DREW & NAPIER

DATA PROTECTION MID-YEAR UPDATE

June 2019

In this issue

WELCOME MESSAGE

The Drew & Napier Data Protection and Privacy Practice Group is pleased to present the inaugural issue of our new Data Protection Mid-Year Update, which is designed to catch you up on the most important data protection law developments in Singapore and around the world.

In this special bumper issue, we highlight key takeaways from the enforcement decisions issued by the Personal Data Protection Commission (***PDPC***) between April 2018 and June 2019, and examine several of the PDPC's latest publications, including the Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers. Next, we examine some of the most significant developments in the year since the European Union (***EU***) General Data Protection Regulation (***GDPR***) came into effect. We will also analyse the emergence of new regulatory instruments and frameworks in ASEAN, Hong Kong, and Canada as well as the United States with the introduction of the California Consumer Privacy Act.

We hope that this new publication will be useful to you, as your business navigates the increasingly complex regulatory landscape in data protection law. We welcome your feedback and questions on any of the data protection news and articles featured in this Mid-Year 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 Data Protection and Privacy Practice Group, please visit: **https://www.drewnapier.com/Our-Expertise/Data-Protection-Privacy**.

IN THE NEWS

SINGAPORE

PDPC enforcement decisions: April 2018 – June 2019

The PDPC continues to be very active on the enforcement front. Between April 2018 and June 2019, the PDPC issued 46 enforcement decisions involving 51 organisations and their obligations

under the Personal Data Protection Act (No. 26 of 2012) (***PDPA***).

Breaches of the Protection Obligation under the PDPA continued to make up a majority of the enforcement decisions issued by the PDPA, being at issue in 33 cases. Of these, 27 breaches of the Protection Obligation were due overwhelmingly to two causes of breaches – disclosure via the Internet because of insufficient security practices or programming flaws, and errors made in mass post or email processes. These cases are a good reminder that organisations should ensure that they conduct regular patching, testing, and checking of their web-facing servers (whether or not they contain personal data), and exercise care when sending out batch emails or letters particularly where personal data is involved. Organisations may wish to have regard to the guides issued by the PDPC on these topics, such as the Guide to Securing Personal Data in Electronic Medium, the Guide on Building Websites for SMEs, the Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data, and the recently-released Guide to Printing Processes for Organisations.

Breaches of the Openness, Consent, and Purpose Limitation Obligations under the PDPA were also significant, being at issue in 9, 11, and 7 cases respectively. There is significant overlap in cases dealing with the Consent and Purpose Limitation Obligations – the Consent Obligation was involved in every case in which the Purpose Limitation Obligation was at issue. In this connection, organisations should review the documents setting out the purposes for which they collect personal data to ensure that such purposes are clearly defined and notified to their customers so that valid consent can be obtained.

Several cases in this period are distinctive, representing various landmarks and firsts for the PDPC. Most notably, the PDPC handed out the largest financial penalties to date in the wake of the SingHealth data breach, establishing a benchmark for the issuance of large financial penalties approaching the statutory limit of S$1 million. The Access, Accuracy, and Transfer Limitation Obligations were also dealt with for the first time.

Brief summaries of the PDPC's decisions in this period are listed in the attached Annex but we highlight some of the more noteworthy decisions in this period below:

(i) *Re MyRepublic Limited* [2018] SGPDPC 13 (issued 14 May 2018) (***MyRepublic***);

(ii) *Re Credit Bureau (Singapore) Pte Ltd* [2018] SGPDPC 14 (issued 14 May 2018) (***Credit Bureau***);

(iii) *Re Management Corporation Strata Title Plan No. 4436* [2018] SGPDPC 18 (issued 2 August 2018) (***MCST Plan No. 4436***);

(iv) *Re Bud Cosmetics* [2019] SGPDPC 1 (issued 3 January 2019) (***Bud Cosmetics***); and

(v) *Re Singapore Health Services Pte. Ltd. and anor* [2019] SGPDPC 3 (issued 14 January 2019) (***SingHealth***).

MyRepublic

Background

The PDPC received a complaint from a member of the public (***Complainant***) regarding the use of his personal data for debt recovery. MyRepublic had engaged a debt collection company to pursue the payment of outstanding amounts allegedly due to it. The debt collection company contacted the Complainant once by letter and once by phone call within the span of 8 days.

However, as the Complainant alleged that he did not actually have any outstanding debt to MyRepublic, he lodged a complaint with the PDPC on the grounds that MyRepublic did not have his consent to use his personal data for debt collection purposes.

PDPC's Decision

The PDPC found MyRepublic not to be in breach of the section 13 of the PDPA (***Consent Obligation***). The Consent Obligation requires either that (a) the individual gives, or is deemed to have given, his consent to the collection, use, or disclosure of his personal data; or that (b) collection, use, or disclosure without consent is required or authorised under the PDPA or any other written law.

The PDPC found that the Complainant had validly given consent for the use of his personal data for debt collection purposes, by using MyRepublic's

services pursuant to their terms and conditions of service.

Investigations showed that administrative time-lag in MyRepublic's systems caused MyRepublic to deem that the Complainant was in debt. The Complainant had terminated his account with MyRepublic on 25 September 2016, and his payment of outstanding amounts owed to MyRepublic was processed via bank GIRO on 28 September 2016. However, MyRepublic only received the bank GIRO report on 29 September 2016, and updated their debt records only on 30 September 2016. In the meantime, MyRepublic had generated a debt aging report as of 29 September 2016, at which point the Complainant's account was still tagged as being in debt and his personal data sent to the debt collection agency for action.

The PDPC found that such batch processing with weekly updating of customers' account status was a reasonable practice. It therefore declined to find that MyRepublic was in breach of the PDPA.

The decision can be accessed **here**.

Key Takeaways

The PDPC noted that while the PDPA imposes data protection obligations on organisations, the PDPA does not "demand infallibility in an organisation's personal data processing activities and systems". Instead, the PDPA requires organisations to do what is reasonable to fulfil their obligations under the PDPA. Therefore, even if accounts were mistakenly tagged, the PDPC may not find organisations to be in breach if they can show that their processing systems incorporated reasonable measures to ensure accuracy in personal data.

Credit Bureau

Background

The PDPC received a complaint from a member of the public (***Complainant***) regarding the accuracy and retention of his personal data by Credit Bureau. Credit Bureau, a consumer credit bureau, is in the business of aggregating credit-related information from its members to generate risk profiles of individuals in its Enhanced Consumer Credit Report (***ECCR***).

The Complainant had had a bankruptcy application taken out against him in June 2012, but the application was subsequently withdrawn in July 2012. Nonetheless, Credit Bureau gave him a "HX" risk grade in the ECCR, indicating that there could be a past or existing bankruptcy record associated with the complainant. The Complainant took issue with the "HX" risk grading, as he thought it implied that he was either an outstanding bankrupt or was not creditworthy, and requested that Credit Bureau amend his risk grading. Credit Bureau declined to do so, stating that it was its practice to display bankruptcy-related data for 5 years. The Complainant lodged a complaint with the PDPC.

The PDPC's Decision

The PDPC found that Credit Bureau was not in breach of either section 23(b) of the PDPA (***Accuracy Obligation***) or section 25 of the PDPA (***Retention Obligation***). The Accuracy Obligation requires organisations to make reasonable efforts to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be disclosed by the organisation to another organisation. The Retention Obligation requires an organisation to cease to retain its documents containing personal data, or to remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose for which that personal data was collected is no longer being served by the retention of the personal data, and (b) retention is no longer necessary for legal or business purposes.

The PDPC noted that, for Credit Bureau's business purposes, the "HX" risk grading was accurate as it merely meant that there was a past or existing bankruptcy record associated with the graded individual, and not that that individual was a bankrupt. Furthermore, Credit Bureau also cautioned creditors against upfront rejection of credit applications on the basis of the "HX" risk grading, reinforcing its position that the "HX" risk grading alone did not determine creditworthiness. Also, according to the Association of Banks in Singapore, financial institutions would consider information from multiple sources before making lending decisions, and not rely solely on the ECCR.

In addition, Credit Bureau's display of bankruptcy-related information for 5 years in its ECCR,

including "HX" risk gradings, aligned with the display period of the publicly available Insolvency Search maintained by the Insolvency and Public Trustee Office. Noting that the 5-year policy facilitated financial institutions' lending decisions by allowing them to obtain the credit history of potential borrowers, the PDPC found that Credit Bureau, as a credit reporting service, had a valid business purpose in a 5-year display and retention period. Such retention was therefore not unreasonable.

The decision can be accessed **here**.

MCST Plan No. 4436

Background

The PDPC received a complaint from two subsidiary proprietors (***Complainants***) of the River Isles condominium, managed by MCST Plan No. 4436 (***Organisation***), regarding the Organisation's permission for another subsidiary proprietor to view CCTV footage in the presence of two council members but without the presence of a security supervisor.

The Complainants were concerned that there might be other individuals captured in the CCTV footage, and asserted that only security guards, the staff of the managing agent, or police could view the CCTV footage, and not other subsidiary proprietors or even the organisation's council members. In reply, the Organisation argued that section 47 of the Building Maintenance and Strata Management Act (***Inspection Right***) applied, giving any subsidiary proprietor the right to ask for inspection as well as request a copy of any other record or document in the possession of the management corporation, i.e., the Organisation. The Organisation therefore took the view that the Inspection Right gave the subsidiary proprietor the right to view the CCTV footage.

The PDPC's Decision

The PDPC found the Organisation not to be in breach of section 21(3)(c) of the PDPA (***Access Obligation***), having regard to section 4(6)(b) of the PDPA (***Subordination Provision***) read together with the pleaded Inspection Right. The Access Obligation requires that an organisation shall not provide an individual with the individual's personal data or other information if the provision of that personal data or other information, as the case may be, could reasonably be expected to, among others, reveal personal data about another individual. The Subordination Provision, however, provides that save where expressly provided, the provisions of other written law shall prevail to the extent that any provision of Parts III to VI of the PDPA is inconsistent with the provisions of that other written law.

The PDPC found that the CCTV footage was a record within the meaning of the Inspection Right, and also that the Inspection Right was inconsistent with the Access Obligation. The Inspection Right contained no restrictions on a subsidiary proprietor's right to inspect and take copies of any document or record, i.e. the CCTV footage. For example, it was not necessary to redact any such requested documents or records to obviate any personal data that might have been contained within. On the other hand, the Access Obligation contained obligations imposed on the Organisation to decline to disclose personal data about a data subject if that disclosure would also divulge, among others, the personal data of other persons.

The PDPC therefore noted that when the Inspection Right was being invoked by a subsidiary proprietor (as was the case), the Subordination Provision would operate to permit the Organisation to provide the relevant documents for inspection without the necessity of redacting any personal data as would otherwise be required by the Access Obligation. Therefore, on the facts, the Organisation was not in breach of the PDPA.

However, the PDPC also made two further points on the application of the Inspection Right. First, the Subordination Provision only operated to subordinate the Access Obligation to the Inspection Right when the Inspection Right was validly invoked by a person properly entitled to it. The Organisation should treat other inspection requests as access requests solely under the Access Obligation. Second, the PDPC clarified its earlier decision of *Re Exceltec Property Management and others* [2017] SGPDPC 8 (***Re Exceltec***), stating that Re Exceltec did not hold that any document sought to be inspected under the Inspection Right was publicly available and therefore exempt from the PDPA.

The decision can be accessed **here**.

Key Takeaways

Management corporations should be careful about relying on the Inspection Right as a broad excuse for non-compliance with the PDPA, and should implement policies and practices to ensure that personal data is not disclosed in excess of what would be required under the Inspection Right. In this connection, management corporations would be well-advised to have regard to the PDPC's newly-released Advisory Guidelines for MCSTs.

Bud Cosmetics

Background

The PDPC received a complaint from a member of the public regarding the publication of a list of approximately 2,300 of Bud Cosmetics' members online (***Member List***). The Member List was kept in an online image folder typically used for newsletter distribution that was not secured, and was therefore subsequently indexed by search engines and publicly available online.

Apart from a possible breach of section 24 of the PDPA (***Protection Obligation***), the PDPC's investigations also indicated possible breaches of section 12 (***Openness Obligation***), as Bud Cosmetics did not appear to have a suitable privacy policy in place, as well as section 26 (***Transfer Limitation Obligation***), as Bud Cosmetics appeared to have hosted personal data on servers in Australia and the United States.

The PDPC's Decision

The PDPC found Bud Cosmetics to be in breach of the Protection, Openness, and Transfer Limitation Obligations. The Protection Obligation requires organisations to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or other similar risks to personal data in its possession or under its control. The Openness Obligation requires organisations to, among others, develop and implement policies and practices necessary for the organisation to meet its obligations under the PDPA. The Transfer Limitation Obligation requires that organisations not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA (namely, the Personal Data Protection Regulations (S 362/2014)) to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

In relation to the Transfer Limitation Obligation, it was undisputed that Bud Cosmetics had engaged an Australian and then a US service provider to host its website, and personal data was hosted on their servers outside of Singapore. As Bud Cosmetics was ignorant of its obligations under the PDPA, it did not consider the location of the web hosting servers to be a relevant factor when it engaged the service providers. It therefore failed to consider whether the laws in the service providers' jurisdictions afforded personal data with protection comparable to that under the PDPA. The PDPC noted that this failure to consider the data protection laws in the recipient jurisdictions was itself sufficient to put Bud Cosmetics in breach of the Transfer Limitation Obligation under the PDPA.

The PDPC's Actions

The PDPC's directions to Bud Cosmetics, in order to ensure compliance with the PDPA, were therefore as follows:

(i) to pay a financial penalty of S$11,000;

(ii) to engage duly qualified personnel to conduct a security audit of its website and IT system and to furnish a schedule stating the scope of risks to be assessed and the time within which a full report of the audit can be provided to the PDPC, within 30 days of the date of the PDPC's directions;

(iii) to develop an IT security policy to guide its employees on the security of personal data on its website and IT system, within 60 days of the date of completion of the above security audit; and

(iv) to implement a training policy for its employees handling personal data to be trained to be aware of, and to comply with the requirements of the PDPA when handling personal data, and to require all employees to attend such training within 90 days from the date of the PDPC's directions.

The decision can be accessed **here**.

Key Takeaways

When engaging service providers, organisations should be mindful of whether the services will involve the transfer of personal data to jurisdictions outside of Singapore. If so, organisations should undertake an assessment of the personal data protection laws in those jurisdictions to determine if the protections afforded to personal data are comparable with the protections under the PDPA. If the protections under the recipient jurisdictions are not comparable, the organisation should then consider whether it can impose contractual safeguards to ensure such comparable protection, or whether it should source for alternative service providers able to provide such comparable protection.

SingHealth

Background

In the wake of the public announcement on 20 July 2018 by the Ministry of Communications and Information and the Ministry of Health (***MOH***) that SingHealth's patient database system had been the target of an unprecedentedly massive cyber attack (***Data Breach***), the PDPC received several complaints from members of the public in relation to the Data Breach, and commenced its own investigations thereafter.

The relationship between SingHealth and its IT service provider, Integrated Health Information Systems (***IHiS***), was not a straightforward contractual service provision relationship. Pursuant to policy actions by MOH in consolidating IT services across public healthcare institutions (***PHIs***), IT staff from all PHIs were consolidated into IHiS in 2008, and then seconded back to PHIs to provide IT support services. This included the SingHealth Group Chief Information Officer (***GCIO***) and the Cluster Information Security Officer (***CISO***), as well as their support staff, who were all staff of IHiS at the material time. Because of this unique arrangement, it was not immediately clear with which organisation – SingHealth or IHiS – responsibility for the actions of IHiS staff seconded to SingHealth lay.

The PDPC's Decision

The PDPC considered the roles of the GCIO and CISO in relation to SingHealth and IHiS, and noted that while the GCIO and CISO were IHiS employees and did owe duties and responsibilities to IHiS, the fact that they were carrying out functions within SingHealth's organisational structure and performed work on behalf of SingHealth meant that their actions should be attributed to SingHealth rather than IHiS.

Considering that SingHealth had outsourced data processing activities to IHiS, the PDPC reviewed generally SingHealth's security arrangements to determine if SingHealth had sufficient security arrangements in place to supervise IHiS' processing of personal data on its behalf. The PDPC found that where the SingHealth CISO had failed to discharge his duties, this failure was not a one-off incident that was difficult to foresee. Rather, the SingHealth CISO's failure to discharge his duties was part of a systemic problem with SingHealth's organisational structure.

The PDPC found that given the size and scale of SingHealth's IT systems and networks, and the large databases of sensitive medical personal data that SingHealth was responsible for, it would have been reasonable to expect that the SingHealth CISO would have been supported with considerable resources. However, the SingHealth CISO worked alone and had no staff reporting to him, which meant that there was no one to cover the CISO's duties while he was away on medical leave during the investigation. For this reason, the PDPC found that SingHealth had failed to put in place reasonable security arrangements to protect the personal data in its possession or under its control from unauthorised access and copying.

In relation to IHiS, the PDPC noted that, by IHiS' own admission, there were gaps in the implementation of its own security measures, such as failures to comply with such measures on the ground, and IHiS had not taken steps to remediate and address such vulnerabilities as had been surfaced from time to time. The PDPC therefore found that IHiS had failed to take sufficient security steps or arrangements to protect the personal data under its control from unauthorised access, collection, use, disclosure, and copying.

The PDPC's Actions

The PDPC imposed a financial penalty of S$750,000 on IHiS and a financial penalty of S$250,000 on SingHealth. Noting that these were the largest and second-largest financial penalties to be imposed to date, the PDPC considered that

the following factors rendered the size of the penalty appropriate.

First, this was the largest data breach with almost 1.5 million unique individuals affected. Second, while the data of 1.5 million people was actually exfiltrated, the data of over 5.01 million individuals was put at risk. Third, especially sensitive data in the form of the Dispensed Medication Records of 159,000 unique individuals was also disclosed, from which it could be possible to deduce conditions for which a patient was being treated, including serious or socially embarrassing illnesses.

The decision can be accessed **here**.

Key Takeaways

Large organisations which purport to already take IT security seriously should not be complacent as to the adequacy of the existing measures. It is important to conduct periodic reviews of the actual implementation of its IT security policies on the ground, particularly since such organisations are more likely to hold a large volume of personal data that might include sensitive personal data like financial information. In addition, it is insufficient to simply designate someone to be responsible for IT security; sufficient organisational resources must also be devoted to ensuring that any designee is able to carry out his duties to a level commensurate with the personal data within the organisation's possession and control.

Other Decisions

Court rules Singapore Swimming Club did not defame woman or breach data protection laws by publishing notice labelling her a trespasser

On 19 February 2019, the State Court dismissed a claim brought by a woman (the ***Applicant***) against the Singapore Swimming Club (the ***Club***) for defamation and breach of the PDPA.

The case concerned the Applicant's visit to the Club on 1 June 2017, as an invited guest of a member of the Club (the ***Member***). This was the Applicant's third visit to the Club. According to the Club's rules, all guests were required to sign in but the Applicant had omitted to do so as the Member had left to attend to personal matters upon his arrival at the Club without informing the Applicant. Subsequently, the Club discovered the lapse and downloaded a photo of the Applicant from its CCTV cameras. In accordance with the Club's zero-tolerance policy, the Club displayed the Applicant's photo and listed her name on the Club's notice board, which declared her as *personae non grata* for trespassing on the Club's premises.

Against the above backdrop, the Applicant instituted legal proceedings against the Club for defamation, and more pertinently, for breaches of the PDPA in publishing her name and photo in the notice without her consent.

In his oral grounds of judgment, District Judge Loo Ngan Chor dismissed the Applicant's claims in their entirety. In particular, the judge ruled that there was no contravention of the PDPA as the Applicant had given or was deemed to have given her consent to the Club's data protection policy through her previous two visits to the Club.

Written grounds of judgment are not available as at the time of writing. Notwithstanding, this case is significant as it appears to be the first time where the Singapore courts was asked to consider whether there was a breach of the PDPA and the PDPC did not make any decision in respect of any purported contravention of the PDPA by the Club.

PDPC publications on data protection topics: April 2018 – June 2019

Between April 2018 and June 2019, the PDPC issued several updates on data protection topics:

(i) Advisory Guidelines for MCSTs (published 11 March 2019);

(ii) Public Consultation Paper on Data Portability (published 22 May 2019);

(iii) Proposed Model AI Governance Framework (published 23 January 2019);

(iv) Data Protection Trustmark Certification (published 9 January 2019);

(v) Response to the Public Consultation for Managing Unsolicited Messages and the Provision of Guidance to Support Innovation in the Digital Economy (published on 8 November 2018);

(vi) Announcements on NRIC Rules to Enhance Consumer Protection (published 31 August 2018); and

(vii) Guide for Printing Processes for Organisations (published 3 May 2018).

We highlight the key updates below.

Data Protection Trustmark Certification

On 9 January 2019, the PDPC launched the Data Protection Trustmark Certification (***DPTM Certification***), as part of advancing Singapore's digital economy as a trusted data hub that supports competition, innovation, and the cross-border flow of data.

The key objectives of the DPTM Certification are for organisations to demonstrate sound and accountable data protection practices, to enhance and promote consistency in data protection standards across all sectors, to provide a competitive advantage for businesses that are certified, and to boost consumer confidence in organisations' management of personal data.

The DPTM certification is a voluntary enterprise-wide certification looking at an organisation's standard of data protection policies, processes, and accountability practices. The DPTM certification is valid for 3 years, and organisations will need to reapply at least 6 months from the date of expiry of the certification.

Further information on the DPTM Certification can be accessed **here**.

Response to the public consultation for managing unsolicited messages and the provision of guidance to support innovation in the digital economy

On 8 November 2018, the PDPC issued its Response to Feedback on the Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy (***Response***).

Review of DNC Provisions and the SCA

(a) Scope and applicability

In the original Public Consultation, the PDPC had proposed to merge the PDPA's Do-Not-Call provisions (***DNC***) with the Spam Control Act (Cap. 311A) (***SCA***) under a new Act (***New Act***). The DNC would continue to apply to specified voice, text, and fax messages while the SCA provisions would continue to apply to emails sent in bulk. In addition, the DNC under the New Act would apply also to unsolicited marketing calls and text messages to Singapore telephone numbers, whether in bulk or otherwise, and the SCA provisions would extend to unsolicited commercial text messages where addressed to instant messaging identifiers and were sent in bulk.

As a result of the public consultation, the PDPC further issued three clarifications. First, in relation to IM platforms where a sender had to be added by a user before the sender could send a commercial text message, the commercial text message would be considered unsolicited and the SCA provisions would apply if sent in bulk. Second, the New Act would not apply to in-app notifications or a mobile device's notification feature. Last, the New Act's provisions would not be limited to unsolicited marketing and commercial messages sent via text but would also apply to images, videos, and audio files.

(b) Period for effecting withdrawal requests

In response to feedback over the sudden streamlining of DNC requests from 30 days to 10 days, the PDPC proposed to reduce the time

period in two phases, first to 21 days, then to 10 days. The PDPC also noted that the prescribed duration of validity for DNC Registry checks would correspondingly be reduced, and that it would be reviewing the pricing mechanism for DNC Registry checks in view of the increased compliance costs.

(c) Dictionary attack and address harvesting software

The PDPC proposed to prohibit the sending of commercial messages to telephone numbers, IM identifiers, and email addresses generated by or obtained through the use of dictionary attacks or address harvesting software, and for these provisions to be enforced as an administrative regime.

The PDPC also further clarified that senders would be liable for the use of mailing lists generated through dictionary attack or address harvesting software, regardless of whether the use of such software is carried out by a human or through automated means. However, organisations would not be prohibited from using address harvesting software on their own database.

(d) Enforcing DNC breaches under an administrative regime

The PDPC also stated that it intended to enforce the DNC under an administrative regime, with egregious breaches still prosecutable as criminal offences with similar defences as at present, and with affected individuals and organisations continuing to have the right to take private action under the New Act.

(e) Liability of third-party DNC checkers and resale of DNC Registry lists

The PDPC originally proposed to impose an obligation on third-party checkers to ensure the accuracy of DNC registry lists, and to prohibit the reselling of lists of telephone numbers screened through DNC Registry. However, in response to feedback, the PDPC stated that it would not prohibit the resale of lists of telephone numbers screened through the DNC Registry, as it was persuaded that the prohibition would not be necessary if third-party checkers are already legally obliged to provide accurate DNC Registry results. The resale of telephone numbers would also be subject to the Consent and Notification Obligations under the PDPA.

Enhanced Practical Guidance

(a) Criteria and scope of the EPG Framework

The PDPC also proposed a framework under which it would provide Enhanced Practical Guidance (***EPG***) to businesses seeking guidance on complex compliance queries with regulatory certainty (***Determinations***) as to whether a particular business activity complied with the PDPA. The PDPC proposed to exclude hypothetical queries or queries that entailed a review of the organisation's entire business model from the EPG framework, and to assess requests for Determinations based on three criteria:

(i) that the query relates to a complex or novel compliance issue for which there is currently no clear position for its treatment under the PDPA;

(ii) the query cannot be addressed by PDPC's general guidance and existing published resources; and

(iii) the query does not amount to a request for legal advice.

In response to queries, the PDPC clarified that it would provide Determinations for proposed activities that were more than just exploratory, and Determinations could be sought by professional advisors or by industry bodies on behalf of organisations. The PDPC also further clarified that it intended to further issue a guide to provide clarity on the types of queries that may or may not satisfy the criteria for a Determination under the EPG framework.

(b) Validity and effect of EPG Determinations

The PDPC proposed that Determinations generally remain valid unless there have been changes made to the PDPA relevant to the Determination, or the information provided by the organisation is false, misleading, or no longer accurate. In addition, the PDPC would forbear from initiating investigations in the event that it found non-compliance with the PDPA solely on the information submitted for the purpose of the Determination. However, the PDPC reserves the right to terminate a Determination assessment in the event that it receives a complaint during the course of the assessment. In response to queries,

the PDPC further clarified that only the requesting organisation can rely on the Determination, and that Determinations would have a validity period, on the condition of there being no changes to the basis to the Determination.

(c) Publication of EPG, fees, and timeframe

The PDPC proposed to publish redacted versions of its Determinations on a case-by-case basis to raise awareness. The PDPC also proposed to charge organisations according to the type and size of the organisation, to ensure that EPG costs were not prohibitive for SMEs and start-ups. The PDPC further clarified that it will take into account factors such as the size and number of organisations involved in the EPG application, as well as the complexity of the query. More details and guidance on the administrative and procedural issues relating to the EPG application and assessment process, including the fee structure, will be set out in the guide on the EPG framework.

Key Takeaways

With the New Act and the EPG Framework, organisations can look forward to a streamlining of their compliance obligations, as well as access to a liability-free means of determining their compliance with the PDPA. Conversely, easier compliance and access to means of determining compliance may also mean that failures to comply will be looked upon less favourably.

NRIC rules to enhance consumer protection

On 31 August 2018, the PDPC released three documents related to the use of NRIC and other national identification numbers under the PDPA:

(i) the Closing Note on the Public Consultation on the Proposed Advisory Guidelines on the PDPA for NRIC Numbers (***NRIC Closing Note***);

(ii) Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (***NRIC Advisory Guidelines***); and

(iii) the Technical Guide to Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (***NRIC Technical Guide***).

Together, these three documents establish what is considered to be acceptable practice in relation to the collection of NRIC numbers and other national identifier numbers such as Work Permit numbers, FIN, and Birth Certificate numbers. As these national identification numbers are permanent and irreplaceable identifiers that can be used to unlock large amounts of information relating to the individual, the collection, use, and disclosure of such numbers is of special concern. Therefore, organisations will generally not be allowed to collect, use, or disclose national identification numbers.

NRIC advisory guidelines

The NRIC Advisory Guidelines provides an in-depth examination of the application of the PDPA to the collection, use, and disclosure of NRIC numbers and physical NRICs, and provides examples of several scenarios involving the collection, use, and disclosure of NRIC numbers and physical NRICs.

The NRIC Advisory Guidelines lay down the principle that organisations are generally not allowed to collect, use, or disclose NRIC numbers or copies of NRICs, save in the following two circumstances:

(i) where such collection, use, or disclosure is required under the law (or an exception to the PDPA applies), or

(ii) where such collection is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

In relation to the second exception, the PDPC further stated that it would generally consider it necessary to accurately establish or verify the identity of the individual to a high degree of fidelity in two situations. First, where the failure to accurately identify the individual to a high degree of fidelity may pose a significant safety or security risk, e.g., visitor entry to preschools where ensuring the safety and security of young children is an overriding concern. Second, where the inability to accurately identify an individual to a high degree of fidelity may pose a risk of significant impact or harm. This includes reputational, financial, personal, or proprietary damage, to an individual or the organisation, e.g., healthcare, financial or real estate matters,

insurance applications and claims, financial aid, credit checks, and medical check-ups and reports. The NRIC Advisory Guidelines also state that given the importance of the NRIC and the impact to an individual should the physical NRIC be misplaced, stolen, or used illegally, organisations should not retain an individual's physical NRIC unless its retention is required under the law.

The NRIC Advisory Guidelines suggest several alternative identifiers that organisations should adopt in place of NRIC numbers, such as organisation or user-generated IDs, tracking numbers, organisation-issued QR codes, or monetary deposits. In addition, the PDPC recognises that the collection of partial NRIC numbers will not be treated as collection of the full NRIC numbers and the NRIC Advisory Guidelines would not apply. Nevertheless, organisations should be mindful that the personal data risks associated with the collection of NRIC numbers are still present when partial NRIC numbers are collected.

The interpretation of the PDPA in Part II of the NRIC Advisory Guidelines will be applied by the PDPC from **1 September 2019**.

NRIC technical guide

The NRIC Technical Guide provides in-depth practical guidance on the following topics: the alternatives in place of collecting NRIC numbers, the measures to replace the existing use of NRIC numbers in systems and databases, and the scanning of NRIC numbers.

The NRIC Closing Note can be accessed **here**, the NRIC Advisory Guidelines can be accessed **here**, and the NRIC Technical Guide can be accessed **here**.

Key Takeaways

Organisations should begin assessing their operations for compliance with the NRIC Advisory Guidelines and Technical Guide as a matter of priority, as 1 September 2019 is fast approaching. In addition, given greater public awareness of personal data protection in general and the NRIC Advisory Guidelines in particular, organisations should be prepared to justify its collection, use, and disclosure of NRIC numbers, if it is not presently exempted under one of the exceptions in the Advisory Guidelines.

Guide to printing processes

Following a spate of cases involving errors made in mass post processes, which resulted in letters containing personal data sent to the wrong recipients, the PDPC released a Guide for Printing Processes for Organisations (***Printing Processes Guide***) on 3 May 2018. The Printing Processes Guide provides practical guidance on how to achieve compliance with the PDPA at various stages of the printing lifecycle, such as setting up, pre-printing, printing, enveloping, mailing, and e-mailing via mail merge. The Printing Processes Guide also discusses other pertinent considerations for printing processes, which includes data retention, maintenance, disposal of personal data, the management of data breach incidents, and key considerations for outsourcing and data transfer.

The Printing Processes Guide can be accessed **here**.

ASEAN

Brunei to implement new laws to tackle cybersecurity threats

On 10 January 2019, Brunei's Attorney General announced that the Attorney General's Chambers is working closely with other government agencies in Brunei to draft new legislation in respect of the monitoring and efficient reporting of cybersecurity threats. The new cybersecurity laws will also introduce a licensing regime that will regulate the control of data security by telecommunications networks and data security providers.

Indonesia Government publishes new version of draft data protection law

In May 2018, the Indonesian government issued a new draft personal data protection law (***Draft Law***) in light of recent data breaches, which would have extraterritorial reach.

Amongst others, the Draft Law makes a distinction between categories of personal data, introduces the concepts of data controller and data processor, and provides certain rights to individuals such as the right to make a written request to data controllers to stop using their personal data for direct marketing activities.

A breach of the Draft Law may lead to criminal and administrative sanctions. The Draft Law will establish a commission which will administer the Draft Law, and whose powers include issuing orders to cease infringing activities, to delete personal data and to stop unauthorised use of personal data. The commission will also have powers to impose monetary penalties for any breaches of the Draft Law. There are also criminal sanctions for serious offences under the Draft Law, such as personal data forgery and the unauthorised sale of personal data.

Malaysia publishes a public consultation paper on the implementation of Data Breach Notification

The Malaysia Personal Data Protection Act applies to all companies operating in Malaysia, and includes persons not established in Malaysia if they use equipment in Malaysia for the processing of personal data other than for the purposes of transit through Malaysia.

On 7 August 2018, Malaysia's Department of Personal Data Protection issued a Public Consultation Paper (No. 1/2018) entitled "The Implementation of Data Breach Notification" (***Consultation Paper***), which is intended to seek feedback from data users and other relevant parties on personal data breach management, in particular, the implementation of a data breach notification requirement.

Under the Consultation Paper, the Personal Data Protection Commissioner (***Commissioner***) is to be notified within 72 hours of the data user being aware of a data breach. In the notification to the Commissioner, data users must provide a summary of the data breach and its circumstances, the type and amount of personal data involved and the estimated number of affected data subjects.

The notification should also describe on the method in which affected data subjects are notified and the advice given to such data subjects.

In addition, the notification should state whether the data user had provided personal data protection training programmes to staff members prior to the data breach, and in particular, whether the staff members involved in the incident received training in the last 24 months and received any detailed guidance on the handling of personal data.

The data breach notification requirement is expected to be implemented by way of imposing conditions to the certificate of registration issued by the Commissioner to data users registered under the Personal Data Protection (Class of Data Users) Order 2013.

Philippines National Privacy Commission releases updated templates on security incident and personal data breach reporting requirements

On 26 June 2018, the Philippines' National Privacy Commission (***NPC***) issued Advisory No. 2018-02 (Updated Templates on Security Incident and Personal Data Breach Reportorial Requirement) (***Advisory***). The Advisory is applicable to personal information controllers and processors in the public and private sector, which are processing personal data within and outside the Philippines.

The Advisory provides updated templates for the reportorial requirements of the NPC on security incidents and data breaches, which include:

(i) annual security reports to be submitted to the NPC by personal data controllers and processors at the end of the first quarter of the succeeding calendar year; and

(ii) mandatory notifications to the NPC and affected data subjects in the event of data breaches in accordance with the mandatory notification requirements under the Philippines' Data Privacy Act of 2012.

In the annual security report, personal data controllers and processors are required to give a summary of the number of security incidents that occurred in the year and categorise these security incidents by type.

In the mandatory notification to the NPC, an organisation affected by data breaches is to list down the details of the head of the organisation, its data protection officer, and those involved in the data breach. In addition, the notification should include a brief description of the nature and the likely consequences of the data breach, as well as a list of all the sensitive personal data involved. Lastly, the organisation is to expressly indicate the measures taken to address the data breach, the effectiveness of such measures, and the steps taken to inform the affected data subjects and to prevent a recurrence of the data breach.

Philippines passes the Mobile Number Portability Act

On 8 February 2019, President of Philippines, Rodrigo Duterte, signed the Mobile Number Portability Act (***Act***), which will allow mobile phone users to retain their existing numbers even after they switch service providers. The Act takes effect 15 days after its publication in the Official Gazette or in any newspaper of general circulation. The National Telecommunications Commission, working with other government agencies, is charged with promulgating the Act's implementing rules and regulations, within 90 days from the effective date of the Act. Within six months of the promulgation of these rules and regulations, telecommunications service providers are to comply with the provisions of the Act.

In a public statement released on 20 February 2019, the National Privacy Commission of Philippines (***NPC***) noted that the Act will give data subjects control over their data which is consistent with the right of data portability under the Philippines' Data Privacy Act of 2012.

Under the Act, telecommunications service providers risk a fine between 10,000 pesos (approximately S$720) and 1 million pesos (approximately S$72,000) for failing to comply with the requirements under the Act, and may also lose their operating licences.

Thailand National Legislative Assembly passes Personal Data Protection Act and Cybersecurity Bill

Personal Data Protection Act

On 28 February 2019, Thailand's Personal Data Protection Act (***Thai PDPA***) was approved and endorsed by the Thai National Legislative Assembly. Upon being signed by the Thai King and published in Thailand's Gazette, it will become the first consolidated law generally governing data protection in Thailand. The Thai PDPA establishes the Personal Data Protection Commission which will oversee the administration and enforcement of the PDPA.

The principal legal basis for the collection, use and/or disclosure of personal data under the Thai PDPA is consent. In particular, personal data can only be collected if the data owner provided

consent for such collection, and the collection is for a lawful purpose and is directly relevant to, and necessary for, the activities of the data controller.

On or before the collection of a data owner's personal data, he/she must be informed of the purpose of the collection, the personal data to be collected and their retention periods, persons to whom the personal data may be disclosed, the contact information of the data controllers and the rights of the data owner, among others.

The rights of a data owner include (but are not limited to) the right to withdraw consent to the future collection of personal data (but does not affect the collection, use or disclosure of personal data that has already been consented to), the right to request access or make a copy of their personal data, the right to request the deletion or destruction of his/her personal data, and the right of correction.

The Thai PDPA has extraterritorial effect and will apply to the collection, use or disclosure of personal data, whether in Thailand or elsewhere, by the data controller or processor which resides in Thailand. In addition, it also applies to persons residing outside of Thailand if these persons offer products or services to the data owner residing in Thailand.

A breach of the Thai PDPA may result in civil, criminal and administrative forms of liability. In particular, the PDPC may levy a fine not exceeding 5 million Baht (approximately over S$200,000) for breaches of the Thai PDPA.

Cybersecurity Bill

The Thailand National Legislative Assembly also approved and endorsed the Cybersecurity Bill (***Cybersecurity Bill***) on 28 February 2019. The Cybersecurity Bill will also establish a National Cybersecurity Committee, with the authority to gather information, documents and witnesses to support analyses on cyber threats.

Under the Cybersecurity Bill, private organisations may be deemed as "critical information infrastructure organisations" (***CIIO***) within the meaning of the Cybersecurity Bill if they use computer systems to maintain national security, public security, national economic security or fundamental infrastructure for public interest. CIIOs are required to comply with certain obligations under the Cybersecurity Bill, including but not limited to the following:

- provide names and contact information of the person(s) possessing / monitoring the computer system;
- comply with the code of practice and minimum cybersecurity standards;
- conduct risk assessment; and
- notify the relevant authorities of any cyber threats

In addition, the relevant Thai authorities have certain powers in respect of private organisations which are not CIIOs, including, requiring such organisations to (i) provide access to relevant computer data or a computer system, or other information related to the computer system to the extent necessary to prevent cyber threats; (ii) monitor the computer or computer system; and (iii) allow Thai government officials to test the operation of the computer or computer system, or seize or freeze a computer, a computer system, or any equipment.

Thailand's cabinet approves the draft Digital Identification Bill

On 11 September 2018, the draft Digital Identification Bill (***Digital ID Bill***) was approved in-principle by the Cabinet of Thailand. The Digital ID Bill is expected to be passed by Thailand's National Legislative Assembly and come into effect by mid-2019.

One of the principal aims of the Digital ID Bill is to establish a platform (***Digital ID Platform***) for which an organisation may electronically authenticate the identity of end-users, by relying on existing information and Know-Your-Client (***KYC***) results previously obtained by a licensed third-party digital identification service provider (***IDP***). The Digital ID platform thus allows businesses to share KYC results and eliminates the need to conduct duplicative KYC checks.

The Digital ID Bill also establishes a 12-member National Digital Identification Committee to supervise the Digital ID Platform, and to set terms and conditions governing the use of the Digital ID Platform. A company that seeks to become an IDP under the Digital ID Bill must first obtain a licence

from the Minister of Digital Economy and Society, and would be subject to foreign ownership requirements.

Vietnam's National Assembly passes new cybersecurity law, effective as of 1 January 2019

On 12 June 2018, Vietnam's National Assembly passed the Law on Cybersecurity (***Cybersecurity Law***), which is effective as of 1 January 2019. Among other objectives, the Cybersecurity Law seeks to regulate activities of protecting national security and ensuring social order and safety in cyberspace.

The Cybersecurity Law will apply to all agencies, organisations and individuals involved in the protection of cybersecurity, and would also apply to domestic and foreign companies that provide services on a telecommunications network, the Internet and other services in cyberspace in Vietnam which collect, exploit, analyse and process certain types of data of users in Vietnam. Foreign companies that violate the law, or allow users to commit cyberattacks or cybercrimes that threaten national security or public order are expected to establish branches or representative offices in Vietnam.

Similar to legislative regimes in Russia and China, online service providers are required to comply with prescribed data localisation and data retention requirements. For instance, in respect of personal data belonging to service users residing in Vietnam, the service provider is required to retain the personal data for the duration in which the service provider continues to provide its online services. Data created or uploaded by users and data regarding the relationships of users are required to be stored for at least 36 months, and system logs must be stored for at least 12 months. Such data must be provided to the Vietnamese government authorities upon request.

The Cybersecurity Law also states that covered companies are to submit to the government's requests to delete data deemed illegal by the state. Such illegal data includes forms of criticism or dissenting statements made against the government, content deemed to encourage political or socioeconomic activism, or false information in certain sectors such as finance, banking and e-commerce. Companies are to remove illegal content within 24 hours of being notified by the government and take preventive measures against any reoccurrence.

In addition, the Cybersecurity Law requires online service providers to notify users should there be an occurrence or possible occurrence of damage or loss to user data. Under the Cybersecurity Law, any agency, organisation or individual which detects any act of cyberterrorism or certain cybersecurity attacks are required to notify the relevant Cybersecurity Task Force.

EUROPEAN UNION

EDPB publishes draft guidelines on territorial scope of the GDPR

Following the Third and Fourth Plenary Sessions of the European Data Protection Board (***EDPB***) held in September and November 2018, new draft guidelines on the territorial scope of the GDPR were adopted and published (*Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, or ***Article 3 Guidelines***). The Article 3 Guidelines provide a common interpretation of the territorial scope of the GDPR and clarify the application of the GDPR in various situations. In particular, organisations established outside of the EU would find the Article 3 Guidelines especially helpful when considering whether the provisions of the GDPR would be applicable to their operations, and whether they need to comply with the GDPR.

Article 3(2) of the GDPR

The GDPR applies mainly to organisations established in the EU and those that process personal data belonging to individuals in the EU regardless of where the processing itself takes place. However, Article 3(2) of the GDPR provides that an organisation based outside of the EU (e.g., in Singapore) may potentially also be subject to the GDPR if it processes personal data belonging to data subjects in the EU in the context of:

(i) offering goods or services to such individuals in the EU (whether or not payment for such goods or services is required); or

(ii) monitoring their behaviour insofar as the behaviour of such individuals takes place within the EU.

In assessing the conditions for the application of the GDPR to an organisation based outside of the EU with respect to the above activities, the EDPB recommended a twofold approach in the Article 3 Guidelines as follows:

(i) first, to determine that the processing relates to personal data of individuals who are in the EU; and

(ii) second, to determine whether the processing relates to the offering of goods or services or to the monitoring of individuals' behaviour in the EU.

(a) The location of the "data subject" in the EU

Under the first limb, the EDPB clarified that the application of Article 3(2) of the GDPR is not limited by the citizenship, residence or other type of legal status of the data subject whose personal data is being processed, on account of the fact that the GDPR applies to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This means that the location of the data subject within the EU, which is assessed at the point in time when the relevant "target" activity under the second limb takes place, is the determinative factor triggering the application of the GDPR instead.

(b) Specific offers directed to individuals in the EU or monitoring of behaviour in the EU

Notwithstanding the above, the mere fact that the personal data of an individual in the EU was processed is not sufficient to trigger the application of the GDPR to that organisation's processing activities. The organisation must "target" individuals in the EU through the offering of goods or services or alternatively, the monitoring of their behavior in the EU as well. To illustrate using an example provided in the Article 3 Guidelines, a U.S. company whose news app was downloaded and used by a U.S. citizen who was in the EU on holiday, is not subject to the GDPR if the app was exclusively targeted at the U.S. market and not the EU market.

Similarly, in cases where the data subject is an EU citizen or resident and the processing of personal data takes place outside of the EU, the EDPB underlined that the application of the GDPR may not be triggered so long as the processing is not related to a specific offer directed at individuals in the EU or to the monitoring of their behaviour in the EU. Looking at another example from the Article 3 Guidelines, a Taiwanese bank which processes the personal data of German citizens residing in Taiwan, is not subject to the GDPR if it is active only in Taiwan and its activities are not targeted at the EU market.

In this regard, the EDPB considered that there needs to be a connection between the

organisation's processing activity and the offering of goods or services, and that both direct and indirect connections are relevant and may be taken into account. For instance, elements such as the use of a top-level country domain name (e.g., ".de", or ".eu"), or the use of a language or a currency belonging to one or more EU Member States, if taken alone, may not amount to a clear indication of intention to offer goods or services. However, the combination of factors relating to the organisation's commercial activities may together be considered as an offer of goods or services targeted at data subjects in the EU.

With respect to the monitoring of data subjects' behaviour insofar as their behaviour takes place within the EU, the Article 3 Guidelines stated that the EDPB does not consider that the collection or analysis of personal data of individuals in the EU (whether online, or through other types of network or technology e.g. wearables) would automatically count as "monitoring" per se, as the use of the word "monitoring" implies that the organisation has a specific purpose in mind for the collection and subsequent reuse of data about an individual's behaviour within the EU.

In this regard, the EDPB clarified that it is necessary to consider the organisation's purpose for processing the personal data and to this end, subsequent behavioural analysis or profiling techniques involving that data would be key considerations. Based on another example from the Article 3 Guidelines, a US-based marketing company which analyses customers' movements throughout a shopping centre in France using Wi-Fi tracking for the purpose of providing advice on the shopping centre's retail layout, would be subject to Article 3(2) of the GDPR in respect of the processing of customers' data for this purpose. According to the Article 3 Guidelines, Article 3(2) of the GDPR could therefore potentially apply to a broad range of monitoring activities, including behavioural advertisements, geo-localisation activities for marketing purposes, online tracking through cookies or other tracking techniques, market surveys and other behavioural studies based on individual profiles, and monitoring or regular reporting on an individual's health status.

Designating a representative in the EU

Another key feature of the applicability of the GDPR to organisations based outside of the EU is that if Article 3(2) of the GDPR applies to their processing activities in the EU, the GDPR imposes an obligation to designate a representative in an EU Member State. Notwithstanding, under the derogations provided in the GDPR, there is no need to designate a representative in the EU if the processing activities are:

(i) occasional;

(ii) not carried out on a large-scale in respect of special or sensitive categories of data or data relating to criminal convictions or offences; and

(iii) are not likely to result in a risk to the rights and freedoms of individuals.

Where a representative is required to be designated in the EU, the EDPB has emphasised that the function of a representative is not considered to be compatible with the role of an external data protection officer (***DPO***) as appointed within the EU. This is because DPOs are supposed to act in an independent manner with a sufficient degree of autonomy within their organisations, whereas representatives perform their tasks according to the written mandate laid out by their designating organisations.

In addition, the Article 3 Guidelines confirmed that the criterion for the establishment of the representative is the location of the data subjects whose personal data are being processed, and not the place of processing, even if it is done by a processor established in another EU Member State. As a matter of good practice, that representative should be established in the same EU Member State where a significant proportion of data subjects whose personal data are processed are located.

The Way Forward

While the Article 3 Guidelines provide timely clarification and valuable illustrations, they were subject to a public consultation conducted by the EDPB from 23 November 2018 to 18 January 2019. While no further information on the outcome of the public consultation is available as at the time of writing, given the EDPB's present attempt to elucidate the interpretation and application of Article 3 of the GDPR for organisations and supervisory authorities, it is expected that any real issues of concern would be noted and duly addressed by the EDPB prior to the finalisation of the guidelines.

Significant developments in GDPR enforcement

It has been a year since the GDPR came into effect on 25 May 2018. According to the European Commission, data protection authorities across Europe received over 95,000 complaints from individuals or organisations and more than 41,000 data breach notifications by companies since the GDPR came into force. While the first GDPR fines have been relatively modest, heftier fines are generally expected in 2019 as the amnesty period for implementing the GDPR is over.

We round up some of the more notable developments in GDPR enforcement below:

Google fined €50 million under GDPR in France for GDPR violations

On 21 January 2019, the French data protection authority, Commission Nationale de l'Informatique et des Libertés (***CNIL***), issued a financial penalty of €50 million against US-incorporated Google LLC (***Google***) for breaches with respect to (i) Google's failure to communicate "essential information" to users on its processing of their personal data, and (ii) failing to obtain valid consent from users (specifically, Articles 4 and 6 of the GDPR) to process users' data for ads personalisation purposes. The decision stands out as the first major example of a European data protection authority sanctioning a company with global operations such as Google under the GDPR with a multimillion dollar fine. The decision also raised a number of important issues, which we discuss below.

Background

On 25 and 28 May 2018, CNIL received group complaints from two associations, None Of Your Business (***NOYB***) and La Quadrature du Net (***LQDN***). NOYB had, on the first day the GDPR came into force, filed four complaints against Google, Facebook, WhatsApp and Instagram. They alleged that users (in this case, Android users) were asked to agree to privacy policies which they did not understand, which constituted "forced consent" to data processing. Therefore, there was a lack of a valid legal basis for such companies to process users' personal data. Similarly, LQDN's complaint concerned the creation of an account to access Google's services, namely, that regardless of the medium (e.g., Youtube, Gmail or Search), Google did not have a valid legal basis to process users' personal data for the purposes of analysing user behaviour and personalising content and ads displayed.

The "one-stop-shop" mechanism

A preliminary aspect of the decision concerned CNIL's determination that it was competent to handle the complaints. Although the GDPR establishes a "one-stop-shop" mechanism which provides for the Data Protection Authority (***DPA***) of the country hosting the organisation's main establishment to be the lead supervisory authority in respect of that organisation's cross-border processing activities, CNIL considered that the "one-stop-shop" mechanism was not applicable in this case. Even though Google's EU headquarters is based in Ireland, CNIL determined that Google's Irish establishment did not exercise any decision-making power on the data processing operations carried out with respect to Google Android and other services. On this basis, CNIL considered that it was competent to take any decision regarding Google's data processing operations.

CNIL's findings

CNIL found two types of GDPR breaches.

First, CNIL observed that the information provided by Google was not easily accessible to users. Users had to click on multiple buttons and links, which were distributed across several documents, to access essential information regarding Google's data processing purposes, data storage periods or the categories of personal data processed for ads personalisation. CNIL also noted that the information provided by Google was not clear and comprehensive. The purposes of processing were described in generic or vague terms despite the massive scale and intrusiveness of processing operations. There was also no information regarding data storage periods for some types of data. The lack of accessibility and clarity meant that users were unable to effectively understand and exercise their right to opt out of Google's data-processing for ads personalisation. This was in contravention of Google's transparency and information obligations (specifically, Articles 12 and 13 of the GDPR) under the GDPR.

Second, CNIL observed that Google lacked a valid legal basis for processing users' data for ads

personalisation on two grounds. One, because of the lack of accessibility and clarity in the information provided to users, as mentioned above, and two, because the consent collected was neither specific nor unambiguous. CNIL noted that when creating an account in the first instance, users were asked to give their consent in full for all processing operations purposes (e.g., ads personalisation, speech recognition, etc.) carried out by Google by checking the boxes for agreeing to Google's Terms of Service and Privacy Policy. As the GDPR provides that consent is "specific" only if it is given distinctly for each purpose, this constituted a contravention of the GDPR. CNIL further noted that while users could access the option for ads personalisation after creating an account, a further step had to be taken by the users in clicking on the button to show more options, which revealed a pre-ticked box for the displaying of personalised ads. This was in contravention of the GDPR, which requires consent to be given by clear affirmative action from the user, for example, by ticking a non-pre-ticked box.

Financial penalty

While CNIL's imposition of a €50 million penalty stands out as the first instance of a multimillion dollar fine under the GDPR's new percentage thresholds on an organisation's worldwide annual turnover, it is notable that the quantum fell far short of the maximum amount which could have been imposed under the GDPR based on Google's annual worldwide turnover. In justifying the quantum, CNIL referred to the severity of the contraventions regarding the essential principles of transparency, information and consent under the GDPR, as well as the fact that these contraventions were not one-off or time-limited infringements. In closing, CNIL also pointed out that in light of Google's impact on the French market and its economic operating model, Google has utmost responsibility to comply with the GDPR.

Germany's first GDPR fine issued against social media provider for breach of data security

On 21 November 2018, Germany's Staatsministerium Baden-Württemberg (***LfDI***) issued its first fine under the GDPR against social media provider Knuddels.de (***Knuddels***) for breaches of its data security obligations under Article 32 of the GDPR. Knuddels suffered a data breach incident in July 2018, which led to the subsequent publication of the personal data of approximately 330,000 users in September 2018. Once Knuddels became aware of the data breach incident, it immediately informed its users in accordance with Article 34 GDPR, and notified the LfDI of the same.

LfDI's findings

During the course of investigations, the LfDI found that Knuddels had stored the passwords of users in plain text and in an unencrypted format. In doing so, Knuddels had breached its obligations to ensure data security in the processing of personal data pursuant to Article 32(1)(a) of the GDPR.

Financial penalty

While the breach was severe, the LfDI only imposed a fine of €20,000, on account of Knuddels' exemplary conduct. Knuddels had reached out to its users in a comprehensive and transparent manner, notified the LfDI of the data breach incident and rendered full cooperation during the course of investigations. The LfDI also took into account Knuddels' implementation of comprehensive and far-reaching measures to improve its IT security infrastructure during the course of investigations, and subsequently based on recommendations made by the LfDI. In sum, the LfDI considered that the fine of €20,000 was proportionate and appropriate to address Knuddels' contravention of the GDPR.

Datatilsynet recommends Denmark's first GDPR fine against taxi company

On 18 March 2019, the Danish data protection agency, Datatilsynet, issued a decision recommending a fine of 1.2 million kroner (€160,754) against a Copenhagen-based taxi company, Taxa 4x35 (***Taxa***), for retaining customers' personal data relating to nearly 9 million trips for 5 years without any factual purpose, in contravention of the GDPR's data minimisation principle.

Datatilsynet's findings

Under the GDPR, personal data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which such data is being processed, except under certain circumstances. Contrary to Taxa's claim that customer information was anonymised after 2 years, Datatilsynet found that Taxa had only deleted customers' names from its database, but retained their phone numbers and other ride records for a further 3 years. Taxa's anonymisation attempts were insufficient as the information in Taxa's database could still be linked to individuals through phone numbers and other details despite the deletion of names.

Financial penalty

As Datatilsynet is unable to issue fines directly, its decision to recommend a fine has been referred to the Copenhagen police, to be pursued through the judicial system.

The United Kingdom's ICO serves data analytics firm with first-ever formal notice under GDPR, subsequently narrows scope of formal notice

On 6 July 2018, the UK's Information Commission Office (***ICO***) served an enforcement notice (the ***First Notice***) on Canadian data analytics firm AggregateIQ Data Services Ltd (***AIQ***), directing it to cease the processing of any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes. AIQ has been associated with the Facebook-Cambridge Analytica scandal as a provider of software and tools for the management of data intended for use in voter targeting and processing personal data on behalf of UK political organisations. On 24 October 2018, the ICO issued a second enforcement notice (the ***Second Notice***), which clarified and narrowed the scope of the personal data of individuals to be deleted.

The First Notice

AIQ has been associated with the Facebook-Cambridge Analytica scandal as a provider of software and tools for the management of data. Prior to the GDPR coming into force, AIQ was engaged by organisations such as Vote Leave, BeLeave, Veterans for Britain, and DUP Vote to Leave during the Brexit referendum campaign in 2016 to target advertisements at prospective voters. As part of AIQ's contract with these organisations, AIQ received the personal data of UK individuals, including names and email addresses, which it retained and stored on a code repository until the issuances of the Notices.

The ICO found AIQ to be non-compliant with Articles 5(1)(a) to (c) (principles relating to the processing of personal data), and Article 6 of the GDPR (lawfulness of processing). In addition, the ICO found that AIQ failed to comply with Article 14 of the GDPR as the processing of personal data was conducted in a way that the data subjects were not aware of, for purposes which were not expected, and without lawful basis. Under Article 14 of the GDPR, a data controller must provide certain information to data subjects about the processing of their data where such data was not obtained from the data subjects.

The Second Notice

Whilst the ICO did not change their assessment of AIQ's non-compliance with Articles 5(1)(a) to (c), 6, and 14 of the GDPR, it clarified and narrowed the scope of the directions imposed in the Second Notice. In contrast to the First Notice, AIQ was only required to erase any personal data of individuals in the UK, as determined by reference to the domain name of email addresses processed by AIQ and retained by AIQ on its servers, within 30 days of the Office of the Information and Privacy Commissioner of British Columbia (***OIPC***) notifying AIQ that either AIQ was no longer the subject of any investigation by the OIPC, or that the OIPC was content for AIQ to comply with the ICO's Second Notice. The references to the OIPC concerned an appeal by AIQ against the ICO's

First Notice, as AIQ claimed to have continued to hold the personal data of UK individuals as it was subject to a Canadian preservation order. This appeal was later withdrawn by AIQ following the ICO's issuance of its Second Notice.

Takeaways

The ICO's First Notice marked the first instance that a formal enforcement action was taken against an organisation since the GDPR came into force. Crucially, as AIQ is based outside of the ICO's jurisdiction, such an action was therefore based on the premise that AIQ is subject to the obligations under the GDPR pursuant to the provisions on the GDPR's territorial scope, specifically where the processing of personal data concerned UK or EU citizens obtained from UK political organisations constituted the monitoring of data subjects' behaviour taking place within the EU. Notwithstanding, it should be noted that the ICO did not explicitly set out its reasoning on how to determine whether or when to act against an organisation based out of jurisdiction for processing personal data of UK or EU citizens.

Austrian Data Protection Authority imposes first GDPR fine on company for breaches relating to CCTV operations

On 12 September 2018, the Austrian Data Protection Authority, Österreichische Datenschutzbehörde (***DSB***), issued its very first administrative fine against a sports betting café operator for infringements of the GDPR and the Austrian Data Protection Act. Since 22 March 2018 (or possibly earlier), the operator had installed two CCTV cameras in front of his café's entrance which, in addition to recording the front entrance of the café, covered a large part of the public street and parking lots as well. It was not disputed that the recorded images constitute personal data under the GDPR, and the storage and transmission of the same constituted processing under the GDPR.

In fining the operator €5,280.00, the DSB found that the operator's large-scale monitoring of public spaces was in contravention of the GDPR as there was no legal basis for the operator to process the personal data of pedestrians who did not reasonably expect to be recorded. The scale of the monitoring was not adequate for the purposes of the processing, and was not limited to the extent necessary for the operator. The DSB also found that the operator failed to comply with the applicable transparency obligations under the GDPR as it did not display the necessary signage to inform pedestrians about the video surveillance. The operator also failed to delete the recorded images within 72 hours, notwithstanding that there was no justification for storing the surveillance footage for an extended period.

The operator has lodged an appeal to the Federal Administrative Court against the DSB's decision. No further information is available as at the time of writing.

HONG KONG

Hong Kong's Privacy Commissioner for Personal Data commences investigation against Cathay Pacific in respect of data leak involving 9.4 million passengers

In late October 2018, Cathay Pacific Airways disclosed that it had suffered a data breach in March 2018. The personal data of more than 9.4 million passengers had been accessed without authorisation following suspicious activity in its network. The personal data accessed included the individuals' names, dates of birth, passport numbers, Identity Card numbers, credit card numbers, membership numbers, travel history etc. The airline faced much criticism for the seven-month delay in its announcement of the data breach even though they had confirmed the breach in early May.

In response, the Privacy Commissioner for Personal Data of Hong Kong announced on 5 November 2018 that following an initial compliance check, the Privacy Commissioner will be commencing a compliance investigation against Cathay Pacific, and its wholly owned subsidiary, Hong Kong Dragon Airlines Limited, pursuant to section 38(b) of the Personal Data (Privacy) Ordinance (***PDPO***) as there are reasonable grounds to believe that there may have been contravention of privacy laws.

According to the Privacy Commissioner, the compliance investigation will examine in detail, amongst others, the security measures taken by Cathay Pacific to safeguard its customers' personal data and the airline's data retention policy and practice. Under the PDPO, the Privacy Commissioner has the power to summon witnesses, enter premises, require them to furnish to him evidence, and carry out public hearings in the course of such an investigation.

Following the Cathay Pacific data breach, the PCPD announced in early 2019 that Hong Kong saw a record number of 129 user data breaches in 2018, representing a 22 per cent increase, and that the PCPD conducted 289 compliance checks and four compliance investigations in 2018. Under the PDPO, companies do not have any mandatory data breach reporting obligations, whether to the PCPD or to the affected individuals. The PCPD noted that the public had expressed concerns on mandatory reporting requirements and in light of the calls for Hong Kong to revamp its laws to make the reporting of potential data breaches mandatory, the PCPD said that it would discuss reforms with the government in the first half of 2019.

CANADA

New data breach notification requirements take efect in Canada

On 1 November 2018, organisations subject to the Personal Information Protection and Electronic Documents Act of Canada (***PIPEDA***) will be required to report to the Canadian Privacy Commissioner's Office (***OPC***) any breach of security safeguards and notify individuals affected by a breach of security safeguards where there is a "real risk of significant harm". Records of all breaches of security safeguards that affect the personal information under the organisations' control are to be kept for two years.

The amendment to the PIPEDA implementing the new data breach notification requirements is titled Breach of Security Safeguards Regulations (***Regulations***), and the OPC has published accompanying guidelines which provide a broad overview of such notification requirements. Some of the key features are as follows:

(a) Who has the obligation to report a breach?

Under the Regulations, the obligation to report a breach lies with the data controller, who is required to report any breach of security safeguards involving personal information if it is reasonable in the circumstances to believe that the breach of security safeguards creates a real risk of significant harm to an individual. This is the case even if the personal information has been transferred to a third party for processing.

(b) What is a "real risk of significant harm"?

The organisation must determine if the breach of security safeguards poses a "real risk of significant harm" to any individual whose information was involved in the breach by conducting a risk assessment. Factors that are relevant to determining whether such a breach creates a real risk of significant harm to the individual include the sensitivity of the personal information involved in the breach, and the probability that the personal information has been, is being, or will be, misused.

(c) How to report a breach?

Under the Regulations, the report must contain certain prescribed information such as a description of the circumstances and cause of the breach, the day on which or the period during which the breach occurred, a description of the personal information that is the subject of the breach, and the number of individuals affected.

The Regulations allow for data breach reports to be submitted with the best information available to the organisation at the time of reporting and for the organisation to submit any new information that the organisation becomes aware of after the report.

The OPC has also provided a non-mandatory breach report form which organisations can use to report such breaches.

(d) How and when to notify individuals / organisations?

As described above, the data controller has the obligation to notify, as soon as feasible, an individual of any breach of security safeguards involving the individual's personal information under the organisation's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

According to the OPC, the notification must be conspicuous and must be given directly to the individual, except in certain circumstances described in the Regulations where indirect notification is required. The notification must contain the information required under the Regulations.

In addition to the requirement to notify individuals, the Regulations also impose the requirement to notify government institutions or other organisations that the organisation believes can reduce the risk of harm that could result from the breach or mitigate the harm.

Businesses to follow more robust guidelines on meaningful consent for personal information from January 1 2019

On 1 January 2019, the Guidelines for Obtaining Meaningful Consent (***Consent Guidelines***), issued jointly by the Office of the Privacy Commissioner of Canada (***OPC***) and the Privacy Commissioners in Alberta and British Columbia, came into effect.

Under the Personal Information Protection and Electronic Documents Act (***PIPEDA***), the knowledge and consent of an individual are required for the collection, use, or disclosure of his personal information, and consent is only valid if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

The Consent Guidelines set out seven guiding principles for obtaining such consent from individuals, which are set out in summary below:

(a) Emphasise key elements

The Consent Guidelines provide that information about the collection, use and disclosure of individuals' personal information must be readily available in complete form, in a comprehensive and understandable manner.

To facilitate understanding and avoid information overload and allow individuals to quickly review key elements impacting their privacy decisions, certain key elements should generally be given additional emphasis:

(i) what personal information is being collected;

(ii) with which parties personal information is being shared;

(iii) for what purposes personal information is collected, used or disclosed; and

(iv) risk of harm and other consequences.

(b) Allow individuals to control the level of detail they get and when

Information should be provided to individuals in a layered format or any other means that supports user-control over the level of detail provided to them, and information should remain available to individuals as they engage with the organisation to allow them to re-consider whether to maintain or withdraw their consent.

(c) Provide individuals with clear options to say 'yes' or 'no'

Collections, uses or disclosures of personal information which are integral to the provision of the product or service, such that the organisation is required to fulfil its explicitly specified and legitimate purpose, are called conditions of service. Organisations should be prepared to explain why any given collection, use or disclosure is a condition of service.

Beyond that, individuals must be given a choice (unless an exception to the general consent requirement applies). Such choices must be explained clearly and made easily accessible.

(d) Be innovative and creative

Organisations should take advantage of digital capabilities in order to create consent processes that are specific to the context and appropriate to the user interface. Organisations are encouraged to use various communications strategies, such as "just-in-time" notices (i.e. bringing relevant privacy information to the forefront where it is conspicuous, quick to access, and intuitive), interactive tools and having the privacy policy customised for mobile interfaces.

(e) Consider the consumer's perspective

Consent processes must take into account the consumer's perspective to ensure that they are user-friendly and that the information provided is customised to the nature of the product or service offered and generally understandable from the point of view of the organisation's target audience.

(f) Make consent a dynamic and ongoing process

When information flows are complex, organisations should provide some interactive and dynamic way to anticipate and answer users'

questions. When significant changes are made to privacy practices, organisations must notify uses and obtain consent prior to such changes coming into effect.

Organisations should also consider sending periodic reminders to individuals about their privacy options, invite them to review their privacy settings, and audit their information management practices to ensure that it is compliant with their privacy policies.

(g) Be accountable: Stand ready to demonstrate compliance

Organisations should be in a position to demonstrate compliance, when asked. In particular, their consent processes must be sufficiently robust to obtain valid consent from individuals.

The OPC also highlighted that it is important for organisations to consider the appropriate form of consent to use for any collection, use or disclosure of personal information for which consent is required.

UNITED STATES

California Consumer Privacy Act

The California Consumer Privacy Act (***CCPA***) was signed into law on June 2018 and is set to take effect on 1 January 2020. The CCPA is California's new privacy law and is part of a series of privacy measures adopted by the state, including legislation such as the Online Privacy Protection Act and the Privacy Rights for California Minors in the Digital World Act. The introduction of the CCPA is also a sign of greater recognition of the importance of data privacy and consumer rights in California and elsewhere.

Definition of personal information

For the purposes of the CCPA, "personal information" is defined broadly as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household".

Personal information does not include publicly available information, i.e. information that is lawfully made available from federal, state, or local government records, for a purpose that is compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.

Applicability of the CCPA

The CCPA will apply to any entity that does business in the State of California and satisfies one or more of the following:

(i) annual gross revenue in excess of US$25 million (as may be adjusted pursuant to the CCPA);

(ii) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or

(iii) derives 50 percent or more of its annual revenues from selling consumers' personal information.

Rights granted under the CCPA

Broadly, the CCPA grants consumers four basic rights in relation to their personal information, which are set out in summary below:

(a) The right to know

Businesses are required to notify consumers of details such as what personal information they have collected, the sources from which the personal information is collected, the business or commercial purpose for collecting or selling the personal information, and to whom it is being disclosed or sold, through a general publicly-available privacy policy and more specifically upon request.

(b) The right to "opt out/in"

Businesses are required to grant consumers the right to "opt out" of having the business sell their personal information to third parties. The right shall be made easily accessible to consumers by providing a clear and conspicuous link on the business' Internet homepage titled "Do Not Sell My Personal Information".

For consumers who are under 16 years old, they have the right not to have their personal information sold without them, or their parents, opting-in. For those under the age of 13, the affirmative consent of a parent or guardian is required.

(c) The right to have businesses delete their personal information

Consumers may request that businesses delete their personal information, and businesses must inform consumers that they have this right. Businesses must comply with these requests and ensure the consumer's personal information is also deleted by any third-party service providers engaged by the business.

There are some exceptions to the requirement to delete upon request, specifically, if it is necessary for the business or service provider to maintain the consumer's personal information for purposes such as compliance with a legal obligation or completing the transaction for which the personal information was collected.

(d) The right to service equality

Businesses cannot discriminate against consumers who exercise their rights under the CCPA, although businesses can charge consumers a different price or rate or provide a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data. Furthermore, businesses may offer financial incentives for the collection, sale or deletion of personal information, subject to specific conditions and notice requirements.

In the meantime, new supplementary regulations, which must be implemented by July 2020, are being written. Some of the proposed measures include allowing consumers to commence proceedings against businesses that violate the CCPA for monetary damages, which could potentially render companies which amass user data, such as Facebook and Google, targets of mass class-action litigation from California consumers.

Nonetheless, there have been reports that advocacy groups are seeking more protections for consumers and business groups are working to rein it in, arguing that it will stifle competition and increase compliance costs for businesses. Thus, the ensuing implications of the CCPA remain to be seen.

The Drew & Napier Data Protection and Privacy Team

Drew & Napier's Data Protection & Privacy Team sits within our Telecommunications, Media and Technology (***TMT***) Practice Group.

Our work in data protection precedes the advent of the PDPA. Our expertise extends beyond general data protection law to sectoral frameworks, in particular, in the TMT, financial, and healthcare sectors.

We have been at the forefront of data protection laws in Singapore, given that we were involved with the Info-communications Media Development Authority (***IMDA***) / PDPC in setting up the implementing data protection laws in Singapore. We continue to represent the IMDA/PDPC in advisory, enforcement and policy work. We also regularly act for a wide range of clients on a variety of data protection matters, including the implementation of group-wide data protection compliance programmes, the localisation of global data privacy policies, data protection training programmes, advising companies on dealing with data breaches, conducting regulatory risk audits, and addressing ad hoc queries.

For more information on the Data Protection & Privacy 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* '*good knowledge of the telecommunications industry and consistently excellent service*' *(**Asia Pacific Legal 500**);* and is cited to be '*really exceptional - he has the pragmatism, he's plugged-in, and he gives solid, clear advice,' (**Chambers Asia 2017***: Standalone 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: TMT 2016*** and the ***Who's Who Legal: Competition 2016***. ***Asialaw Profiles*** notes: "*He's provided excellent client service and demonstrated depth of knowledge. Always responsive and available for ad hoc assistance."*

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

Janice Lee • Associate Director

Janice is an Associate Director in Drew & Napier's TMT Practice Group. She is frequently involved in advising clients 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. In addition to her broad data protection experience, Janice regularly assists in advising private entities and statutory boards on a range of contractual, corporate advisory, and regulatory matters. Janice is a Certified Information Privacy Professional for Europe (CIPP/E).

Tel: +65 6531 2323 • Fax: +65 6535 4864 • Email: **janice.lee@drewnapier.com**

DATA PROTECTION MID-YEAR UPDATE

ANNEX

Summary of the PDPC's enforcement decisions: April 2018 – June 2019

S/N	Date	Organisation(s)	Details
1.	19 Apr 2018	Aviva Ltd	A financial penalty of $30,000 was imposed on Aviva for failing to make reasonable security arrangements to prevent the unauthorised disclosure of personal data of policyholders. This is a second case within a period of 12 months. Decision can be found **here**.
2.	19 Apr 2018	Actxa Pte. Ltd.	A financial penalty of $6,000 was imposed on Actxa for breach of Section 13 (Consent Obligation) and Section 18 (Purpose Limitation Obligation) of the PDPA. Decision can be found **here**.
3.	30 Apr 2018	Singapore Management University Alumni Association	A financial penalty of $5,000 was imposed on SMU Alumni Association for failing to put in place reasonable security arrangements to protect the personal data of membership applicants from unauthorised disclosure. Decision can be found **here**.
4.	30 Apr 2018	Aventis School of Management Pte Ltd	A financial penalty of $12,500 was imposed on Aventis for using the personal data of individuals beyond the notified purposes, and for failure to give effect to the withdrawal of consent within a reasonable time. Decision can be found **here**.
5.	3 May 2018	AIG Asia Pacific Insurance Pte Ltd	A financial penalty of $9,000 was imposed on AIG for failing to make reasonable security arrangements to prevent the unauthorised disclosure of personal data. This case involved an incorrect facsimile number used by AIG on its renewal notices. Decision can be found **here**.
6.	3 May 2018	Habitat for Humanity Singapore Ltd	Directions were issued to Habitat for Humanity Singapore for breaches of the PDPA. The organisation did not make reasonable security arrangements to prevent unauthorised disclosure of its volunteers' personal data, failed to put in place data protection policies, and omitted to communicate data protection policies and practices to its staff. Decision can be found **here**.
7.	3 May 2018	NTUC Income Insurance Co-operative Ltd	A financial penalty of $10,000 was imposed on NTUC Income for lapses in its print process which resulted in an unauthorised disclosure of personal data of 212 individuals. Decision can be found **here**.
8.	14 May 2018	Information Technology Management Association (Singapore)	A warning was issued to Information Technology Management Association (Singapore) for failing to put in place reasonable security measures to prevent the accidental disclosure of the personal data of 28 individuals via email. Decision can be found **here**.
9.	14 May 2018	Watami Food Service Singapore Pte Ltd	A warning was issued to Watami Food Service Singapore for failing to make reasonable security arrangements to prevent unauthorised access of employees' personal data stored online. Decision can be found **here**.

S/N	Date	Organisation(s)	Details
10.	24 May 2018	Spring College International Pte Ltd	Spring College International failed to notify and obtain consent from the parents of young students before disclosing online the students' personal data for marketing purposes. Directions were issued to Spring College International. Decision can be found **here**.
11.	11 Jun 2018	Flight Raja Travels Singapore Pte Ltd	Directions were issued to Flight Raja Travels for failing to make reasonable security arrangements to prevent unauthorised disclosure of individuals' personal data on its online travel booking system. Decision can be found **here**.
12.	22 Jun 2018	Singapore Taekwondo Federation	A financial penalty of $30,000 was imposed on Singapore Taekwondo Federation for failing to make reasonable security arrangements to prevent the unauthorised disclosure of minors' NRIC numbers on its website. Directions were also issued to the organisation to appoint a data protection officer and to put in place data protection policy. Decision can be found **here**.
13.	21 Aug 2018	1) Singapore Cricket Association 2) Massive Infinity Pte Ltd	Directions were issued to Singapore Cricket Association for failing to make reasonable security arrangements to prevent unauthorised disclosure of individuals' personal data on its website, and for failing to put in place data protection policies. Decision can be found **here**.
14.	21 Aug 2018	Dimsum Property Pte Ltd	A warning was issued to Dimsum Property for failing to make reasonable security arrangements to prevent unauthorised access of individuals' personal data stored in web directories. Decision can be found **here**.
15.	11 Sep 2018	Jade E-Services Singapore Pte Ltd	A warning was issued to Jade E-Services for failing to make reasonable security arrangements to prevent webpages containing customers' personal data from being cached and displayed to other customers. Decision can be found **here**.
16.	25 Sep 2018	Galaxy Credit & Investments Pte Ltd	A warning was issued to Galaxy Credit and Investments for failing to make reasonable security arrangements to protect the personal data of its borrowers, and using personal data not for a purpose that a reasonable person would consider appropriate in the circumstances. Decision can be found **here**.
17.	4 Oct 2018	GrabCar Pte Ltd	A financial penalty of $6,000 was imposed on Grabcar for failing to make reasonable security arrangements to prevent the unauthorised disclosure of GrabHitch drivers' personal data. Decision can be found **here**.
18.	4 Oct 2018	Club the Chambers	A financial penalty of $7,000 was imposed on Club the Chambers for failing to make reasonable security arrangements to prevent the unauthorised disclosure of the identity documents of 11 individuals in a LAN gaming centre. Decision can be found **here**.

S/N	Date	Organisation(s)	Details
19.	28 Nov 2018	Big Bubble Centre	A warning was issued to Big Bubble Centre for disclosing personal data online without the consent of the individuals concerned. Decision can be found **here**.
20.	13 Dec 2019	WTS Automotive Services Pte Ltd	A financial penalty of $20,000 was imposed on WTS Automotive Services for failing to make reasonable security arrangements to prevent the unauthorised disclosure of its customers' personal data. Decision can be found **here**.
21.	13 Dec 2019	SLF Green Maid Agency	Directions were issued to SLF Green Maid Agency for failing to make reasonable security arrangements to prevent the unauthorised disclosure of individuals' personal data. Decision can be found **here**.
22.	13 Dec 2019	Institute of Singapore Chartered Accountants	A financial penalty of $6,000 was imposed on Institute of Singapore Chartered Accountants for failing to make reasonable security arrangements to prevent the unauthorised disclosure of the personal data of its members. Decision can be found **here**.
23.	13 Dec 2019	Funding Societies Pte Ltd	A financial penalty of $30,000 was imposed on Funding Societies for failing to make reasonable security arrangements to prevent the unauthorised disclosure of the personal data of its members. Decision can be found **here**.
24.	3 Jan 2019	1) AIG Asia Pacific Insurance Pte Ltd 2) Toppan Forms (S) Pte Ltd	A financial penalty of $5,000 was imposed on Toppan Forms for failing to put in place reasonable security arrangements to protect the personal data from unauthorised disclosure. Decision can be found **here**.
25.	22 Jan 2019	COURTS (Singapore) Pte Ltd	A financial penalty of $15,000 was imposed on COURTS for failing to put in place reasonable security arrangements to protect the personal data of its customers from unauthorised disclosure on its online portal. Decision can be found **here**.
26.	23 Apr 2019	Tutor City	A warning was issued to Tutor City for failing to make reasonable security arrangements to prevent the unauthorised access of individuals' personal data stored in web directories. Decision can be found **here**.
27.	23 Apr 2019	PAP Community Foundation	A warning was issued to PAP Community Foundation for failing to make reasonable security arrangements to prevent the unauthorised disclosure of personal data. Decision can be found **here**.
28.	3 Jun 2019	Matthew Chiong Partnership	A financial penalty of $8,000 was imposed and directions were issued to Matthew Chiong Partnership for breaches of the PDPA. The organisation did not make reasonable security arrangements to prevent the unauthorised disclosure of its clients' personal data and failed to put in place data protection policies to comply with the provisions of the PDPA. Decision can be found **here**.

S/N	Date	Organisation(s)	Details
29.	3 Jun 2019	German European School Singapore	German European School Singapore was found not to be in breach of the PDPA in relation to allegations that there was no consent given for the collection of its student's hair sample for the purpose of drug testing. Decision can be found **here**.
30.	6 Jun 2019	H3 Leasing	A warning was issued to H3 Leasing for disclosing personal data online without the consent of the individual concerned. Decision can be found **here**.
31.	6 Jun 2019	Option Gift Pte Ltd	A financial penalty of $4,000 was imposed on Option Gift for failure to conduct sufficient testing before deployment of a programme script which resulted in an unauthorised disclosure of up to 426 individuals' personal data. Decision can be found **here**.
32.	6 Jun 2019	Ncode Consultant Pte Ltd	A financial penalty of $30,000 was imposed on Ncode Consultant for failing to put in place reasonable security arrangements to prevent unauthorised access and modification to an IT system provided to a school. The failure resulted in unauthorised access and modification of students' personal data. Decision can be found **here**.
33.	6 Jun 2019	1) StarHub Mobile Pte Ltd 2) M1 Limited 3) Singtel Mobile Singapore Pte. Ltd.	Telcos were not found in breach of the PDPA for charging subscribers for the provision of Caller Number Non-Display value added services. Decision can be found **here**.
34.	11 Jun 2019	Skinny's Lounge	A warning was issued to Skinny's Lounge for failing to ensure that consent was obtained from its patrons to re-play recorded CCTV footage on a screen in its public lounge. Skinny's Lounge also failed to provide due notification to its patrons on the full purposes of the CCTV footage recorded at its premises. Decision can be found **here**.
35.	11 Jun 2019	Grabcar Pte. Ltd.	Directions were issued to GrabCar for failing to put in place reasonable security arrangements for GrabHitch drivers to protect the personal data of passengers that used GrabHitch services. Personal data of some GrabHitch passengers were disclosed by GrabHitch drivers without consent on social media. Decision can be found **here**.
36.	11 Jun 2019	Grabcar Pte. Ltd.	A financial penalty of $16,000 was imposed on GrabCar for failing to put in place reasonable security arrangements to protect the personal data of its customers from unauthorised disclosure. Personalised marketing emails sent to 120,747 customers contained and thereby disclosed the mismatched personal data of other customers. Decision can be found **here**.

S/N	Date	Organisation(s)	Details
37.	13 Jun 2019	DS Human Resource Pte. Ltd.	A financial penalty of $33,000 was imposed on DS Human Resource for breaches of the PDPA. The organisation failed to put in place data protection policies, which resulted in the unauthorised access and deletion of its database containing personal data of approximately 2,100 job applicants. It also did not make reasonable security arrangements to prevent the unauthorised disclosure of the personal data of the individuals. Decision can be found **here**.
38.	20 Jun 2019	InfoCorp Technologies Pte. Ltd.	A financial penalty of $6,000 was imposed on InfoCorp for failing to put in place reasonable security arrangements to protect the personal data of individuals. Personal data of 21 individuals participating in a registration exercise via InfoCorp's website were disclosed to 15 other participants in the course of the registration exercise. Decision can be accessed **here**.
39.	20 Jun 2019	Cigna Europe Insurance Company S.A.-N.V.	Cigna Europe Insurance Company S.A.-N.V. was found not to be in breach of the PDPA in relation to allegation that it had failed to make reasonable security arrangements to prevent the unauthorised disclosure of the personal data of its policy members. Decision can be accessed **here**.
40.	20 Jun 2019	Xbot Pte. Ltd.	A warning was issued to Xbot for failing to put in place data protection policies to comply with the provisions of the PDPA. Decision can be accessed **here**.
41.	20 Jun 2019	AIA Singapore Private Limited	A financial penalty of $10,000 was imposed on AIA for failure to take reasonable security arrangements in its letter generation process, resulting in a total of 245 letters meant for various customers being erroneously sent to 2 customers. Decision can be accessed **here**.