DREW & NAPIER

DATA PROTECTION QUARTERLY UPDATE

January 2017

In this issue

WELCOME MESSAGE

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

At the outset, we will study the reasons behind the five most recent enforcement decisions issued by the Personal Data Protection Commission (***PDPC***), which involved the PDPC taking action against several entities for breaching their obligations under the Personal Data Protection Act (No. 26 of 2012) (***PDPA***). Thereafter, in light of how courts, governments, and regulators around the world continue to deal with rapid technological advancements and its implications on personal data, we will proceed to analyse the emergence of new regulatory instruments and frameworks in several jurisdictions including the Philippines, Hong Kong and France. These developments are undeniably helpful in providing guidance for regulators and businesses in managing their data protection obligations.

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

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

IN THE NEWS

SINGAPORE

PDPC issues Enforcement Decisions in respect of six organisations

Between October and November 2016, the PDPC

issued enforcement decisions against the following six organisations for breaching their data protection obligations under the PDPA:

(a) GMM Technoworld Pte Ltd (***GMM***) (30 September 2016);

(b) Smiling Orchid (S) Pte Ltd (***Smiling Orchid***) (4 November 2016);

(c) My Digital Lock Pte Ltd (***MDL***) (4 November 2016);

(d) Jump Rope (Singapore) (***Jump Rope***) (24 November 2016);

(e) The Cellar Door Pte Ltd (***Cellar Door***) (23 December 2016); and

(f) Global Interactive Works Pte Ltd (***GIW***) (23 December 2016).

GMM

Background

On 30 September 2016, the PDPC took action against GMM, a company retailing products such as waterproof gadgets and measuring instruments, for the unauthorised disclosure of approximately 190 of its customers' personal data as a result of the lack of adequate security measures on its website.

In 2014, GMM included a product warranty registration feature to its corporate website, which was hosted on a third party server. This feature utilised Formidable Forms, a third-party paid plug-in for WordPress, which authorised GMM's website to collect personal data. As this plug-in could dynamically list and display on the website the personal data collected via the plug-in, this eventually led to the personal data of about 190 individuals being collected and displayed in a publicly accessible manner on the Internet.

PDPC's Findings

Upon conducting investigations, GMM was found to be in breach of section 24 of the PDPA as it had failed to implement reasonable security arrangements to protect the personal data in its possession or under its control. Specifically, GMM's "*lack of awareness of the Plug-in's actual functions, its wrong use of the Plug-in, and failure to take steps to configure it appropriately led to the unauthorised disclosure of the personal data of approximately 190 individuals"*.

The PDPC dismissed GMM's claims that it was ignorant and unaware that one of the functions of the plug-in was to display the personal data collected on its website and found that there was no reasonable excuse for the ignorance as Formidable Forms have, on its website, clear, accessible explanations and pictorial guides of the plug-in. The PDPC was of the view that an organisation ought to have sufficient understanding and appreciation of a product before making use of it.

Action by the PDPC

In considering the type of enforcement action to be taken against GMM, the PDPC took into account the following factors:

(a) **GMM's co-operation during investigations**: GMM was co-operative by providing its responses on a timely basis**.**

(b) **GMM's immediate and corrective action**: GMM took immediate steps to stop the further unauthorised disclosure and implemented corrective measures to protect its customer's personal data.

Accordingly, the PDPC imposed a financial penalty of S$3,000.

Smiling Orchid

Background

Smiling Orchid, a provider of food catering services, has a website that allows its customers to place their orders. Smiling Orchid outsourced the design and development of its website to T2 Web Pte Ltd (***T2***), the hosting of its website to Cybersite Services Pte Ltd (***Cybersite***), and the management of IT-related issues to East Wind Solutions Pte Ltd (***East Wind***).

On or around 10 November 2014, a customer of Smiling Orchid performed a random search of his full name on **www.yahoo.com.sg**, and discovered a link to a website containing his old order and his personal data (***Data Breach Incident***). By modifying the numerals at the end of the Uniform Resource Locator, the order details of other customers could also be accessed. In addition, there was a further hyperlink that could be easily

accessed without authentication to reveal a whole list of orders.

PDPC's Findings

Upon concluding its investigations, the PDPC found that Smiling Orchid breached its obligations under section 24 of the PDPA for failing to take reasonable security measures to protect its customers' personal data, an obligation to be met regardless of whether it had appointed data intermediaries to process customer personal data on its behalf.

In its decision, the PDPC considered the following issues: first, what the obligations did each of the relevant entities owe under the PDPA; and second, whether each entity had fulfilled or complied with the same.

(a) Obligations owed by each entity under the PDPA

At the outset, the PDPC established that Smiling Orchid was required to comply with section 24 of the PDPA as it was an organisation that had its customers' personal data in its possession or under its control.

It considered that T2 was not a data intermediary for the purposes of the PDPA, as its main job scope was to improve the design of the website, and not to carry out personal data processing activities. As such, it has no obligation to protect the personal data on Smiling Orchid's website.

In relation to Cybersite, the PDPC noted that it was a data intermediary as it hosted Smiling Orchid's website, and the personal data of Smiling Orchid's customers were stored in its servers. Thus, Cybersite is under an obligation to protect the personal data of Smiling Orchid's customers.

Lastly, whilst East Wind was categorised by the PDPC as a data intermediary of Smiling Orchid, as its engagement with Smiling Orchid only took place after the Data Breach Incident, East Wind's role does not factor in the PDPC's considerations pertaining to the Data Breach Incident.

(b) Did each entity fulfill their obligations under the PDPA?

The PDPC found that Smiling Orchid was in breach of its obligation under section 24 of the PDPA and noted that there was:

(i) **A failure to clearly designate security responsibilities between T2 and itself**: This resulted in general confusion between Smiling Orchid and T2 as to who was responsible for the protection of personal data on the website.

(ii) **A weak protection of system accounts and passwords**: Passwords were unprotected and stored in plain text, and there was no policy relating to password length or strength. New administrator accounts and passwords could be easily created, and there was no indication of any policy or logs as to who maintained those accounts and removed unused accounts.

(iii) **A failure to take sufficient corrective actions to remedy the defects in the system**: This was so even after it was made aware of the Data Breach Incident.

The PDPC also emphasised that parties must understand and agree on what services the service provider is providing, and properly document this information. Data controllers should follow through with the procedures to check that the outsourced provider is indeed delivering the services.

In contrast, the PDPC did not find Cybersite in breach of its obligations under the PDPA. As the host of Smiling Orchid's website, they had adopted adequate security arrangements, which included the consistent changing of system passwords and the updating of firewalls and related software. Moreover, the Data Breach Incident concerned issues that were at the application-level, and did not pertain to Cybersite, which was merely responsible for hosting the website.

Action by the PDPC

In considering the type of enforcement action to be taken against Smiling Orchid, the PDPC took into account the following factors:

(a) **Lack of co-operation on the part of Smiling Orchid**: Despite several attempts by the PDPC to establish the facts via verbal clarifications and issuance of a notice, the PDPC still had difficultly during its investigations to gain a clear picture of the facts it required.

(b) **Recurring breach and failure to take sufficient corrective action**: A year after the Data Breach Incident, Smiling Orchid experienced a recurring breach of the exact same nature, but had again failed to take sufficient corrective action, and to ascertain the root cause of such breaches.

(c) **Risk of database being easily disclosed**: Smiling Orchid's whole database was at risk of being easily disclosed.

(d) **Limited impact of the data breach**.

(e) Smiling Orchid's **attempts to remedy the breach**: This was done by engaging a new vendor East Wind.

Accordingly, apart from the imposition of a fine S$3,000 on Smiling Orchid, the PDPC also issued the following directions:

(a) The adoption of security arrangements to protect personal data on the new website.

(b) The conduct of a web application vulnerability scan of the new website, and to remedy all vulnerabilities identified by such a scan.

(c) Within 14 days after the above being carried out, the submission of a written update on the results of the vulnerability scan, and the measures that were taken by Smiling Orchid to patch all vulnerabilities identified by the vulnerability scan.

MDL

Background

After purchasing a gate from MDL, a company that sells digital locks and doors, a customer of MDL (***Complainant***) thereafter alleged that there were defects in the gate. A dispute subsequently ensued between the Complainant and the director of MDL, Mr A. Thereafter, Mr A proceeded to upload and post screenshots of his WhatsApp correspondence with the Complainant, which included the Complainant's phone number and residential address, onto his Facebook page. Mr A claimed that he did this only to transfer the screenshots from his WhatsApp application to his desktop computer, for the purposes of sending them to his solicitors in relation to legal proceedings between himself and the Complainant.

The PDPC had to determine the following issues:

(a) Whether the disclosure of the Complainant's personal data on Facebook without the Complainant's prior consent was in breach of the requirement to obtain consent under the PDPA, and whether it fell within the exceptions to obtaining consent (sections 13 and 17 of the PDPA).

(b) Whether MDL had failed to protect the personal data in its control by using Mr A's Facebook page as a means of transferring the Complainant's personal data (section 24 of the PDPA).

PDPC's Findings

(a) Consent Obligation

The PDPC held that the disclosure of the Complainant's personal data on Facebook without the Complainant's prior consent was not allowed under sections 13 and 17 of the PDPA. Section 17 of the PDPA provides that organisations are allowed to collect, use and disclose personal data without consent, in the circumstances set out in the Second, Third and Fourth Schedules of the PDPA.

At the outset, the PDPC established that Mr A was acting in the course of his employment as a director of MDL when transferring the Complainant's personal data through his Facebook page. Accordingly, any such disclosure by Mr A was regarded as a disclosure by MDL.

Next, the PDPC considered if the disclosure of personal data without consent fell within one of the exceptions to consent under the Fourth Schedule of the PDPA. In this regard, whilst MDL claimed that consent was not required because firstly, the personal data disclosed was publicly available data, and secondly, that was disclosed pursuant to investigations and proceedings, both of which are listed as exceptions in the Fourth Schedule, the PDPC held that neither of these exceptions were met. Not only was the specific information not publicly available, the disclosure of the screenshots on Facebook was not necessary for the transfer of files to Mr A's lawyers, as there were other ways in which this could be done.

As such, MDL was found to be in breach of section 13 of the PDPA for the disclosure of personal data without an individual's consent.

(b) Protection Obligation

By using Mr A's Facebook page as a means of transferring the Complainant's personal data, the PDPC found that MDL was in breach of section 24 of the PDPA as it had failed to protect personal data under its control. The method utilised by Mr A in transferring the personal data – via Facebook – was "*wholly inappropriate*" and entailed a "*substantial risk*" that the Complainant's personal data would be viewed.

As to what "reasonable security measures" mean and what this obligation entailed, the PDPC highlighted that this meant that the personal data is to be "reasonably protected from unauthorised access or interference, until the personal data reaches its intended destination". For illustration purposes, MDL could have password protected the uploaded screenshots, such that only authorised persons could view them. Alternatively, MDL could have transferred the screenshots by connecting the phone to the PC, without making use of the open internet.

Action by the PDPC

In considering the type of enforcement action to be taken against MDL for its breach of sections 13 and 24 of the PDPA, the following factors were taken into account by the PDPC:

(a) The personal data was only exposed on Mr A's Facebook page for a short period of one hour.

(b) The personal data exposed was of limited sensitivity, and consisted only of a mobile number and residential address.

(c) The breach was triggered by an error by a single employee, and not by failures of MDL's policies or processes.

(d) MDL had given its full cooperation in the investigation.

Accordingly, a warning was issued by the PDPC to MDL.

Jump Rope

Background

Jump Rope, a non-profit organisation that promotes and oversees the sport of rope skipping in Singapore, provides rope skipping training to students in Singapore schools. Jump Rope was set up by an individual who was also the owner and director of Emotion Learning Pte Ltd (***Emotion***) and Eltitude Pte Ltd (***Eltitude***), which provide enrichment and sports coaching services to schools respectively. The complainant was formerly employed by Emoticon and Eltitude as a part time instructor, and held a certification in rope skipping coaching issued by Jump Rope (***Complainant***).

Jump Rope alleged that the Complainant had engaged in unethical conduct during the course of his employment. After revoking the Complainant's certification, Jump Rope subsequently sent out an email to approximately thirty government schools, notifying them of the revocation of the Complainant's certification and of them blacklisting the Complainant. The said email contained the Complainant's name and NRIC number.

PDPC's Findings

Upon concluding its investigations, the PDPC found Jump Rope in breach of its obligations under sections 11, 13 and 20 of the PDPA, for disclosing the personal data of two former employees without consent and notification.

First, the PDPC established that consent had not been obtained from the Complainant in disclosing his personal data in the email sent to the schools.

Next, the PDPC considered if the disclosure without consent was reasonable in the specific situation. Section 11 of the PDPA provides that "*in meeting its responsibilities under the PDPA, an organisation shall consider what a reasonable person would consider appropriate in the circumstances."* In this regard, the PDPC did note that there could be circumstances where it is reasonable for an organisation to disclose personal data without consent, in respect of a blacklisting to warn others, but such situations are limited and highly dependent on the facts of each case. For example, one scenario where disclosure might be deemed reasonable would be if a former employee had misrepresented his employment status with his or her former employer. In such a case, it may be reasonable for the former employer to write to existing customers informing them of the facts.

In the present case, however, the PDPC found that there was no good business or legal reasons that justified Jump Rope's actions in writing to the schools to inform them of the blacklisting.

Furthermore, it is common for employees to leave for various reasons, including that of poor conduct.

In this regard, and given the potential adverse impact on the Complainant's reputation, Jump Rope's actions were neither appropriate nor reasonable.

Action by the PDPC

In considering the type of enforcement action to be taken against Jump Rope for its breach of sections 11, 13 and 20 of the PDPA, the following factors were taken into account by the PDPC:

(a) **Limited disclosures**: disclosures were made to a limited number of government schools; the personal data that was disclosed was limited; and the personal data that was disclosed was in relation to limited individuals.

(b) Jump Rope's **co-operation and forthcoming attitude** during the investigations.

Therefore, a warning was issued to Jump Rope.

Cellar Door and GIW

Background

Cellar Door, a company selling food and wine products, engaged GIW, its data intermediary, to host its website and customer database.

The PDPC found that personal data (including the full names, mobile and residential telephone numbers, residential addresses, email addresses and passwords) of some customers and users of Cellar Door's website had been leaked onto a website known as "Pastebin".

The issues to be determined by the PDPC were as follows:

(a) Whether GIW acted as data intermediary for Cellar Door with respect to the personal data hosted on GIW's servers.

(b) The respective obligations of GIW and Cellar Door under the PDPA.

(c) Whether Cellar Door and GIW had complied with these obligations.

PDPC's Findings

(a) Whether GIW acted as data intermediary for Cellar Door

"Data intermediary" is defined under the PDPA as an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation. The PDPC found that GIW would be categorised as a data intermediary for Cellar Door with respect to the personal data hosted on GIW's servers. This was because GIW was engaged to store, organise and manage personal data of Cellar Door's customers on GIW's servers and thus, this fell within the definition of "processing".

(b) The respective obligations of Cellar Door and GIW under the PDPA

The PDPC found that both Cellar Door and GIW were obliged under section 24 of the PDPA to provide reasonable security arrangements to protect the personal data of Cellar Door's customers. For Cellar Door, as section 4(3) of the PDPA provides that an organisation which outsources the processing of data to a data intermediary is obliged to protect the personal data processed on its behalf and for its purposes as if the personal data were processed by the organisation itself, accordingly, Cellar Door had to comply with section 24 of the PDPA.

While Cellar Door had engaged a data intermediary to provide hosting and database services, the PDPC held that Cellar Door still retained the main responsibility of ensuring the overall protection of the personal data, by taking steps such as implementing contractual arrangements that clearly outline the scope of GIW's responsibilities, and following through with operational checks to ensure that GIW carried out its functions adequately.

In relation to GIW, the PDPC held that GIW had the direct responsibility of protecting the personal data as it was the site administrator for the website and customer database. The extent of responsibility was dependent on the contractual arrangements it had with Cellar Door, which, in this case, was the protection of the customer database hosted by it.

The PDPC further emphasised the distinction between the possession and control of personal data, and highlighted that it was possible for a single set of personal data to be in the possession

of one organisation and still remain under the control of another. In this case, the personal data handled by GIW was considered to still be under the control of Cellar Door, given that GIW was Cellar Door's service provider and the personal data that GIW had processed were for Cellar Door's business purposes.

(c) Compliance of obligations under the PDPA

Upon concluding its investigations, the PDPC found that both Cellar Door and GIW had breached their protection obligation under section 24 of the PDPA as there were inadequate security policies and processes to protect the personal data; and both organisations had failed to put in place an overall security to guard against intrusions, attacks or unauthorised access.

(i) Inadequate security policies and processes

The PDPC found several key issues in the system's policies and processes.

First, Cellar Door had no procedure in place to carry out penetration testing on the IT system, which meant that there was no systematic way of identifying potential vulnerabilities. Next, it did not have an ongoing maintenance process to regularly update or patch the website against such risks and vulnerabilities. Lastly, there was no proper incident-reporting and management policy or process that managed technical issues and tracked them to their resolution.

Given the above shortcomings, the PDPC found that both Cellar Door and GIW failed to provide the necessary oversight, accountability, and control for the proper protection of the personal data of Cellar Door's customers.

(ii) Failure to protect against intrusions, attacks or unauthorised access

Further, the PDPC found the following significant gaps in the security measures implemented by Cellar Door and GIW:

- There was no firewall installed to protect GIW's server at the material time.
- The unused ports on the server were not closed at the time of the data breach, leaving it open to the risk of an external hacker exploiting the services running on these ports.
- The login credentials used to access the website were transferred in clear and unencrypted text.
- The administration password of the system was weak and consisted only of six-characters, which increases the chances of an intruder cracking the password and gaining full access to the system.

These security gaps exposed the system to unnecessary risks and attacks, such as penetration attacks, cracking and hijacking. Consequently, any intruder that was able to enter through these security gaps in the system would have gained access to the personal data held on that system.

In this regard, both GIW and Cellar Door were in breach of section 24 of the PDPA.

Action by the PDPC

In assessing the remedial directions to be imposed against Cellar Door and GIW, the PDPC took into account the following mitigating and aggravating factors:

(a) **Sub-standard security measures**: the security measures on the website to protect the personal data fell below the standard reasonably expected.

(b) **Lack of awareness or knowledge of required security measures**: Cellar Door and GIW had demonstrated a clear lack of awareness or knowledge of required security measures expected over the personal data in the website or their hosting environment.

(c) **Lack of co-operation during investigations**: Cellar Door and GIW were not cooperative during the PDPC's investigations and had displayed a cavalier attitude by providing incomplete responses to the notices issued by the PDPC.

(d) **The entire customer database was at risk**: while not all the personal data of the customers of Cellar Door had been disclosed, the fact was that the entire customer database was put at risk.

Consequently, the PDPC imposed a financial penalty of S$3,000 against GIW and also issued the following directions to Cellar Door:

(a) To conduct a vulnerability scan of its website, and patch all vulnerabilities identified by such a scan.

(b) To provide a written update providing details on the results of the vulnerability scan and the measures that were taken by Cellar Door to patch all vulnerabilities identified by the vulnerability scan in 14 days after the conduct of the abovementioned vulnerability scan.

(c) To pay a financial penalty of S$5,000.

PDPC updates Advisory Guidelines on the Personal Data Protection Act for Selected Topics

The PDPC has updated its Advisory Guidelines on the Personal Data Protection Act for Selected Topics (***ST Guidelines***). The ST Guidelines provide guidance on how the PDPA applies in specific contexts such as employment, the anonymisation of personal data, analytics and research activities, and data activities concerning minors.

The ST Guidelines are one of several sets of guidelines issued by the PDPC, which generally aim to assist in organisations and individuals' general understanding of the PDPA. They provide guidance on the manner in which the PDPC will interpret the provisions of the PDPA, and are not legally binding on the PDPC or any other party.

The main revision to the ST Guidelines is the updated Chapter 4 on Photography, Video and Audio Recordings, which provides clarification on the considerations for organisations engaging in photography, video or audio recording activities which capture personal data.

The revised Chapter 4 merges Chapter 4 (Closed-circuit television cameras) and Chapter 9 (Photography) of the previous ST Guidelines, and includes a new section on drones. The content of the previous Chapter 4 (Closed-circuit television cameras) and Chapter 9 (Photography) remains largely the same, while the main revisions are derived from the new section on drones.

The following non-exhaustive summary on drones will be discussed in the following order:

(a) What should organisations consider when using drones?

(b) What should organisations do if the drones used are likely to capture personal data?

(c) What should organisations do if personal data was unintentionally collected by the drones?

What should organisations consider when using drones?

At the outset, the ST Guidelines state that organisations will need to consider whether the drones that they deploy are likely to capture the personal data of individuals.

According to the ST Guidelines, generally, the use of drones with photography, video and/or audio recording functions are subject to the same obligations under the PDPA as those applicable to other equipment with similar functions. As such, an organisation which deploys drones that are likely to capture personal data of individuals, must generally notify and seek consent from such individuals in respect of the purposes for its collection, use, or disclosure of their personal data captured by the drones, unless an exception in the PDPA applies.

In addition, the ST Guidelines emphasise that organisations should be aware of the guidelines and requirements of other authorities in relation to the operation of drones. Division 4 of the Air Navigation Act (Cap. 6) and Part III of the Public Order Act (Cap. 257A) are some examples of legislation which provides the boundaries and prohibitions of an organisation's operation of drones. If organisations are in any doubt as to the applicability of any laws and regulations in relation to the operation of drones, the organisations should clarify their doubts with the Civil Aviation Authority of Singapore.

What should organisations do if the drones used are likely to capture personal data?

The PDPA requires organisations to obtain consent from individuals before collecting, using and disclosing their personal data. Accordingly, to fulfil this consent requirement, an organisation must provide notification of the purposes for the collection, use or disclosure of personal data captured by its drones.

The notifications should fulfil the following requirements:

(a) The notification should specify that photography, video and/or audio recording is taking place.

(b) The notification should generally be placed so as to enable individuals to have sufficient awareness that drones are in operation in the general locale.

For example, a notice can be placed at points of entry to the area of operation of the drones.

In addition, the ST Guidelines highlight that there is an exception to the consent requirement for the collection, use and disclosure of personal data that is publicly available under the PDPA. "Publicly available" personal data refers to personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

As such, when the individual appears at a public event, a photograph, video or audio recording taken of the individual at such an event or location would likely be personal data that is publicly available, and consent is not likely to be required for the collection, use or disclosure of such personal data.

Nevertheless, organisations may still opt to provide notifications as a matter of prudence and best practice. The ST Guidelines state that there are several possible ways of providing notifications which include placing signages at entrances to the areas where the drones would be flown, at clearly identifiable locations along the drone's flight path, or at the launch site.

What should organisations do if personal data was unintentionally collected by the drones?

The ST Guidelines provide that organisations should ensure that they adhere to the pre-planned flight path of drones, and implement policies restricting the use of any personal data that is unintentionally collected, such as when drones accidentally veer off-course from the pre-planned flight path and consequently collect personal data without consent.

Notably, the ST Guidelines set out that the deletion of such personal data would not prevent the PDPC from taking any enforcement actions against the organisation.

The updated ST Guidelines may be accessed **here**.

PDPC to revise Anonymisation Chapter of its Advisory Guidelines

The PDPC has announced that it will be revising the anonymisation chapter of its ST Guidelines, which was first issued in September 2013. Anonymisation refers to the process of stripping out information in data sets that can identify a person.

Generally, the revision of the chapter on anonymisation aims to:

(a) Provide greater clarity on what the PDPC considers as anonymised data.

(b) Highlight important considerations that organisations should take into account when deciding whether to anonymise data.

(c) Clarify the responsibilities of organisations in using such data.

This clearly reflects the PDPC's continuous efforts in ensuring that the ST Guidelines that it publishes remain updated and relevant to suit the changing landscape, particularly in light of rapid technological advancements.

Currently, as the PDPC is consulting the industry on the proposed revisions, further details will be published in the coming months.

HONG KONG

Tips and advice on personal data protection when using e-Wallets

The Hong Kong Payment Systems and Stored Value Facilities Ordinance commenced operation on 13 November 2015. In connection with its commencement, the Hong Kong Monetary Authority (***HKMA***) and the Office of the Privacy Commissioner for Personal Data (***PCPD***) have respectively highlighted, in August 2016, certain privacy-related issues that users and providers of stored value facilities (***SVFs***), loosely understood as "e-wallets", should pay attention to.

General privacy issues

Both the HKMA and PCPD have noted that mobile applications of SVFs often request access to their users' mobile phone contact lists and other stored information, such as locations. Such collection of additional personal data might not always be intrusive of privacy although SVFs should obtain the necessary consents before doing so.

The PCPD has also offered the following tips and advice on personal data protection. SVF licensees are expected to:

(a) Allow users to determine if they wish to grant the mobile application permission to access or collect their personal data pursuant to the stated purposes and to withdraw their consent at any time without prejudice to their use of the SVF.

(b) Adhere to the requirements of proportionality and transparency under the Personal Data (Privacy) Ordinance (***Ordinance***) when making such requests for access or collection.

(c) Adopt simple, succinct and user-friendly language and presentation to communicate their purposes for collection of personal data.

(d) Seek explicit and voluntary consent from their users where they intend to use personal data collected through the SVF for purposes not directly related to payment, and adhere to the requirements of the Ordinance which apply to direct marketing.

(e) Perform formal risk assessments on the full data cycle to determine the appropriate level of protection to be given to the personal data, pursuant to their obligations to ensure the accuracy and security of the personal data they collect.

(f) Comply with the data access and correction requests of their users, pursuant to the Ordinance.

(g) Adopt contractual or other means to ensure the following in situations where an outsourcing agent is engaged to process personal data on the SVF licensee's behalf: (i) prevent personal data transferred to the data processor from being kept longer than necessary for the processing of the data, and (ii) prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Users of SVFs are advised to:

(a) Find out more about how the SVF licensees will handle and process the personal data they collect.

(b) Understand and select the appropriate privacy settings for the SVF application they use.

(c) Understand what types of mobile device data that the SVF application will access and disable access as appropriate.

(d) Avoid operating the SVF application over public or unsecured networks.

(e) Use complex passwords and avoid recycling passwords that are used for less-sensitive services.

(f) Ensure that the device on which the SVF application is operated from has appropriate anti-theft features, security patches and anti-virus software enabled.

(g) Avoid opening attachments or accessing links in unexpected email messages unless clarified with the sender beforehand.

(h) Regularly monitor their transaction records for unauthorised activities.

Privacy issues arising from commercial partnerships

HKMA has noted that some SVF licensees may collaborate with merchants to send marketing communications to users of the particular SVF. Users are advised to read the terms and conditions of these SVFs carefully and to understand the types of personal data collected and the purpose of doing so. In addition, users should also be aware that while individual SVF licensees may not retain their users' personal data for marketing purposes, collaborating merchants may store the personal data of these users if they effect payment through the SVFs.

Staff of five financial firms arrested for illegal use of customer data

On 13 December 2016, the PCPD released a media statement responding to media enquiries

relating to the arrest of staff from five financial firms for alleged bribery in connection with the disclosure of confidential customer information.

The PCPD declined to comment on the case as it was still under investigation by another law enforcement agency but highlighted to the public that it was an offence under section 64 of the Ordinance to disclose personal data without consent. In particular, it explained that:

> "*Under section 64 of the Personal Data (Privacy) Ordinance, any person who discloses personal data without the consent of the data controller of such data (e.g., the banks in this case) with an intent to obtain financial gain or to cause financial loss to the data user is an offence with a maximum fine of HK$1 million and imprisonment for 5 years.*"

The PCPD also referred the public to the "Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry" and the "New Guidance on Direct Marketing" for further information on the requirements of the Ordinance and recommended practices for the handling of customers' personal data.

Elsewhere, the Hong Kong Independent Commission Against Corruption had issued a press release on 12 December 2016 confirming the arrest of 29 current and former employees of five financial institutions, comprising four banks and a finance company in connection with this matter, which arose from a corruption complaint. It was revealed that the bank managers (who formed part of those arrested) had allegedly accepted bribes in exchange for the disclosure of confidential customer information for the purposes of touting personal loan business.

Signing of Asia Privacy Bridge Forum Joint Declaration 2016 to promote privacy research, education and policy co-operation in Asia

On 10 November 2016, the PCPD released a media statement announcing its signing of the Asia Privacy Bridge Forum Joint Declaration 2016 (***Declaration***) in Seoul, South Korea, on 2 November 2016. Other signatories included the Korea Internet & Security Agency, Barun ICT Research Center (based at South Korea's Yonsei University), and privacy experts and academia from China, South Korea and Japan.

The Asia Privacy Bridge Forum was established to determine the practical steps that Asian economies may take to bridge the gaps in their data protection regimes. Pursuant to the Declaration, parties agreed to "uphold the following tenets that advance [their] essential values on privacy, while remaining respectful of one another's historical and procedural differences":

(a) To deepen international research relations: by promoting collaboration and co-operation in their research agenda, policy development and enforcement in the area of personal data protection, while acting responsibly and cooperatively to ensure a balance between protection and fair use of personal data.

(b) To collaborate on privacy research programmes: by participating in joint research programmes to share knowledge on issues that can improve personal data protection and the fair use of information, as well as to find solutions to bridge the gaps among different personal data protection regimes in the Asian region.

(c) To strengthen policy cooperation: by organising the Asia Privacy Bridge Forum on an annual basis to consider regional and international laws, policies and other controversial issues on personal data protection, and to promote co-operation and communication with other regional forums with the objective of effectively implementing the ideas and opinions raised during the forum.

Privacy Commissioner issues "Bring Your Own Device (*BYOD*)" information leaflet

On 31 August 2016, the PCPD issued the "Bring Your Own Device (***BYOD***)" Information Leaflet (***Leaflet***) to highlight the risks to personal data privacy protection that an organisation needs to consider when it develops a policy to allow employees to use their own mobile devices to access and handle the organisation's information (***BYOD Devices***). Such a policy is often referred to as a "BYOD policy".

In the Leaflet, the PCPD reminded organisations that the decision to allow BYOD Devices would enable personal data collected by the organisation (***Organisation-collected Personal Data***) to be transferred from a secure corporate environment to the less secure BYOD Device, over which the organisation has less control despite remaining fully responsible for compliance with the Ordinance in relation to such transferred Organisation-collected Personal Data.

The PCPD identified four potential aspects that an organisation intending to implement a BYOD policy should consider:

(a) How the organisation may implement its personal data retention and destruction policies to the Organisation-collected Personal Data stored in the BYOD Device.

(b) How the organisation may retain control over the Organisation-collected Personal Data that is stored in the BYOD Device and the subsequent use of such personal data by its employees.

(c) How the organisation may protect the Organisation-collected Personal Data stored in the BYOD Device without infringing the personal data privacy of the employee.

(d) How the organisation may access and correct the Organisation-collected Personal Data stored in the BYOD Device pursuant to the data subject's request.

It also provided the following guidance:

(a) Notwithstanding the need for the organisation to protect the transferred Organisation-collected Personal Data, it should respect the private information contained in the BYOD Device when implementing any protective measures.

(b) Organisations should consider the following as part of their compliance with the Ordinance:

  (i) Whether employees are sufficiently reminded not to misuse the Organisation-collected Personal Data that they transfer to their BYOD Devices.

  (ii) Whether they have implemented sufficient technical measures to balance the access and storage of Organisation-collected Personal Data by the BYOD Device against the private information in the same device, with relevant considerations including the existence of any alternatives to directly storing such personal data in the device, the existence of any effective control system for accessing such personal data, and the implementation of any security measures to protect the personal data accessed via or stored in the device.

As part of the best practices that an organisation may adopt, the PCPD recommended that organisations should adopt the following measures:

(a) Establish a BYOD policy setting out:

  (i) The respective roles and obligations of the organisation and its employees in relation to BYOD.

  (ii) Criteria by which the organisation determines the information and mobile applications that the BYOD Device may access, the permitted types of BYOD Devices, and the applicable standards.

  (iii) Technical measures to protect the Organisation-collected Personal Data from the employee's own information.

  (iv) Measures through which the organisation may ensure compliance with, and enforce, the BYOD policy.

(b) Conduct a risk assessment on the types of personal data accessible by or stored in the BYOD Device and the damage and likelihood of a data breach, and develop (or seek appropriate assistance to develop) commensurate access controls and security measures.

(c) Apply technical solutions to protect the transferred Organisation-collected Personal Data and enhance the security of the BYOD Device, such as implementing an independent additional access control measure (e.g. two-factor authentication, time-out after inactivity etc.), suitable additional encryption, proper authenticating and encrypting procedures for the transmission of Organisation-collected Personal Data to and from the BYOD Device to prevent unauthorised access, and auto-erasure mechanisms for Organisation-

collected Personal Data stored in the BYOD Device if warranted.

(d) Regularly monitor, review and ensure compliance with its policies and measures, as well as monitor the continued compliance of these policies and measures in light of technological advances or business changes.

CHINA

China passes its Cybersecurity Law

On 7 November 2016, the Standing Committee of the National People's Congress of the People's Republic of China passed its new cybersecurity law (***Cybersecurity Law***) after months of public consultation and the release of two drafts. As it currently stands, the new Cybersecurity Law substantially adopts the second draft released on 5 July 2016, and is slated to come into effect on 1 June 2017.

This law is aimed at tightening China's network and national security, protecting the lawful rights of citizens, legal persons and organisations, and promoting healthy social and economic development in this increasingly information driven age. The Cybersecurity Law focuses on the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the mainland territory of China.

Under the Cybersecurity Law, there are three key aspects, namely technology regulation, co-operation with authorities and data localisation.

Technology regulation

Under Article 23, the Cybersecurity Law stipulates that critical network equipment and specialised network security products are required to be certified by a qualified establishment or meet the requirements of safety inspections. An official catalogue of critical network equipment and specialised network security products is expected to be formulated and released, in the hope of promoting reciprocal recognition of safety certifications and inspection results, so as to avoid duplicate certifications and inspections.

Co-operation with authorities

The Cybersecurity Law introduces new requirements for network operators to co-operate with the authorities, such as Article 21 requiring them to perform security protection duties according to the requirements of China's tiered network security protection system, which include network operators keeping network log records for six months. Article 22 also stipulates that network operators are to notify the authorities of any security defects discovered in their systems. Article 28 of the Cybersecurity Law also imposes duties on network operators in the provision of technical support and assistance to the public security organs' and state security organs' lawful activities in preserving national security and investigating crimes.

Data localisation

Critical information infrastructure operators are subject to the data localisation obligation, whereby they are required to store personal data and other important business data collected within mainland China. If cross-border data transfers for collection and use is necessary for business requirements, security assessments will be conducted.

Furthermore, critical information infrastructure operators are also subject to other duties, which are in addition to those imposed on network operators, such as security protection (Article 34), going through national security reviews (Article 35) and entering into security and confidentiality agreements with the network product and service providers (Article 36).

Other personal data-related requirements

The Cybersecurity Law also emphasises that network operators are to abide by the principles of legality, propriety and necessity when collecting and using personal information of users. They are obliged to state the purposes, means and scope for collecting or using the personal information, and are also required to obtain the consent of the individual concerned (Article 41).

Network operators are also prohibited from disclosing a user's personal data to third parties, tamper with, or destroy the personal data gathered without the consent of the user unless the data has been so processed such that the user is unidentifiable (Article 42). Network operators are therefore obliged to adopt technological measures to ensure the security of the citizens' personal information and prevent the loss of such information.

The passing of this Cybersecurity Law has raised concerns amongst business groups that the new rules will isolate China from the wider digital economy and discourage foreign entry, despite the Chinese government's confidence that the law is consistent with the rules of international trade and is not intended to shut out foreign companies.

THE PHILIPPINES

The Philippines finalizes Data Privacy Act Implementing Rules

The National Privacy Commission of the Philippines (***NPC***) has issued the Implementing Rules and Regulations of the Data Privacy Act of 2012 (Republic Act No. 10173) (***IRR***), representing a significant development in data privacy regulation in the Philippines. The IRR complements the Data Privacy Act of 2012 (***DPA 2012***), by effectively implementing the provisions of the DPA 2012. The IRR took effect 15 days after its publication on 9 September 2016.

Scope and Application of the IRR

The IRR emphasises the general policy of the DPA 2012, which is to safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development. The IRR and the DPA 2012 apply to the processing of personal data by any natural and juridical person in the government or private sector, and apply to an act done or practice engaged in and outside of the Philippines if:

(a) the natural or juridical person involved in the processing of personal data is found or established in the Philippines;

(b) the act, practice or processing relates to personal data about a Philippine citizen or Philippine resident;

(c) the processing of personal data is being done in the Philippines; or

(d) the act, practice or processing of personal data is done or engaged in by an entity with commercial links to the Philippines, such as by contract or business.

General Data Privacy Principles

Section 17 of the IRR provides that the processing of personal data must be done in adherence to the general principles of transparency, legitimate purpose, and proportionality. Furthermore, section 18 sets out the general principles in the collection, processing and retention of personal data. They are as follows:

(a) Collection must be for a declared, specified, and legitimate purpose.
(b) Personal data shall be processed fairly and lawfully.

(c) Processing should ensure data quality.

(d) Personal data shall not be retained longer than necessary.

(e) Any authorised further processing shall have adequate safeguards.

General requirements under the IRR

The IRR builds on the more general requirements of the DPA 2012 by imposing several registration and compliance obligations on personal information controllers and processors. The key obligations are as follows:

(a) Registration of Personal Data Processing Systems.

The IRR requires certain persons to register their personal data processing systems with the NPC. A personal information controller or personal information processor that is involved in the processing of sensitive personal information belonging to at least 1,000individuals need to comply with this registration requirement. Controllers or processors that employ less than 250 persons are generally exempt from the registration requirement, subject to certain conditions.

The IRR also requires personal information controllers that carry out any wholly or partly automated processing operations to notify the NPC when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject.

(b) Reporting requirements

The IRR also provides more detail on the notification process to the NPC and data subjects for data breaches. Section 38 of the IRR states that the NPC and affected data subjects shall be notified by the personal information controller within 72 hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that, a personal data breach requiring notification has occurred.

According to section 39 of the IRR, a notification must describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. It must also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the personal information controller, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

(c) Security measures for the Protection of Personal Data

The IRR provides further detail on the security measures to be adopted in the processing of personal information. Section 25 provides that personal information controllers and personal information processors shall implement reasonable and appropriate organisational, physical, and technical security measures for the protection of personal data.

Organisational security measures include the following:

(i) Designation of a Compliance Officer who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

(ii) Implementation of data protection policies that provide for organisation, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

(iii) Maintenance of records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data.

(iv) Select and supervise its employees, agents, or representatives, particularly those who will have access to personal data.

(v) Develop, implement and review procedures and policies on the processing of personal data.

(vi) Enter contractual agreements to ensure that its personal information processors also implement the security measures required by the DPA 2012 and the IRR.

Physical security measures include the following:

(i) Implement policies and procedures to monitor and limit access to and activities in the room, workstation or facility.

(ii) Design office space and work stations with the aim of providing privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.

(iii) Clearly define the duties, responsibilities and schedule of individuals involved in the processing of personal data to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time.

(iv) Implement policies and procedures regarding the transfer, removal, disposal, and reuse of electronic media, to ensure appropriate protection of personal data.

(v) Implement policies and procedures that prevent the mechanical destruction of files and equipment. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Lastly, technical security measures include the following:

(i) Establish a security policy with respect to the processing of personal data.

(ii) Establish safeguards to protect the computer network against accidental, unlawful or unauthorised usage.

(iii) Regularly monitor for security breaches.

(iv) Establish a process for regularly testing, assessing, and evaluating the effectiveness of security measures.

(v) Encrypt personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

According to section 67 of the IRR, personal information controllers and personal information processors have a one year grace period to register their data processing systems or automated processing operations with the NPC. In this one year, they may apply for an extension of the period within which to comply with the issuances of the NPC. The NPC may then grant such request for good cause shown. The one year period starts from the date of effectivity of the IRR, which is 9 September 2016.

Philippines National Privacy Commission issues its first four Memorandum Circulars

In the final quarter of 2016, the NPC issued its first set of four memorandum circulars concerning personal data. They are as follows:

(a) NPC Circular 16-01 – Security of Personal Data in Government Agencies.

(b) NPC Circular 16-02 – Data Sharing Agreements Involving Government Agencies.

(c) NPC Circular 16-03 – Personal Data Breach Management.

(d) NPC Circular 16-04 – Rules of Procedure.

Security of Personal Data in Government Agencies

The first circular, MC No. 16-001 (***First Circular***), relates to the **Security of personal data in government agencies**, and applies to all government agencies engaged in the processing of personal data. It aims to assist government agencies engaged in the processing of personal data to meet their legal obligations under the DPA 2012 and the IRR.

The First Circular defines the duties and responsibilities of such government agencies. Broadly, a government agency engaged in the processing of personal data shall observe the following duties and responsibilities:

(a) designate a data protection officer;

(b) conduct a privacy impact assessment for each program, process or measure within the agency that involves personal data;

(c) create privacy and data protection policies, taking into account the privacy impact assessments, as well as sections 25 to 29 of the IRR;

(d) conduct a mandatory, agency-wide training on privacy and data protection policies once a year;

(e) register its data processing systems with the NPC in cases where processing involves personal data of at least one thousand individuals; and

(f) cooperate with the NPC when the agency's privacy and data protection policies are subjected to review and assessment, in terms of their compliance with the requirements of the DPA 2012, the IRR, and all issuances by the NPC.

Section 5 further elaborates on what a privacy impact assessment should entail. The First Circular also has provisions on the storage and transfer of personal data, agency access to personal data, and the disposal of personal data. For more information, the First Circular can be found **here**.

Data Sharing Agreements Involving Government Agencies

The second circular, MC No. 16-002 (***Second Circular***) contains rules and guidelines on **Data Sharing Agreements involving government agencies**. Government agencies are allowed to share or transfer personal data under its control or custody to a third party through a data sharing agreement, in order to facilitate the performance of a public function or the provision of a public service. The Second Circular applies to personal data under the control or custody of a government

agency that is being shared with or transferred to such a third party.

Importantly, section 6 provides that a data sharing agreement must be in writing and must comply with several conditions. Broadly, the conditions are as follows:

(a) The data sharing agreement must specify the purpose of the data sharing agreement, including the public function or public service the performance or provision of which the agreement is meant to facilitate.

(b) The data sharing agreement must identify all personal information controllers that are party to the agreement.

(c) The data sharing agreement must specify the term or duration of the agreement.

(d) The data sharing agreement must contain an overview of the operational details of the sharing or transfer of personal data under the agreement;

(e) The data sharing agreement must include a general description of the security measures that will ensure the protection of the personal data of data subjects, including the policy for retention or disposal of records.

(f) The data sharing agreement must state how a copy of the agreement may be accessed by a data subject.

(g) If a personal information controller grants online access to personal data under its control or custody, the data sharing agreement must specify the following information:

  (i) Justification for allowing online access;
  (ii) Parties that shall be granted online access.
  (iii) Types of personal data that shall be made accessible online.
  (iv) Estimated frequency and volume of the proposed access.
  (v) Program, middleware and encryption method that will be used.

(h) The data sharing agreement must identify the method that shall be adopted for the secure return, destruction or disposal of the shared data and the timeline therefor.

(i) The data sharing agreement must specify any other terms or conditions that the parties may agree on.

The Second Circular also sets out other data-sharing safeguards to be implemented by personal information controllers in the government. These include ensuring that adequate security measures are in place before allowing online access to personal data, and providing for the return, destruction or disposal of transferred personal data. For more information, the Second Circular can be found **here**.

Personal Data Breach Management

The third circular, NPC Circular 16-03 (***Third Circular***) provides the framework for personal data breach management and the procedure for personal data breach notification and other requirements, and apply to any natural and juridical person in the government or private sector processing personal data in outside of the Philippines.

Rule II of the Third Circular sets out guidelines for organisations on personal data breach management, including the creation of a data breach response team to ensure timely action in the event of a security incident or personal data breach, and the implementation of organisational, physical and technical security measures to prevent or minimize the occurrence of a personal data breach.

Rules III and IV further set out guidelines for the prevention of a personal data breach, and guidelines for incident response policy and procedure in the event of a data breach.

Lastly, Rule V provides for the procedure for personal data breach notification and other requirements. The Third Circular provides a summary table of the requirements, as follows:

What is subject to the notification requirements	A security breach that: • Involves sensitive personal information, or information that may be used to enable identity fraud. • There is reason to believe that information have been acquired by an unauthorised person. • The unauthorised acquisition is likely to give rise to a real risk of serious harm.

Who should notify	The personal information controller, which controls the processing of information, even if processing is outsourced or subcontracted to a third party.
When should notification of Commission be done	Within 72 hours from knowledge of the personal data breach, based on available information. Follow up report should be submitted within five (5) days from knowledge of the breach, unless allowed a longer period by the Commission.
When should data subjects or individuals be notified	Within seventy-two (72) hours from knowledge of the breach, unless there is a reason to postpone or omit notification, subject to approval of the Commission.
What are the contents of notification to Commission	In general: 1. nature of the breach 2. sensitive personal information possibly involved 3. measures taken by the entity to address the breach 4. details of contact person for more information
What are the contents of notification to data subject	In general, same contents as notification of Commission but must include instructions on how data subject will get further information and recommendations to minimize risks resulting from breach.
How will notification be done?	Commission may be notified by written or electronic means but the personal information controller must have confirmation that the notification has been received. Data subjects or affected individuals shall be notified individually, by written or electronic means, unless allowed by the Commission to use alternative means.
How will notification be done?	Commission may be notified by written or electronic means but the personal information controller must have confirmation that the notification has been received. Data subjects or affected individuals shall be notified individually, by written or electronic means, unless allowed by the Commission to use alternative means.
Other requirements	Cooperate with the Commission where there is an investigation related to the breach. Documentation of all security incidents and the submission of an annual report to the Commission.

For more information, the Third Circular can be found **here**.

Rules of Procedure

The fourth circular, NPC Circular 16-04 (***Fourth Circular***) applies to all complaints filed before the NPC or such other grievances, requests for assistance or advisory opinions, and other matters cognizable by the NPC.

Broadly, the Fourth Circular sets out guidance on who may file complaints, the procedure for filing complaints, such as the filing fees to be paid, and the form and content of any complaint. The Fourth Circular also sets out the evaluation procedure that the NPC has to undertake upon receipt of a complaint, and provides for the option to resort to alternative modes of dispute resolution in relation to complaints received, such as the assignment of a mediation officer to assist the complainant and respondent to reach a settlement agreement.

For more information, the Fourth Circular can be found **here.**

AUSTRALIA

Australia introduces the Privacy Amendment (Notifiable Data Breaches) Bill 2016

On 19 October 2016, the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (***Bill***) had its First Reading in the Australian Parliament. If the Bill is passed, the Bill will require organisations subject to the Privacy Act 1988 (***Act***) to notify the Australian Information Commissioner (***Commissioner***) and the affected individuals if the entity experiences a data breach of a certain severity as specified in the Bill.

What type of data breach will require mandatory notice?

A data breach requiring mandatory notice refers to one that involves any unauthorised access, disclosure or loss of personal data which is objectively likely to result in serious harm to any of the individuals to whom the information relates.

As to what "likely to result in serious harm" refers to, the Bill suggests the consideration of the following factors:

(a) What type of information was accessed, disclosed or lost and how sensitive it was?

(b) What security measures are in place to protect that information, such as passwords, access control restrictions or encryption, and how secure these measures are?

(c) Would the security measures make the information unintelligible or meaningless to the unauthorised?

(d) What kind of person can obtain the said information? What is the likelihood that those who obtain the information will be able to circumvent the existing security measures or technology?

(e) What was the nature of harm resulting from the breach?

When must an entity provide notice under the Bill?

The two grounds that obliges organisations to provide notice under the Bill are:

(a) if the entity has reasonable grounds to believe that an eligible data breach has occurred; or

(b) if the Commissioner directs the company to provide notification of the breach.

Duty to investigate

If an entity has reasonable grounds to suspect a data breach, the Bill introduces an obligation on the entity to carry out a reasonable and expeditious assessment of whether the relevant circumstances amounts to an eligible data breach, which is to be conducted within 30 days of learning of the reasonable grounds.

What are the obligations under the notification requirement?

(a) Upon investigation, if the entity finds reasonable grounds for believing there has been an eligible data breach, the entity must prepare a statement and provide a copy to the Commissioner.

(b) The statement should include the following information:

  (i) the entity's name and contact details;
  (ii) a description of the breach;
  (iii) the type of information that was affected by the breach; and
  (iv) the steps that individuals should take in response to the breach.

(c) If upon investigation, the entity discovers that the eligible data breach also affects other entities, the statement should include the name and contact details of the other entities.

(d) If practicable, entities should take steps reasonable in the circumstances to notify the following people with the same information contained in the statement:

  (i) all individuals to whom the information accessed, disclosed or lost relates to; and
  (ii) all individuals who are at risk from the data breach

(e) If not practicable, entities should publish the statement on its website and take reasonable steps to publicise it.

(f) If there are other laws which ordinarily prohibit disclosure of such information as was accessed, disclosed or lost to constitute an eligible data breach, the notification requirements would not apply.

(g) The Commissioner also has the power to provide exemptions from the notification requirements, which may be granted on application by the entity or on the Commissioner's own initiative. Such exemptions are to be considered in light of the public interest or any advice from law enforcement or national security bodies.

(h) However, equally, the Commissioner may direct an entity to notify according to the obligations and circumstances listed above.

Successful remedial action

If the following actions are taken by an entity, the unauthorised access, disclosure or loss would subsequently not be considered as an eligible data breach:

(a) The entity takes remedial action related to the unauthorised access, disclosure or loss.

(b) The remedial action is taken before the unauthorised access, disclosure or loss can do serious harm to the individual concerned.

(c) The result of the remedy would lead a reasonable person to conclude that the access would not likely result in serious harm to any individuals.

After a successful remedial action, entities no longer need to notify individuals. In addition, there will also be no infringement of the Act, which if breached, triggers the enforcement mechanisms of the Act and allows the Commissioner to impose fines of up to A$1.8m (S$1.9m) for serious or repeated infringements of the Act.

Australian Red Cross Blood Service data leak

On 28 October 2016, the Australian Red Cross Blood Service (***Blood Service***) reported an unauthorised access to back-up copy of a database containing donor responses to an online enquiry form. The unauthorised access was due to an error by the third party IT vendor that maintains the Blood Service's website. The vendor placed the backup database containing registration information of 550,000 donors, including their names, addresses, dates of birth and other personal details, on an unsecured part of the website, allowing easy access to the entire database.

Subsequently, apart from reporting the data breach to the Information Commissioner, the Blood Service also took steps to remedy the breach, including the publication of a statement on its website and notifying donors via text message. As the file did not contain sensitive medical information and all known copies of the data has been deleted, the information accessed was deemed to have a low risk of future direct misuse. Thereafter, the Information Commissioner issued a statement indicating plans to open an investigation into the incident and also to work with the Blood Service to deal with other issues arising from the data breach.

FRANCE

France adopts Digital Republic Law

On 7 October 2016, France adopted a Digital Republic Act (***Act***). Prior to the adoption of the Act, the draft bill underwent a public national consultation.

The Act anticipates the European Union (***EU***) General Data Protection Regulations (***GDPR***). In other words, the substantial amendments to French data protection law which implements the GDPR would take effect before the GDPR itself formally enters into force in May 2018. Even though the GDPR establishes a harmonised regime for data protection in Europe, this law shows that Member States still retain the power to enact more stringent country-specific laws.

The following are some of the important changes to French data protection law:

(a) General right for individuals to decide how their data is used or processed

In addition to specific rights that individuals have under the Act, individuals also have a general right to decide and control how their personal data is used. However, it is unclear how this right itself will be enforced in practice. Nevertheless, it seems that this right would be implemented by specific rights that the Act accords to individuals, such as the right to data portability. For example, where data controllers have collected personal data electronically, individuals must be granted the right to exercise their rights by electronic means where possible.

(b) Ability to impose higher fines

The Commission Nationale de l'Informatique et des Libertés (***CNIL***), the French Data Protection Authority, will now be able to impose fines of up to €3m (S$4.6m), up from €150,000 (S$227,800) under the previous regime. When the GDPR enters into force, the CNIL will be able to impose fines up to 4% of the global annual turnover or up to €20 million (S$30.4m) in accordance with GDPR Article 83 of the GDPR.

(c) Right to data portability

Individuals will have the right to obtain from data controllers the personal data that an organisation holds about them in an easily accessible and understandable format. This is an instance of the early implementation of data portability rights, as explicitly guaranteed in Article 20 of the GDPR, before the GDPR comes into force.

(d) Expanded notice requirements for data retention periods

Data controllers must provide individuals with information about the length of time their data will be stored. If that is not possible, the data controller must provide the criteria used in the determination of how long the data will be stored.

(e) Notice requirements for algorithmic decision-making

Decisions made about an individual using algorithmic treatment must be explicitly mentioned to the individual concerned. If the individual requests, the data controller must communicate the rules that govern the algorithmic treatment and the characteristics of its implementation to the individual.

(f) Right to privacy after death

Individuals have the right to decide how their data may be processed, stored, erased or communicated after death. This includes the issuance of general guidelines for how all their data may be used after death, which is stored in a central register maintained by the state. In addition, individuals may also give specific instructions to a data controller on how an organisation is to treat the individual's data after death.

(g) Right to be forgotten

Individuals have the right to request for the deletion of their personal data that was either collected in the context of an information service or when he or she was a minor at the time of collection. Data controllers should also take reasonable measure to inform third parties to whom they have transferred that individual's personal data about the request for deletion of any links or copies of that information.

(h) Obligation to maintain secrecy of correspondence

Communications service providers, who provide online content, services or applications to the public, have an obligation to uphold the secrecy and confidentiality of correspondence between parties. This obligation extends to the automatic processing of the contents of communications for advertising, which is prohibited without express consent. However, this obligation does not apply to the processing of communications for malware detection purposes or to the actual conveyance of the correspondence.

(i) Storage of data outside EU jurisdictions

The Act deleted requirements that all data must be stored within the EU and not transferred to other jurisdictions. Hence, provided cross-border transfers comply with the GDPR, businesses can transfer data out of the EU and store it in non-EU countries.

EUROPEAN UNION

EU-US Privacy Shield pact faces second legal challenge

The EU-US Privacy Shield (***Privacy Shield***), a data-sharing agreement between the US and the EU, intends to provide stronger obligations on companies in the US to protect the personal data of EU citizens and stronger monitoring and enforcement by the United States Department of Commerce and Federal Trade Commission, such as through increased co-operation with the various European data protection authorities.

The Privacy Shield, approved in July 2016, replaced the previous data-sharing agreement (i.e., the Safe Harbour Framework) between the EU and US, which was established as an adequate protection of privacy on 26 July 2000 by the European Commission (***Commission***). This adequacy decision was declared invalid in October 2015 by the European Court of Justice (***ECJ***) (C-362/14), after the revelations of Edward Snowden about mass surveillance of online data in the US.

Generally, the Privacy Shield imposes stronger obligations for American companies to protect EU citizens' data and provides more enforcement powers for the US privacy regulators. This includes the creation of an Ombudsmen mechanism to resolve disputes of complaints

made by EU citizens about potentially intrusive data processing in the US.

However, despite these stronger obligations, several human rights organisations have expressed reservations about the Privacy Shield's ability to protect EU citizens from US government surveillance of data transferred under the Privacy Shield.

In this regard, the first challenge to the Privacy Shield was filed by an Irish privacy rights advocacy group, Digital Rights Ireland (***DRI***). DRI brought an action to annul the Commission's adequacy decision on the Privacy Shield and in the process, invalidate the Privacy Shield. One of the concerns raised by DRI was that under the Foreign Services Intelligence Act, the US government would still be able to access the content of electronic communications and this represents little change from the previous Safe Harbour arrangement.

A second, separate challenge to the Privacy Shield was brought by a French privacy rights advocacy group, La Quadrature du Net, along with a not-for profit internet service provider, French Data Network, and its Fédération FDN industry association. The parties challenged the effectiveness of the privacy Ombudsman in the US in dealing with disputes because it is not a sufficiently independent body to resolve these potential disputes.

Currently, both challenges are still ongoing, and a decision has yet to be issued.

UNITED KINDOM

The Information Commissioner's Office issues record fine to TalkTalk Telecom Group PLC for data breach

TalkTalk Telecom Group PLC (***TalkTalk***) is a broadband, TV, mobile and phone provider. On 5 October 2016, TalkTalk was fined £400,000 (S$702,364) as a monetary penalty under section 55A of the UK Data Protection Act 1998 (***UK DPA***) as it committed a serious breach of the seventh data protection principle (which provides that appropriate technical measures should be taken by organisations to prevent unauthorised access to personal data) by failing to keep their customers data secure.

Notably, the penalty imposed by the Information Commissioner's Office (***ICO***) is the highest monetary penalty issued to date and the ICO generally has the power to prescribe a penalty not exceeding £500,000 (S$877,702) for serious breaches of the UK DPA.

The data breach was a result of a cyber-attack on webpages operated by TalkTalk, which were inherited after TalkTalk acquired Tiscali in 2009. The cyber-attack used an SQL-injection technique to exploit vulnerabilities in the inherited webpages, which existed because the database software utilised by TalkTalk was outdated.

Not only did the hacker access a customer database containing the personal data of 156,959 customers including their names, addresses, dates of birth and contact details, the hacker was found to have also accessed the bank details of 15,656 customers.

The breach was particularly serious given the number of customers affected, particularly the number of people whose financial information was accessed unlawfully, and the consequences of such a breach, which includes the affected customers suffering distress due to the breach. Moreover, given the circumstances, the ICO held that this breach was a foreseeable one. TalkTalk reasonably ought to have known that: such a breach could occur; that Tiscali's webpage existed and had access to customer databases; SQL-injection attacks are common; and that their databases would fall victim to such attacks unless security measures were implemented.

However, TalkTalk failed to take reasonable steps to address these risks, which include: being aware of the inherited webpages and securing or removing them; updating the database software to later versions unaffected by the bug or fixing the bug using a method available three years before the attack; as well as doing proactive monitoring to discover system vulnerabilities despite having the financial ability and expertise to do so.

UK Government confirms implementation of GDPR in UK despite Brexit

On October 24 2016, appearing before the House of Commons Select Committee on Culture, Media and Sport, Karen Bradley MP, Secretary of State for Culture, Media and Sport, confirmed that the

United Kingdom will implement the EU GDPR by May 2018.

Elizabeth Denham, the UK Information Commissioner, officially welcomed the news and expressed that UK data protection laws have to remain equivalent with the EU to enable businesses in the UK to maintain and continue their dealings with the EU customers and businesses.

She further affirmed the ICO's commitment to help both the public and private sector prepare for compliance with the GDPR by May 2018. For example, on 14 March 2016, the ICO published a 12-step guide to assist organisations to comply with the GDPR and will be developing a revised timeline for priority areas that require guidance.

UK Information Commissioner publishes Code of Practice on privacy notices, transparency and control

The ICO has published a Code of Practice for UK organisations' communication of information about the collection, usage, disclosure and storage of personal data to individuals (***Code***).

Generally, the Code provides guidance on the drafting of clear and comprehensible privacy notices so that individuals will be aware of how their information is used by that organisation and the implications of such usage.

In addition, not only does the Code serve as a reminder to all UK data controllers of the legal requirement to provide privacy information to individuals, it also highlights that the GDPR imposes additional obligations that organisations processing personal data have to comply with, and further provides guidance on the drafting of privacy notices to comply with the GDPR.

Furthermore, considering that the first principle of data processing under the UK DPA is to process data fairly and lawfully, the Code sets out a list of best practices to ensure fair and transparent processing of data, including ways to give individuals choice and control about how their personal data will be used. Nevertheless, while transparency forms one important element of fair processing, other elements include:

(a) Using information in line with the reasonable expectations of users.

(b) Ensuring individuals know how their information is going to be used.

(c) Communicating such uses in the most appropriate manner.

The Code also sets out a suggestion for organisations to undertake a privacy impact assessment (***PIA***) to determine the privacy risks that individuals will likely face as a result of the organisation's data processing activities. This will then assist organisations in drafting appropriate privacy notices which inform users of the relevant privacy information at the relevant time.

In terms of the methods to provide the most essential privacy information immediately to all individuals, a suggestion as set out in the Code considers the use of layered notices and having more detailed explanations available as the most effective. The Code further suggests using "just-in-time" notices to collect the required information only at the point of the transaction when it is required and to notify users only at that time. Themethods set out above will also assist organisations in complying with the GDPR requirements.

In relation to how individuals' consent should be collected and recorded more effectively, the Code suggests that it should be done by:

(a) Clearly displaying the method of consent used.

(b) Using 'opt-in' consent as a good practice.

(c) When consent is collected for a range of purposes, providing information on how the information being collected will be used in each of those purposes and giving individuals simple ways to consent to each different purpose.

One suggestion to better manage an individual's consent is to utilise preference management tools which provide individuals a dashboard to control their personal privacy settings.

OTHERS

European data protection authorities issue guidelines on the GDPR

Since the passing of the GDPR in May 2016,

certain European data protection authorities (***DPA***), namely the Hungarian DPA, the UK's ICO and the Belgian DPA, have issued guidelines to assist organisations in preparing for compliance with the GDPR.

Both the Hungarian DPA and the UK ICO released similar 12-step guides, which provide guidance on how organisations can prepare to comply with the GDPR. The steps are as follows:

(a) **Raising Awareness**: Organisations should raise awareness internally about the changes in data protection laws and the likely implications of these changes for the organisation. Organisations should be ready to adapt its processes and strategies in light of the GDPR.

(b) **Review data processing activities**: Organisations should map their data protection activities, including what personal data the organisations collect, use, disclose and store. To this end, organisations may organise information audits.

(c) **Review privacy information communicated with the public**: Organisations should review their privacy policies and notices and plan the required changes to ensure compliance with the GDPR. In particular, organisations should note the need to ensure that privacy information communicated to the public is easily understandable and accessible, under the GDPR.

(d) **Rights of the data subject**: Organisations should ensure that their data processing methods respect the rights of the data subjects, which includes rights to have information erased, to have inaccuracies corrected and the right to data portability, where organisations have to provide data electronically and in a commonly used format.

(e) **Subject access requests**: Organisations should review their processes on how they respond to a data subject's access request in compliance with the GDPR requirements on, for example, response time or data retention periods.

(f) **Legal basis for processing personal data**: Organisations should examine their data processing activities and identify a legal basis for each data processing activity. These legal bases should also be documented.

(g) **Conditions of consent**: Organisations should review how they seek, obtain and record consent from their data subjects and ensure it meets the standards required by the GDPR.

(h) **Rights of minors**: Organisations should begin developing processes for age verification and obtaining parental consent in order to process personal data of minors in accordance with the GDPR.

(i) **Data breach notification**: Organisations should ensure that they develop processes to detect, monitor, investigate and report data breaches in light of personal data breach notification requirements as set out in the GDPR.

(j) **Data protection by design and data protection impact assessment**: Organisations that process personal data should consider how to implement data protection by design into their products and processes. Organisations should prepare to be able to conduct data protection impact assessments, particularly if the data processing might involve high risks to the rights and freedoms of individuals.

(k) **Appointment of a data protection officer**: Organisations should appoint a designated data protection officer or someone who will be responsible for data protection compliance, and consider how this person will function within the management structure of the organisation.

(l) **Competence of supervisory authorities**: Organisations that have international operations should determine which data protection supervisory authority regulates them.

Separately, the Belgian DPA has a thirteenth recommendation, which sets out that organisations are to review existing contracts with subcontractors and other data processors that the organisations may outsource work to, so as to ensure that the contents of these contracts also reflect the requirements of the GDPR.

The Drew & Napier Telecommunications, Media and Technology Team

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

Lim Chong Kin • Director and Head of TMT Practice Group

Chong Kin practices corporate and commercial law with strong emphasis in the specialist areas of TMT law and competition law. He regularly advises on regulatory, licensing, competition and market access issues. Apart from his expertise in drafting "first-of-its-kind" competition legislation, Chong Kin also has broad experience in corporate and commercial transactions including mergers and acquisitions. He is widely regarded as a pioneer in competition practice in Singapore and the leading practitioner on TMT and regulatory work. Chong Kin has won plaudits *for* '*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 2016***: 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**

Charmian Aw • Director

Charmian is a Director in Drew & Napier's TMT Practice Group. She is frequently involved in advising companies on a wide range of corporate, commercial and regulatory issues in Singapore. Charmian has also been actively involved in assisting companies on Singapore data protection law compliance, including reviewing contractual agreements and policies, conducting trainings and audits, as well as advising on enforcement issues relating to security, access, monitoring, and data breaches. Charmian is "recommended for corporate-related TMT and data privacy work" by ***The Asia Pacific Legal 500 2016***, and a Leading Lawyer in ***Who's Who Legal TMT 2016***. In 2015, she was listed as one of 40 bright legal minds and influential lawyers under the age of 40 by ***Asian Legal Business*** and ***Singapore Business Review*** respectively. Charmian is a Certified Information Privacy Professional (Europe) (CIPP/E) and Certified Information Privacy Professional (Asia) (CIPP/A).

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