to organisations within the same corporate group, by:

(a) Clarifying the necessary content of BCRs as stated in working document WP 74 and working document WP 108.

(b) Making the distinction between what must be included in BCRs and what must be presented to data protection authorities in the BCRs application (working document WP 133).

(c) Giving, for each principle, the corresponding text references in working document WP 74 and working document WP 108 for further details.

(d) Providing explanations or comments on each principle.

Working document setting up a table with the elements and principles to be found in Processor BCRs

The table seeks to reflect the requirements referring to BCRs expressly set out in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the GDPR. It does so by:

(a) Adjusting the wording of the previous referential so as to align it with Article 47 GDPR.

(b) Clarifying the necessary content of BCRs as stated in Article 47 GDPR.

(c) Making the distinction between what must be included in BCRs and what must be presented to the competent Supervisory Authority in the BCRs application (document WP 1334).

(d) Giving, for each principle, the corresponding text references in Article 47 GDPR.

(e) Providing explanations or comments on each principle.

Statement by the Dutch Data Protection Authority that data controllers need no longer inform it of Data Processing Activities

On 6 November 2017, the Dutch Data Protection Authority released a statement clarifying that generally, data controllers subject to the Dutch Data Protection Act are no longer required to notify it of their data processing activities. Notification is only required in limited circumstances, such as where high-risk data processing is carried out. This is in light of the GDPR, notwithstanding that it is only slated to come into force on 25 May 2018, at which time data controllers and data processors will be required to keep internal records of data processing activities.

ANNEX: GENERAL DATA PROTECTION REGULATION (*GDPR*)

COMPARISON TABLE

	GDPR (EU)	PDPA (Singapore)
Application	• Replaces the current Data Protection Directive 95/46/EC and is slated to come into effect in all Member States on 25 May 2018 • Applies to Singapore-based organisations which process the personal data of data subjects in the EU (see Q1 below for more details)	• Has yet to articulate/stipulate the application of the GDPR in Singapore and how it should be read in conjunction with the PDPA • Does not apply to Singapore-based public agencies or their data processing agents. "Public Agencies" refer to the Government and certain Statutory Boards
Data Protection Officer (*DPO*)	• Not all organisations require a DPO • Businesses may be required to appoint a DPO who must have sufficient expert knowledge, be involved in all data protection issues and report directly to the highest management within the respective organisation	• Mandates the appointment of a DPO in all circumstances
Minor Consent	• Parental consent is required to process the personal data of children under the age of 16 for online services	• No stipulation as to the age at which consent from the parent of a child is required
Data Processors	• Direct obligation	• Indirect / No obligation
Data Breach Notifications	• Data controllers are required to notify data breaches to the relevant Data Protection Authority (***DPA***) without undue delay and within 72 hours of awareness (where feasible)	• No mandatory guidelines on data breach notifications • Nonetheless, in its Guide to Managing Data Breaches, the PDPC recommends that organisations report data breaches
Corporate Rules	• Binding and accords enforceable rights on data subjects	• No stipulation as to the rules that corporations are subject to
Data Subjects' Rights	• Organisations must receive clearly enunciated consent from data subjects before they can process their data • Organisations can only collect data necessary for the purposes for which it is processed	• Deemed consent from the data subjects can be obtained in place of clearly articulated consent • Not mandatory for organisations to only collect data for the purposes for which it is processed
Penalties	• The DPA may impose fines for breaches of the GDPR of either up to 10 million EUR or 2% of worldwide annual turnover of the preceding financial year (whichever is higher), or up to 20 million EUR or 4% of worldwide annual turnover of the preceding financial year (whichever is higher) • Individuals affected by the breaches may sue the organisation for compensation for both material and non-material damage	• Less stringent penalties • Affected individuals have a right of private action in civil proceedings in court, and may obtain damages

FAQs

1. Does the GDPR apply to Singapore-based organisations?

- Yes, the GDPR applies to Singapore-based organisations that process the personal data of data subjects in the EU, where these processing activities are related to (i) the offering of goods and services to these data subjects, or (ii) the monitoring of the data subject's behaviour as far as their behaviour takes place within the EU.
- In Singapore, the PDPA does not apply to Singapore-based public agencies and/or their data processing agents.

2. Must Singapore-based organisations have a representative within the EU?

- Each Singapore-based private sector organisation carrying out the processing activities described above must have a representative within the EU. More specifically, the representative should be located in one of the EU states where the data subjects (whose data are processed by the organisation) reside.
- While a representative may be liable for a breach of the GDPR by the Singapore-based organisation, the appointment of the representative does not mean that the Singapore-based organisation is immune from legal actions.

3. Does the GDPR apply to only data controllers, or to data processors as well?

- The GDPR defines a data processor to be an organisation which processes personal data on behalf of a data controller. Meanwhile, a data controller is an organisation which determines the purposes, conditions and means of the processing of data by the data processor.
- In Singapore, the PDPA largely applies only to data controllers. However, the GDPR requires data processors to (i) maintain a written record of processing activities carried out on each controller's behalf, (ii) designate a DPO when required (as discussed later), and (3) notify the controller when aware of a personal data breach.

4. What are the penalties for breach of the GDPR?

- There are 2 tiers of fines under the GDPR:
    - The maximum fine of up to 20 million EUR or 4% of worldwide annual turnover of the preceding financial year (whichever is higher) will be imposed on companies who are in serious breach of the GDPR.
    - The lower tier, which involves a fine of up to 10 million EUR or 2% of worldwide annual turnover of the preceding financial year (whichever is higher), will be imposed on companies with less serious breaches.
- Individuals affected by the breaches of the GDPR may also sue the organisation for compensation for both material and non-material damage.
- In Singapore, the PDPC can order an organisation to pay a financial penalty of up to $1 million if it deems fit, as well as give directions to the organisation to stop the collection, use and disclosure of personal data, and/or to destroy personal data collected in contravention of the PDPA.

5. What types of personal data fall within the scope of the GDPR?

- In Singapore, the PDPA defines personal data as data from which an individual can be directly or indirectly identified. The definition of personal data under the GDPR, while similar, is more specific.

- Organisations should note that the GDPR generally does not permit the processing of certain special types of personal data, such as data concerning racial origin and religious beliefs. However, such data may be processed under certain circumstances.

6. Are there special requirements relating to the personal data of children?

- Organisations should note that the age at which parental consent is no longer required for the personal data of children might vary among different EU countries.
- For children below the age of 16, an organisation must first obtain consent from their parents before processing their personal data. While EU Member States may provide for a lower age of consent by law, this age will not fall below 13 years old.
- In Singapore, the PDPA does not specifically deal with the personal data of children.

7. Can organisations transfer the personal data of EU subjects outside of the EU?

- Any transfer of personal data for processing in a country outside of the EU can only take place subject to certain conditions. Hence, Singapore-based organisations must comply with these conditions before they can transfer the personal data of data subjects in the EU to Singapore or other countries for processing.

8. Do all organisations require a DPO?

- Under the GDPR, it depends. A DPO is required for public authorities who process data, or for organisations which perform large-scale, regular and systematic monitoring of data subjects, or large-scale processing of the aforementioned special types of personal data or personal data related to criminal offences. A DPO must be involved in all data protection issues and report directly to the highest management within the organisation.
- In Singapore, the PDPA requires all organisations subjected to its provisions to appoint at least one DPO. Hence, as the PDPA will still apply even after the GDPR comes into effect, all Singapore-based organisations currently subject to the PDPA must still ensure that they have at least one DPO.
- Under the PDPA, the business contact details of at least one DPO must be made available to the public. There is no requirement in the PDPA that the DPO must be an employee of the organisation. However, the DPO must ensure that the organisation complies with the PDPA.

9. Must an organisation receive express consent from the data subjects to process their data?

- Yes, under the GDPR, organisations must receive clearly enunciated consent from the data subjects before they can process their data. The data subjects must have given such consent freely, and must have been informed about the data processing before giving consent.
- In Singapore, the PDPA provides for the notion of deemed consent. Deemed consent to the processing of personal data for a purpose arises where an individual voluntarily provides personal data to an organisation for that purpose, and it is reasonable that the individual would voluntarily provide the data.

10. Must an organisation ensure that the personal data it processes is accurate and updated?

- The GDPR indicates that personal data should be accurate and up to date.

- In Singapore, there is no similar requirement. Under the PDPA, organisations need only make a reasonable effort to ensure that the personal data which they have is accurate and complete, and only if they are likely to use the personal data to make decisions concerning the data subjects or if they are likely to share the data with other organisations.

11. Can a data subject compel a data controller to erase his data or transfer it to another data controller?

- The GDPR gives data subjects the right to compel a data controller to erase their personal data without undue delay. One ground on which data subjects can so compel a data controller is through withdrawing their consent to the data processing.
- Under the GDPR, data subjects also have the right to compel a data controller to transfer their personal data to other data controllers in a commonly-used and machine-readable form, if the first data controller currently processes the data in an automated manner.
- Data controllers must comply with such requests within one month of the requests.
- In Singapore, the PDPA does not expressly provide for a "right to be forgotten". However, a data controller must destroy or deidentify personal data when there is no longer any legal, business or other purpose for the retention of the personal data. Individuals do not have a right to data portability.

12. In the event of a data breach, must the organisation notify the authorities and/or the parties involved?

- If the organisation hit by the breach is a data processor, it must notify its data controller without undue delay.
- If the breach would likely result in a risk to the rights and freedoms of individuals, the data controller must inform the national DPA of the breach. In Singapore, the relevant DPA would be the PDPC. This should be done within 72 hours of its becoming aware of the breach.
- If the breach would likely result in a high risk to the rights of individuals, the data controller must also notify the affected individuals of the breach without undue delay. The notice to the affected individuals should contain details such as the likely consequences of the breach.
- In Singapore, the PDPA currently adopts a voluntary approach and does not require mandatory notification to any party when a data breach has occurred. However, at the time of writing, the PDPC has conducted a public consultation on a proposed mandatory data breach notification regime which closed on 5 October 2017, although it has yet to be implemented.

SUMMARY

1. Introduction

- In April 2016, the new EU data protection framework was updated with the enactment of the GDPR.
- The GDPR is slated to replace the current Data Protection Directive 95/46/EC and take effect in all Member States on 25 May 2018.
- The GDPR imposes a tiered approach to penalties for breach, such that a DPA may impose fines for infringements of up to 20 million EUR or 4% of worldwide annual turnover of the preceding financial year (whichever is higher). Examples of breaches that result in such penalties include those relating to international transfers or breaches of the basic principles for processing. Other specified infringements may result in a fine of up to 10 million EUR or 2% of worldwide annual turnover of the preceding financial year (whichever is higher). Individuals may also sue the company/firm for compensation, so as to recover compensation for both material and non-material damage.

2. Expanded Territorial Reach

- The scope of the GDPR expands to reach data controllers and processors who may not be physically located in the EU, as long as they target consumers or individuals who are in the EU region.
- Many companies/firms need to appoint a representative in the EU (if the company/firm itself is not established in the EU), subject to certain exceptions. Both the representative and the company/firm may face liability for breaches of the GDPR by the company/firm.

3. DPO

- Businesses may be required to appoint a DPO who must have sufficient expert knowledge, be involved in all data protection issues and must report directly to the highest management within the respective business.

4. Consent from Children

- The consent from a child, who is under the age of 16, relating to any online service, will only be valid if it is authorised by a parent. There are also other protections accorded to children, such as the need for the processing to be for the 'legitimate interests' of the organisation.

5. Accountability and Privacy

- Data controllers face substantial accountability obligations to demonstrate compliance with the GDPR, including the following: (i) maintaining certain documentation, (ii) conducting a data protection impact assessment for more risky processing, and (iii) implementing data protection by design and by default.

6. Role of Data Processors

- Data processors now have direct obligations under the GDPR, such as to: (i) maintain a written record of processing activities carried out on each controller's behalf, (ii) designate a DPO in certain circumstances (whenever required), as well as (iii) notify the controller when aware of a personal data breach.

7. Fair Processing Notices

- Data controllers are required to provide transparent information to the data subjects at the time the personal data is obtained, consider their forms of fair processing notice with the new obligations, and check that they are providing the information in a clear, concise and easily accessible manner.

8. Data Breach Notification

- Data controllers are required to notify data breaches to the DPA without undue delay and within 72 hours of awareness (where feasible). Failure to do so would require the organisation to submit a reasoned justification.
- In some cases, the affected data subjects must be notified.

9. Corporate Rules

- The GDPR recognises Binding Corporate Rules (***BCRs***) for controllers and processors as a means of legitimising intra-group international data transfers. These BCRs must be legally binding and apply to and be enforced by every group member who is engaged in a joint economic activity (including their employees).
- The BCRs shall accord enforceable rights on data subjects.

10. Data Subjects' Rights

- The GDPR facilitates the strengthening of data subjects' rights, such as through giving these subjects the right to require information about data being processed about themselves, to access data about themselves that is being processed, to correction of data that is wrong, as well as to restrict certain processing.
- Data portability is also possible, where individuals may receive their personal data in a structured and commonly used format such that it can be transferred to another data controller easily.

11. Transfers outside the EU

- The GDPR prohibits transfer of personal data outside the EU, save where certain conditions are met. These conditions are largely the same as those previously under the Data Protection Directive. Examples of such conditions include the transfer not being repetitive, concerning only a number of data subjects and being necessary for compelling legitimate interests, and the controller assessing all the circumstances and adducing suitable safeguards.

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**