COMPUTER LAW & SECURITY REVIEW 34 (2018) 1166–1174

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Asia pacific news

Gabriela Kennedy

Mayer Brown, 16th - 19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong

ARTICLE INFO

Article history:

Keywords:
Asia-pacific
IT/information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country-by-country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

Gabriela Kennedy *(Partner), Mayer Brown (gabriela.kennedy@mayerbrown.com);*
Karen H.F. Lee *(Senior Associate), Mayer Brown (karen.hf.lee@mayerbrown.com).*

1.1. *Open wide! The HKMA's open API framework*

On 18 July 2018, the Hong Kong Monetary Authority ("**HKMA**") issued its Open Application Programming Interface Framework for the Banking Sector ("**Open API Framework**"), following a consultation process that ended on 15 March 2018. The Open API Framework is aimed at the retail banking sector.

1.1.1. *Background*

Application programming interfaces ("**API**") are software protocols that enable different software systems or applications to communicate and interact with each other. The Open API Framework is not mandatory, and is intended to provide a high level guidance to retail banks to help streamline the process, whilst still providing flexibility.

By encouraging banks to make their system APIs open to third parties, subject to adequate security controls ("**Open APIs**"), third party platforms can more efficiently access the bank's data systems. The intent of the Open API Framework is to encourage the development of innovative technology solutions and the amalgamation of information by third party service providers ("**TSPs**") for the benefit of consumers (e.g. enabling consumers to compare competitive products offered by different banks, to view their various bank account information on one platform, to carry out payment transactions, etc).

The Open API Framework is one of the seven HKMA initiatives announced in September 2017, as part of its "New Era of Smart Banking". The HKMA has already opened the door for virtual banks and amended the licensing regime for stored value facilities, all in an attempt to stay competitive and not to be left behind. Other jurisdictions are already ahead of the game when it comes to Open APIs, including Singapore and the UK, the latter of which made Open APIs mandatory for the largest UK retail banks since January 2018.

1.1.2. *Phased approach*

The HKMA has proposed a four phase timeline for the implementation of the Open API Framework. The level of perceived risk increases with each phase, as does the level of protection required by the banks for the Open API implementation:

E-mail address: gabriela.kennedy@mayerbrown.com

https://doi.org/10.1016/j.clsr.2018.08.003

(a) Phase 1 – "Product and service information" – this is for accessing "read only" bank information concerning details of their products and services. Prior to granting access to a TSP to the bank's Open API, the bank will need to implement safeguards concerning the authentication of the bank sites, the integrity of the data and the authentication of the TSP.
(b) Phase 2 – "Subscription and new applications for product/review" – this is in relation to a customer acquisition process, which will allow customers to make submissions or applications for bank products online. The bank will need to implement safeguards concerning the authentication of the bank sites, the integrity and confidentiality of the data and the authentication of the TSP.
(c) Phase 3 – "Account information" – this is for enabling the retrieval and amendment of account information of customers for standalone or aggregated viewing. As this poses a higher level of risk to customers, the bank will need to implement safeguards concerning the authentication of the bank sites, the integrity of the data, the authentication of the TSP and obtain the customer's authorisation.
(d) Phase 4 – "Transactions" – this relates to enabling the execution of banking transactions or payment instructions of a customer. The same level of protection as Phase 3 needs to be implemented by the bank.

Phase 1 is to be implemented within 6 months of the issuance of the Open API Framework, and Phase 2 is to be implemented with 12–15 months. The timeframe for Phases 3 and 4 shall be determined by the HKMA in the next 12 months.

1.1.3. *TSPs governance*

TSPs that access the Open APIs of banks will not need to be licensed or approved by the HKMA. As the banks will remain fully liable and responsible for any misuse of their customer data, the burden is on the bank to vet each TSP and ensure robust measures and contracts are in place to protect the data.

Phase 1

Under the Open API Framework, due to the limited risks posed by Phase 1 (i.e. no access to customer or proprietary data), the banks are only required to establish a simple TSP registration process and to require TSPs to agree to terms and conditions that incorporate some key terms. These include a requirement of the TSPs not to misrepresent the bank, to inform customers that the bank is not collecting any personal data via the TSPs platform, the TSPs must comply with applicable laws, including the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"), and TSPs should inform customers of the risks and liabilities associated with the TSPs services.

Phase 2 to 4

More stringent requirements are imposed on the banks in Phases 2 to 4. The HKMA expects the banks to work together (e.g. via the Hong Kong Association of Banks) to establish a common baseline for TSP governance. It has been suggested that the banks centralise the process, e.g. appointing a central assessor. This will help make the vetting of TSPs more efficient and streamlined amongst the banks, as TSPs can simply prepare standards documents and evidence required in order to gain approval and access to the Open APIs. The common baseline must require a due diligence of the TSPs business and risk management (e.g. financial stability, reputation, business and technical expertise, customer and data protection measures, cybersecurity controls, etc). In addition, the banks should establish an ongoing monitoring system to ensure that the TSPs continue to comply with the common baseline.

The banks will need to enter into agreements with the TSPs. In light of the potential risks and liabilities involved, it is vital for the banks to clearly set out what the obligations of the TSP are and their minimum responsibilities (i.e. in relation to consumer protection, disclosure, transparency, safeguarding measures, security control, restrictions on use). The banks should also incorporate strong liability and indemnity provisions, so that they can hold TSPs responsible for any losses suffered by the bank as a result of the TSPs actions or their platforms (e.g. any fines, customer claims, etc, imposed on the bank). Lastly, since the regulatory environment is still developing in this area, the TSP contract should be drafted in such a way as to allow some flexibility, e.g. change to be made in light of any regulatory amendments.

Each bank is expected to publish a list of all TSPs that have been granted access to their Open API, with information about the relevant services, mobile application, etc, offered by the TSPs.

1.1.4. *Open API implementation*

Rather than stipulating a standardised set of Open APIs or mandating security measures, the Open API Framework provides a recommended high-level list of Open API functions and recommended architecture and security standards based on existing international practice.

The banks will need to provide a roadmap to the HKMA of its Open API implementation, and to provide an explanation on how it is compliant with the recommended Open API functions, and the reasons for any divergence.

The HKMA also recommends the setting up of a single repository for all Open APIs.

1.1.5. *Conclusion*

The Open API Framework is a welcome step that will help keep Hong Kong competitive and will boost the fintech ecosystem in Hong Kong. However, the banks will need to ensure that any access to their data through the use of Open APIs is consistent with the PDPO, and robust contracts are in place to protect any misuse by TSPs.

With a lot of flexibility left to the banks, now is the time for them to come together to streamline the approach to ensure efficiency – a big job that may fall on the shoulders of the Hong Kong Association of Banks.

2. Japan

Kiyoko Nakaoka *(Attorney-at-Law, Patent Attorney), Kubota (nakaoka@kubota-law.com).*

2.1. *Revised Japanese copyright act*

2.1.1. *Introduction*

A revised Copyright Act ("**Revised Act**") was adopted on 18 May 2018. The majority of the Revised Act will come into effect on 1 January 2019.

The Revised Act aims to (i) expand the free use of copyrighted works, without the need to obtain the copyright owner's permission in response to the progress of digitisation and the Internet; and (ii) promote opportunities to use copyrighted works by persons with disabilities who have difficulty reading books. Unlike the concept of fair use in the United States, the Japanese Copyright Act lists out specific situations where a third party may use the copyrighted work without obtaining the copyright owner's permission. The Revised Act expands the scope of such situations.

The Revised Act mainly regulates the following four aspects:

(i) Improvement of flexible use of copyrighted works to correspond with the progress of digitisation and the Internet;
(ii) Improvement of use of copyrighted works corresponding to informatisation of education;
(iii) Improvement of free use of copyrighted works to enhance information access for persons with disabilities; and
(iv) Improvement of free use of copyrighted works on the promotion of utilisation of archives, etc.

2.1.2. *Improvement of flexible use of copyrighted works to correspond with the progress of digitisation and the internet*

In order to keep pace with the progress of digitisation and the Internet, under the Revised Act, a copyright owner's permission will not be required in the following three situations:

(a) Usage not intended for the enjoyment of ideas or emotions expressed in the copyrighted works
Under the Revised Act, where the copyrighted work is provided (i) for use in testing for the development of technology, (ii) for use in information analysis, (iii) for use in the process of information processing by electronic computers without recognition by human perception, and (iv) for use in other cases where it is not intended for the enjoyment of ideas or emotions expressed in the copyrighted work, the copyright owner's permission is not required. For example, recording copyrighted works in a database as learning data for the development of artificial intelligence (AI) can be done without obtaining the copyright owner's permission.
(b) Accompanying usage of copyrighted works on electronic computers
Under the Revised Act, in relation to the use of the copyrighted work on an electronic computer with a view to enhancing the efficiency of the computer operation, the copyright owner's permission is not required. For example, the act of creating a cache in order to speed up information communication processing through the Internet, or temporarily replacing a music file in the memory with another recording medium can be done without obtaining the copyright owner's permission.
(c) Information processing by electronic computers and minor utilisation accompanying the provision of results
Under the Revised Act, a person who searches for information or analyses information using an electronic computer and provides the results, can make minor use of the copyrighted work. For example, when searching for a specific key word in a book, providing a part of a sentence that includes the keyword in the book together with information concerning the bibliographic information can be done without obtaining the copyright owner's permission. Under the Revised Act, it is possible to add free use by the government's ordinance if a new need arises in a similar situation in the future.

2.1.3. *Improvement of use of copyrighted works corresponding to informatisation of education*

Under the current Copyright Act, the copyright owner's permission is not required to copy copyrighted works for use in face-to-face classes and to transmit the copyrighted works for remote teaching (but only for materials used in face-to-face classes which are simultaneously transmitted to remote classes). However, the copyright owner's permission is required for (i) sending copyrighted works for revision courses of the face-to-face classes by e-mail; and (ii) sending copyrighted works for on-demand, remote classes and so on. Under the Revised Act, the above acts (i) and (ii) can be done without obtaining prior permission of the copyright owner, if a school pays compensation fees to a certain entity that is designated by the Minister of Cultural Affairs.

2.1.4. *Improvement of free use of copyrighted works to enhance information access for persons with disabilities*

Under the current Copyright Act, the copyright owner's permission is not required to transliterate books for the visually impaired. The Revised Act expands the range of beneficiaries to people who have difficulty reading books due to obstacles, such as a person who cannot hold books due to physical disability.

2.1.5. *Improvement of the free use of copyrighted works on the promotion of utilisation of Archives, etc*

Under the Revised Act, the copyright owner's permission is not required for providing a thumbnail image of any art pieces or photos to electronic devices, such as tablet terminals, when a museum exhibits copyrighted works and the thumbnail images are used in order to give comments and introduce the copyrighted works.

Furthermore, the National Diet Library can submit an out-of-print book to a foreign library without obtaining the copyright owner's permission.

3. New Zealand

Karen Ngan *(Partner), Simpson Grierson (karen.ngan @simpsongrierson.com);*

Nick Jens *(Solicitor), Simpson Grierson (nick.jens @simpsongrierson.com).*

3.1. *Privacy bill – update*

The Privacy Bill ("**Bill**") was introduced to the House by the Minister of Justice on 20 March 2018. The Bill intends to replace the 25-year-old Privacy Act and to bring New Zealand's privacy laws in line with recent international developments and reforms. The closing date for public submissions has now expired and the submissions are now being considered by the Select Committee.

Submissions have been made by the Privacy Commissioner and a range of private and public sector agencies.

3.1.1. *Privacy commissioner's submission*

The New Zealand Privacy Commissioner has been advocating reform of New Zealand privacy laws for some time so is supportive of the Bill but his submission makes it clear he is of the view that the Bill needs to go further. A key theme in the Privacy Commissioner's submission is that the proposed reforms need to go further than they do to ensure that the new Privacy Act is "fit for purpose in [a] dynamic data-rich world" and to meet the standards set by recent reforms in other jurisdictions. Mention is made specifically to the standard set by the EU's recently introduced EU General Data Protection Regulations. The Privacy Commissioner's suggested amendments to the Bill include:

(i) civil penalties of up to NZ $1 million for breaches of the Privacy Act;
(ii) the right to information portability;
(iii) the right to erasure;
(iv) algorithmic transparency and automatic decision making; and
(v) clarifying situations in whether the Privacy Act will apply to overseas agencies.

3.1.2. *Other submissions*

Other submissions that have been made cover a range of matters but two of the issues that have been raised in a large number of the submissions are:

(i) the mandatory data breach notification regime; and
(ii) New Zealand's EU adequacy status.

Mandatory data breach notification

The mandatory data breach notification regime has generally been welcomed by submitters, however a common theme has been that the regime should be aligned more closely to the regimes in Australia and the EU. Proposals include:

(i) Increasing the threshold of a "notifiable breach" to "serious risk of harm". Under the current draft of the Bill, a notifiable data breach would include any breach that may cause harm to an individual. The concern is that the low threshold may lead to an over-reporting of inconsequential data breaches and an increase in compliance costs.
(ii) Clarifying the timing of when notification has to be given. As the Bill is currently drafted, an agency must notify "as soon as reasonably possible". However, there have been calls for notification to occur after an investigation into the incident has been conducted. This would reduce the risk of subsequent breaches committed while an agency is investigating the source of vulnerability.

EU adequacy status

There is a concern that the Bill does not go far enough to ensure New Zealand will retain its EU adequacy status.

There are submissions proposing that the Bill should adopt:

(i) relevant GDPR provisions; and
(ii) a mandatory review of the Privacy Act within 2 years of enactment, to ensure that New Zealand retains its EU adequacy status.

3.1.3. *What next?*

The Select Committee is due to release its report on 11 October 2018. This report will prepare any amendments to the Bill that the Select Committee considers appropriate having regard to the submissions received. The Bill will need to pass a second and third reading in Parliament and receive Royal Assent before it is enacted into law.

3.2. Kim Dotcom v crown law office *[2018] NZHRRT*

The Human Rights Review Tribunal ("**HRRT**") recently delivered a judgment regarding access requests under the Privacy Act 1993 ("**Privacy Act**"). With it, the HRRT has provided its interpretation on when an agency can transfer an access request and when an agency can refuse an access request.

3.2.1. *Background*

Under the Privacy Act 1993, an individual has the right to request his or her personal information from an agency. Mr Dotcom, who is currently going through extradition proceedings in New Zealand (relating to copyright infringement in the United States), made numerous access requests to government departments regarding his personal information that such government departments held. The requests were to obtain information to assist with his extradition proceedings.

The majority of the access requests were transferred to the Attorney General ("**AG**"). Subsequently, the AG made the decision to decline Mr Dotcom's access requests under s 29(1)(j) of the Privacy Act, on the grounds that the requests were frivolous or vexatious, or the information requested was trivial.

Mr Dotcom challenged the AG's decision on two grounds:

(i) whether the transfer of the access requests to the AG was permitted under the Privacy Act; and
(ii) whether there was no proper basis to decline the decision under s 29(1)(j).

3.2.2. *Transfer of request*

The HRRT first considered whether the access requests were permitted to be transferred to the AG. Under the Privacy Act,

an agency receiving a request can transfer it to another agency where the information is more closely connected with the functions or activities of that other agency (s 39(b)(ii)).

The HRRT held that the transfers to the AG were not made in accordance with the Privacy Act. In this case the information requested was not more closely connected with the functions or activities of the AG than the functions or activities of the agencies transferring the requests.

3.2.3. *Grounds for declining request*

The HRRT also considered whether, if the transfer of the request had been lawful, there was a proper basis to decline the access requests under s 29(1)(j). The HRRT noted that the threshold for declining a request under s 29(1)(j) requires:

(i) an objective assessment that the request is clearly frivolous, vexatious or trivial; and
(ii) a presumption that the individual making the request is unaware of the nature and content of the personal information held.

The HRRT found that the AG had incorrectly declined the requests on the grounds that the access requests were frivolous, vexatious or trivial. The HRRT was of the view that the AG had made an unreasonable assumption that Mr Dotcom was using the access request to obtain an adjournment of his extradition proceedings – while Mr Dotcom's access requests was viewed by the HRRT as genuine.

As the HRRT found that the transfers to the AG was not permitted, and that the AG had incorrectly denied Mr Dotcom's access requests on the grounds under s 29(1)(j), there was an interference with the privacy of Mr Dotcom. The HRRT awarded Mr Dotcom:

(i) NZ $30,000 for damages; and
(ii) NZ $60,000 for loss of dignity and injury to feelings.

4. Singapore

Lam Chung Nian *(Partner), WongPartnership LLP (chungnian.lam@wongpartnership.com);*
Quek Zhao Feng *(Practice Trainee), WongPartnership LLP (zhaofeng.quek@wongpartnership.com)*

4.1. *Infocomm media development authority announces new artificial intelligence governance and ethics initiatives*

The Infocomm Media Development Authority ("**IMDA**") on 5 June 2018 announced the introduction of three structured and interlinked initiatives aimed at increasing awareness of the benefits and challenges presented by Artificial Intelligence ("**AI**") in Singapore's economy. The relevant initiatives are:

(i) the creation of an advisory council on the ethical use of AI and data;
(ii) the creation of an AI and data governance framework discussion paper; and
(iii) the setting up of a research program on the governance of AI and data use.

These three initiatives relate to IMDA's broader aims to inform the Singapore Government's ongoing plans to support Singapore as a hub for AI development and innovation as well as to assist Singapore in responding to global technological developments.

4.1.1. *Advisory council on the ethical use of AI and data*

An advisory council ("**Advisory Council**") comprised of private sector thought leaders in AI and "Big Data", and consumer interest representatives, will be appointed by the Minister for Communications and Information to advise and work with the IMDA in respect of the responsible development and deployment of AI. The Advisory Council will be tasked (among other things) with assisting IMDA to:

(i) engage with relevant stakeholders (such as ethics boards of commercial enterprises) on various issues arising from the use of AI ad data in the private sector, as well as consumer advocates to obtain information on consumer expectations and acceptance of said use;
(ii) engage the private capital community to increase awareness of the need to incorporate ethics considerations in their investment decisions into businesses that are involved in adopting or developing AI technology; and
(iii) establish a panel of legal and technical experts, as well as a panel of international experts, to assist the Advisory Council.

The Advisory Council also has the role of developing ethical standards and reference governance frameworks for the Government, and will, inter alia, publish advisory guidelines, practical guidance, and codes of practice for voluntary adoption by the industry.

4.1.2. *AI and data governance framework discussion paper*

The Personal Data Protection Commission ("**PDPC**"), Singapore's data privacy watchdog, has also in collaboration with key government and industry stakeholders released a discussion paper on AI and personal data ("**Discussion Paper**") on 5 June 2018[1]. The Discussion Paper serves as a baseline document to support collaborative discussions on the responsible development and adoption of AI, and also facilitates the adoption of industry-wide common definitions and common frames for dialogues related to AI.

The Discussion Paper recommends two key principles:

(i) that decisions made by or with the assistance of AI should be *explainable, transparent and fair to consumers* (for the purpose of fostering trust and confidence among individuals affected by said decisions); and

[1] PDPC: *Discussion Paper on Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI (5 June 2018)* (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD—050618.pdf).

(ii) AI systems, robots and decisions should be human-centric (referring to the use of AI-focused design approaches that place the individual customer or consumer at its heart).

The Discussion Paper also proposes a four-stage governance framework for AI illustrating how these principles may be put into practice by stakeholders, outlining steps such as:

(i) identifying the objectives of an AI governance framework;
(ii) selecting appropriate organisational governance measures;
(iii) putting in place consumer relationship management processes; and
(iv) building a decision-making and risk assessment framework.

The PDPC has invited Singaporean organisations in general to use the Discussion Paper for their own internal purposes, and has encouraged them to adapt the proposed four-stage governance framework for their individual sectors, or the development of voluntary codes of practice.

4.1.3. *Research programme on the governance of AI and data use*

Last but not least, the IMDA and the Singapore National Research Foundation have proposed the creation of a five-year research programme on the governance of AI and data use ("**Research Programme**") at the Singapore Management University. The scope of the Research Programme encompasses the conduct of scholarly research on policy, legal, regulatory, governance, ethics, and other issues relating to AI and data use. The aims of the Research Program include:

(i) the organisation of engagement forums to engage stakeholders to generate and share knowledge concerning AI and data use, and provide clarity on policy and regulatory issues and their impacts; and
(ii) the publication and presentation of research papers to demonstrate Singapore's thought leadership in the international AI and data research communities.

The Research Programme will have the general role of: (i) supporting the Advisory Council; and (ii) informing the Government and industry discussion on AI challenges through its research and conferences.

4.1.4. *Comments*

As the first major step that the Singapore Government (through its agencies) has taken in addressing the growing pervasiveness and potential of AI technology, the IMDA's initiatives provide a useful starting point in lending to Singaporeans' general understanding of this complex topic. The industry-agnostic nature of the Discussion Paper, in concert with the engagement of various industry stakeholders through the Advisory Council and Research Programme also suggest a general anticipation on the part of the Singapore Government of AI technology being taken up across many industries.

In particular, the PDPC's Discussion Paper provides insight into the Government's regulatory approach to AI – a technology-neutral and light-touch regime, which at the same time provides regulatory clarity. The Discussion Paper also highlights that in addition to the Personal Data Protection Act, sector-specific codes of practice could be used to provide assurance to consumers about the use of AI. Industry players may wish to note these points to anticipate the nature of upcoming AI regulation.

4.2. *Singapore privacy watchdog takes action against local martial arts federation for breach of local data protection laws*

In a decision released on 22 June 2018, the Personal Data Protection Commission ("**PDPC**") has ordered the Singapore Taekwondo Federation ("**Organisation**") to, inter alia, pay a financial penalty of SG $30,000 and develop and implement remedial policies and practices for its failure to comply with the following obligations under the Singapore Personal Data Protection Act (No.26 of 2012) ("**PDPA**"):

(i) the obligation under Section 11 of the PDPA to designate one or more persons with the responsibility for ensuring that the Organisation complies with the PDPA ("**Section 11 Obligation**");
(ii) the obligation under Section 12 to develop and implement policies and practices necessary for the Organisation to meet its obligations under the PDPA ("**Section 12 Obligation**"); and
(iii) the obligation under Section 24 to implement reasonable security arrangements to protect Personal Data[2] in the Organisation's possession or under the Organisation's control to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks ("**Section 24 Obligation**").

(collectively, the "**Relevant PDPA Obligations**").

4.2.1. *Background facts*

The Organisation is a society responsible for promoting, supporting and developing taekwondo-related programmes and activities in Singapore. The Organisation had since 2015, been making PDF documents containing the names and schools of student participants of the Singapore Annual Inter-School Taekwondo Championships ("**Championships**") available on the Organisation's website, which were accessible to the general public.

On 30 May 2017, a complaint was lodged by a member of the public ("**Complainant**") with the PDPC alleging an unauthorized disclosure by the Organisation of the National Registration Identity Card ("**NRIC**") numbers of 782 students who were participants of the 2017 Championships. The disclosure occurred when the Complainant, after downloading a PDF doc-

[2] Under Section 2 of the PDPA, "Personal Data" is defined as "data, whether true or not, about an individual who can be identified from that data and other information to which the organisation has or is likely to have access".

ument containing the student names from the Organisation's website, copied and pasted the information therein onto another document ("**Disclosure Method**"). The NRIC numbers of the students (which were minimised on the PDF document) subsequently became visible on the other document as a result of the Disclosure Method.

The PDPC subsequently notified the Organisation and conducted an investigation, which revealed among other things that:

(i) the Organisation's data handling processes involved the following steps:
  (a) the Organisation first received an encrypted Microsoft Excel spreadsheet containing Personal Data (including the NRIC numbers) of students intending to participate in the Championships;
  (b) the Organisation's head of the Tournament Department ("**Tournament Head**") would proceed to rearrange the students' Personal Data into programme lists and bout sheets using Microsoft Excel; and
  (c) the Tournament Head would then minimise the NRIC numbers before converting the Excel spreadsheets into PDF documents for publication on the Organisation's website;
(ii) the Organisation was not aware that the columns of NRIC numbers had been minimised on the PDF documents and could be revealed by way of the Disclosure Method; and
(iii) the Organisation was not aware of the PDPA and the obligations imposed by the PDPA on organisations[3] such as itself, and accordingly, did not appoint any individuals responsible for ensuring the Organisation comply with the PDPA, or put into place any policies or practices necessary for it to meet the obligations under the PDPA.

4.2.2. *Decision of the PDPC*

The Deputy Commissioner for the Commissioner for Personal Data Protection ("**Deputy Commissioner**") took the view that the issues for determination in this case concerned whether the Organisation complied with the Relevant PDPA Obligations.

In finding that the Organisation failed to comply with all three of the Relevant PDPA Obligations, the Deputy Commissioner gave his reasons as follows:

The Organisation's Section 11 and Section 12 Obligations

The Deputy Commissioner held that the Organisation breached its Section 11 Obligation and Section 12 Obligation for the following reasons:

(i) the Organisation's lack of awareness of its data protection obligations under the PDPA was not a legitimate defence to a breach of the PDPA[4];
(ii) the Organisation confirmed that it had failed to designate an individual to be responsible for ensuring the Organisation's compliance under the PDPA, as was required under Section 11(3) of the PDPA; and
(iii) the Organisation also confirmed that it had not put in place any data protection policies or practices necessary to meet its obligations under the PDPA as was required in Section 12(a) of the PDPA. During the PDPC's investigation, the Organisation referred to the manner of handling the students' Personal Data as an "unwritten SOP".

The Organisation's Section 24 Obligation

The Deputy Commissioner also held that the Organisation breached its Section 24 Obligation for the following reasons:

(i) the Personal Data disclosed in question was very sensitive in nature, relating to: (i) NRIC numbers, which are of special concern to individuals given its capacity to identify an individual on its own[5]; and (ii) minors who were less than 21 years of age[6];
(ii) with regard to such sensitive Personal Data, organisations would be required to take extra precautions and ensure higher standards of protection under the PDPA, given that the safeguards to be implemented had to be commensurate with the amount and potential sensitivity of the information at risk;
(iii) the Organisation could have conducted regular training sessions to: (i) impart good data protection practices in staff and to strengthen their awareness; and (ii) ensure that its staff were apprised with the software used to process documents containing sensitive Personal Data; Aggravating and Mitigating Factors

Having found that the Organisation was in breach of the Relevant PDPA Obligations, the Deputy Commissioner saw fit to exercise his powers under the PDPA to issue remedial directions to the Organisation (including the direction for the Organisation to pay a financial penalty). In deciding on the financial penalty quantum to be awarded, the Deputy Commissioner took into account the following aggravating factors:

(i) the Personal Data disclosed was of a sensitive nature and the disclosure could cause substantial action or potential harm to the students;
(ii) the Organisation showed a lack of awareness of its obligations under the PDPA; and
(iii) the investigation process was delayed on many occasions by the Organisation's unwillingness to reasonably co-operate with the PDPC.

[3] Under Section 2 of the PDPA, an "organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore; or (b) resident, or having an office or a place of business in Singapore.

[4] Holding in *Re M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15

[5] Under the PDPC's Advisory Guidelines on the PDPA for Selected Topics at [6.1] (see https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/finaladvisoryguidelinesonpdpaforselectedtopics28march2017.pdf) ("**Selected Topics Guidelines**"), NRIC numbers are recognized as of special concern as they are unique to each individual and are assigned for the purposes of identifying that individual.

[6] Under the Selected Topics Guidelines, the PDPC recognizes certain considerations with regard to the Personal Data of minors, including that "there is generally greater sensitivity surrounding the treatment of minors".

The Deputy Commissioner however, was not inclined to reduce the financial penalty quantum on the basis that:

(i) the Organisation was a small registered charity with a thin budget;
(ii) the Organisation did not appoint a data protection officer and was thus unaware of the requirement to have a data protection policy;
(iii) the breach was due to inadvertence and ignorance that the NRIC data could be seen on its website;
(iv) the delay was caused by their surprise at the lapse and their need to obtain external advice as well as the Organisation's internal approval process to respond to the PDPC.

4.2.3. *Comments*

This case is instructive in illustrating the fundamental importance of putting in place structured internal policies and practices to comply with the PDPA, including the appointment of a data protection officer, and the implementation of data protection policies. Organisations which do not even have such basic policies and practices in place risk substantial enforcement action in the event of a complaint.

Organisations should also take care to evaluate the sensitivity of the Personal Data it is controlling or in possession of, and adopt reasonable security measures accordingly to safeguard such Personal Data. These measures could take the form of:

(i) administrative measures (such as imposing confidentiality obligations in employment agreements, and conducting regular training sessions for staff to impart good data handling practices);
(ii) technical measures (adopting appropriate access controls; or installing appropriate computer security software); or
(iii) physical measures (such as marking confidential documents clearly and prominently, storing them securely, properly disposing such confidential information that is no longer needed, and utilizing modes of delivery or transfer that afford appropriate levels of security).

The appropriate policies, procedures and standards which should be implemented will vary from organisation to organisation depending on, among other things, the type of data which the organisation is processing and the potential impact on the individual should such Personal Data suffer from unauthorised disclosure.

5. Taiwan

Nathan Snyder *(Associate), Eiger (nathan.snyder@eiger.law);* **Wendy Chu** *(Senior Associate), Eiger (wendy.chu@eiger.law).*

5.1. *Taiwan to implement new law on cybersecurity infrastructure*

Taiwan is in the process of implementing a new law governing security procedures for its critical information infrastructures. The newly promulgated law, the Cybersecurity Management Act (資通安全管理法) (the "Act") (also translated as the Information and Communication Security Management Act), was signed into law by the President on 6 June 2018, and is now awaiting enforcement regulations, clarifying rules, and its final effective dates, to be issued by the Executive Yuan.

The Act is intended to create standard operating procedures for monitoring and updating security systems among the following three categories of entities in Taiwan: (i) government agencies, (ii) less critical but specifically indicated non-government agencies, and (iii) critical infrastructure providers. "Critical infrastructure" is defined as all resources, systems and networks, whether physical or digital, any damage or curtailment of which would cause a substantial impact on national security, public interest, daily life, or economic activity.

The specific organisations that will constitute categories (ii) and (iii) will be determined by the Department of Cybersecurity, Executive Yuan. However, the Act so far indicates that category (ii) will include less critical state-owned enterprises and institutions which receive government funding. Category (iii) will be organisations that provide "critical infrastructures" and are indicated by the specific oversight authority for their industry and approved by the Executive Yuan as warranting coverage under the Act.

The Act requires entities falling under those three categories to implement a specific cybersecurity maintenance plan, which is essentially a set of policies, procedures, and mechanisms to ensure the security of any critical infrastructure or information for which the entity is responsible. The plans need to have a required level of rigor that varies depending on the nature and scale of the entity's role within the general infrastructure. These maintenance plans and their implementation must be reported to the relevant oversight authorities of the industries to which an infrastructure provider belongs. In addition to ongoing reporting about these plans, any security incidents must also be reported immediately to the authorities. The Act also grants auditing powers for the Department of Cybersecurity and provides penalties for failing to report incidents or implement an inadequate maintenance plan.

Presently, the Act requires clarifying regulations to be issued and final effective dates to be set by the Executive Yuan before it becomes fully into force. A public comment period for drafts of those regulations (listed below), began on 7 July 2018, and will continue for two months.

The following is a list of the draft regulations under the Act:

(a) "Enforcement Rules of Cybersecurity Management Act";
(b) "Regulations for Classification of Cybersecurity Responsibility";
(c) "Regulations for Reporting and Responding to Cybersecurity Incidents";
(d) "Regulations for Inspecting Implementation Status of Special Non-official Agencies' Cybersecurity Maintenance Programs";
(e) "Cybersecurity Information Sharing Regulations"; and

(f) "Award and Punishment Regulations on Cybersecurity Affairs for the Public Servants".

Director-General Hong-wei Jyan of the Department of Cybersecurity has stated that the Act is expected to be rolled out over three separate effective dates for entities covered under different categories. For category (i) entities, i.e. government agencies, the effective date will likely be 6 months after its legislative passage date. For category (ii) entities, i.e. less critical state-owned enterprises or government-funded institutions, the effective date will likely be 18 months after the Act's legislative passage date. For category (ii) entities, i.e. critical infrastructure providers, the effective date will likely be 12 months after the Act's passage date.