DREW & NAPIER

LEGAL UPDATE

TELECOMS, MEDIA & TECHNOLOGY UPDATE

13 May 2016

PDPC ISSUES ADVISORY GUIDELINES ON ENFORCEMENT OF THE DATA PROTECTION PROVISIONS AND TAKES ACTION AGAINST 11 ORGANISATIONS FOR BREACHING DATA PROTECTION OBLIGATIONS

BACKGROUND

On 21 April 2016, the Personal Data Protection Commission ("**PDPC**") issued the Advisory Guidelines on Enforcement of the Data Protection Provisions ("**Enforcement Guidelines**") and announced that it had taken enforcement actions against 11 organisations for breaching their data protection obligations ("**Decisions**") under the Personal Data Protection Act (No. 26 of 2012) ("**PDPA**").

The Enforcement Guidelines provide guidance on the manner in which the PDPC will interpret the PDPA's provisions relating to enforcement of the Data Protection Provisions, and are not legally binding on the PDPC or any other party. The Enforcement Guidelines include and discuss:

- an overview of the enforcement framework;
- the PDPC's powers relating to alternative dispute resolution;
- the PDPC's approach to resolving complaints;
- the PDPC's powers in relation to the conduct of a review and procedures during reviews;
- the PDPC's powers of investigation in respect of contraventions of the PDPA;
- the PDPC's powers to issue directions to secure compliance and the payment of financial penalties;
- common issues relating to the PDPC's decisions and directions;
- reconsideration of decisions and directions; and
- appeals and rights of private action.

In respect of the Decisions, the 11 organisations that were found to have breached their data protection obligations under the PDPA are listed as follows:

- K Box Entertainment Group Pte. Ltd. ("**K Box**");
- Finantech Holdings Pte. Ltd. ("**Finantech**");
- The Institution of Engineers Singapore ("**IES**");
- Fei Fah Medical Manufacturing Pte. Ltd. ("**Fei Fah**");

- Challenger Technologies Limited ("**Challenger**");
- Xirlynx Innovations ("**Xirlynx**");
- Universal Travel Corporation Pte. Ltd. ("**UTC**");
- Full House Communications Pte. Ltd. ("**Full House**");
- Metro Pte. Ltd. ("**Metro**");
- Singapore Computer Society ("**SCS**"); and
- Yestuition Agency ("**Yestuition**").

In view of the same publication date of both the Decisions and the Enforcement Guidelines, these two sets of documents are timely in illustrating how the Enforcement Guidelines may be applied by the PDPC in taking enforcement action against private organisations.

We now discuss the Enforcement Guidelines and the Decisions in greater detail below.

PART 1: ADVISORY GUIDELINES ON ENFORCEMENT OF THE DATA PROTECTION PROVISIONS

At the outset, we note that our discussion on the Enforcement Guidelines will be limited to the recommendations and/or clarifications by the PDPC in respect of the enforcement framework under the PDPA.

As set forth under the Enforcement Guidelines, the PDPC will typically consider the following two main objectives when deciding whether, and how, to exercise its powers in the enforcement of the Data Protection Provisions:

- to facilitate the resolution of an individual's complaint in relation to a contravention or alleged contravention of any Data Protection Provisions by an organisation; and
- to ensure that private organisations comply with their obligations under the Data Protection Provisions.

With regard to the first objective, the PDPC will generally facilitate the resolution of the matters raised in the complaint between the individual and the organisation concerned instead of immediately exercising its powers of investigation under the PDPA. Where stronger action is warranted, the PDPC will have regard to the second objective through conducting reviews or investigations and accordingly, organisations will be directed to take certain actions based on the outcome of the reviews or investigations.

As the regulator responsible for administering and enforcing the PDPA, the PDPC has:

- powers relating to alternative dispute resolution under Section 27 of the PDPA;
- powers relating to reviews under Section 28 of the PDPA;
- powers relating to the issuance of directions to secure compliance and the payment of financial penalties under Section 29 of the PDPA; and
- powers relating to investigations under Section 50 of the PDPA.

Powers relating to alternative dispute resolution

Section 27 of the PDPA provides for the PDPC's powers relating to alternative dispute resolution for complaints by individuals.

The PDPC may:

- refer the matter to mediation with the consent of the complainant and the organisation under Section 27(1) of the PDPA; or
- where mediation is not appropriate, direct a complainant or an organisation or both to resolve the complaint in the way directed by the PDPC under Section 27(2) of the PDPA.

At the outset, the PDPC has clarified that its powers in relation to alternative dispute resolution do not include:

- deciding on disputes between a complainant and an organisation; or
- ordering an organisation to compensate a complainant who suffers a loss as a result of a contravention of any of the Data Protection Provisions by the organisation.

Instead, any individual who suffers loss or damage may commence civil proceedings in the courts against the organisation (please see discussion below).

Generally, in exercising its powers relating to alternative dispute resolution, the PDPC explained that it will first consider whether a complaint can be appropriately resolved by adopting some or all of the measures described in Section 5 of the Enforcement Guidelines. Section 5 of the Enforcement Guidelines sets out a list of measures that are recommended and/or may be taken by the PDPC, where appropriate, when seeking to facilitate the resolution of a complaint. For your convenience, we list them below for your reference:

- **Encouraging self-resolution**: individuals who are concerned with an organisation's conduct with respect to their personal data should first clarify the reasons for the organisation's conduct and seek an appropriate resolution of the matter. In addition, individuals who would like the organisation to stop using their personal data will have to give reasonable notice to the organisation to withdraw their consent as the PDPC cannot withdraw consent on behalf of the individuals.
- **Referring a complaint to an organisation**: the PDPC may refer a complaint to the organisation involved by forwarding a copy of the complaint and disclosing the complainant's identity to the organisation to better enable the organisation to address the complainant's concerns.
- **Facilitating resolution between the complainant and the organisation**: the PDPC will generally monitor the progress of discussions between the complainant and the organisation and may facilitate the resolution of the complaint, if necessary.
- **Referring a complaint to mediation**: the PDPC may refer the matter for mediation by a qualified mediator after obtaining both the complainant and the organisation's agreement that the matter is to be referred for mediation. At the time of writing, there are two mediation bodies that the PDPC may refer the complaint to: (i) the Consumer Association of Singapore; and (ii) the Singapore Mediation Centre. However, the complainant and the organisation have the liberty to utilise other mediation services or other alternative dispute resolution services to resolve the complaint.
- **Directing the parties to attempt to resolve the complaint**: the PDPC will only take such a measure after considering the manner in which the complaint may be more appropriately or more expeditiously resolved.

The factors that the PDPC may consider before taking any of the measures mentioned above are:

- whether, in the PDPC's view, the issues in the complaint relate solely to the complainant (or whether other individuals may be affected by the organisation's conduct in question);
- whether, in the PDPC's view, the issues may be more effectively resolved through discussion between the complainant and the organisation;
- whether the remedies or other corrective action preferred by the complainant are within the PDPC's powers;
- whether the remedies or other corrective action preferred by the complainant may voluntarily be provided by the organisation; or

- whether the organisation concerned has the required policies and processes in place to address complaints.

In the event that a complainant and the organisation are able to resolve the issues in a complaint and reach an agreement on the matter, the PDPC has clarified that it will consider the nature of the agreement reached in determining whether to take any further enforcement action. In particular, the PDPC may suspend, discontinue or refuse to conduct an investigation where the parties involved mutually agree to settle the matter.

Powers relating to reviews

Section 28 of the PDPA provides for the PDPC's powers relating to reviews. The procedures that the PDPC will adopt in a review are set out mainly under Part II of the Personal Data Protection (Enforcement) Regulations 2014 ("**Enforcement Regulations**").

Under Section 28(1), the PDPC may review the following three matters upon the application of an individual:

- an organisation's refusal to provide access to personal data requested by the applicant in a request under Section 21 of the PDPA, or a failure to provide such access within a reasonable time;

- the fee required by an organisation from the applicant in relation to the applicant's access request or a correction request; or

- an organisation's refusal to correct personal data requested by the applicant in a request under Section 22 of the PDPA, or a failure to make such a correction within a reasonable time.

In the Enforcement Guidelines, the PDPC has clarified that when it receives an application for a review, it will first consider whether the matter may be resolved in accordance with the guidance as set out under Section 5 of the Enforcement Guidelines as described herein. Generally, the PDPC will not proceed with the review if the matter is resolved.

In addition, the PDPC makes further recommendations for individuals with regard to the application for a review:

- **Clarify the reasons for an organisation's refusal to accede to the individual's request**: before applying for a review, the PDPC recommends that individuals should clarify with the organisation the reasons for the organisation's refusal to provide access to personal data or make a correction request.

- **Confirm with the organisation that it has received the request and make any necessary clarifications**: if an individual has not heard from an organisation within 30 days of his access request or correction request, the individual should confirm with the organisation that it has received his request and clarify with the organisation the time frame within which it will reply to the request.

- **Check the reasons for any delay**: when an organisation has specified the period within which it would respond to the individual's request, individuals should not apply for a review until the specified period has expired or exceeds what would be a reasonable period. Rather, individuals should check if there has been any delay, such that the organisation may require additional time in order to respond to the request.

- **Understand the nature of the fee that is levied**: individuals should be aware that where a fee is levied, it may exceed the cost of producing a copy of the document containing the personal data, as such a fee may include other incremental costs to reflect the time and effort required to respond to the request.

The Enforcement Regulations set out the list of information that is required to be included in an application for a review. The information required include, amongst other things, the reasons for making the application and a copy of all correspondence between the applicant and the

organisation relating to the access or correction request.

Upon the commencement of the review, the Enforcement Guidelines provide that the PDPC will serve a copy of the review application and any accompanying documents on the organisation concerned. Consequently, the PDPC will require the organisation to submit a response within 14 days of the date of the notice of review application, setting out the organisation's explanation to the issues raised in the complaint and any other information required by the PDPC.

In the event that the organisation:

- **submits a response**: the PDPC will generally invite the applicant to submit a reply within 14 days to the organisation's response; or

- **fails to submit a response**: the PDPC may proceed to commence an investigation into the conduct of the organisation (in which case the PDPC may suspend the review pending the outcome of the investigation) or proceed to make its decision based on the information and documents obtained by the PDPC during the review. Generally, the PDPC may commence investigations prior to or during a review and would only commence investigations after the completion of a review if there appears to be a significant non-compliance with Section 21 or 22 of the PDPA or there are other exceptional circumstances.

The PDPC may, at any stage of the review, seek further information or clarifications from the applicant or respondent. In other words, the PDPC may exercise its powers under regulations 4(3), 6(3) and 7(3) of the Enforcement Regulations to require the production of documents and information; and to require an applicant or a respondent to furnish a statutory declaration.

Under regulation 8 of the Enforcement Regulations, an applicant would be able to withdraw his/her review application by way of notice, before the PDPC gives notice of its decision. The PDPC has clarified under the Enforcement Guidelines that if such a withdrawal is done, the PDPC will terminate the review.

Upon the completion of the review, Section 28(2) of the PDPA provides that the PDPC may make directions. The PDPC is empowered through Section 30 of the PDPA to enforce its directions by registering them in the District Court.

PDPC's power of investigation

Section 50 of the PDPA provides for the PDPC's powers of investigation. In the Enforcement Guidelines, the PDPC has clarified that the following factors would be considered in deciding whether to commence an investigation:

- whether the organisation may have failed to comply, whether intentionally, negligently or for any other reason or cause, with all or a significant part of its obligations under the PDPA;

- whether the organisation's conduct indicates a systemic failure by the organisation to comply with the PDPA or to establish and maintain the necessary policies and procedures to ensure its compliance;

- the number of individuals who are, or may be, affected by the organisation's conduct;

- the impact of the organisation's conduct on the complainant or any individual who may be affected;

- whether the organisation had previously contravened the PDPA or may have failed to implement the necessary corrective measures to prevent the recurrence of a previous contravention;

- whether the complainant had previously approached the organisation to seek a resolution of the issues in the complainant but failed to reach a resolution;

- where the PDPC has sought to facilitate dispute resolution between the complainant and the organisation, whether the complainant and the organisation agreed to participate in the dispute resolution process, their conduct during the dispute resolution process and

the outcome of the dispute resolution process;

- where a review has been commenced by the PDPC, whether the organisation has complied with its obligations under the Enforcement Regulations in relation to a review, the organisation's conduct during the review and the outcome of the review;
- public interest; and
- any other factor that, in the PDPC's view, indicates that an investigation should or should not be commenced.

For the avoidance of doubt, the PDPC may commence an investigation notwithstanding that the complainant and the organisation have resolved the issues in the complaint or that the complaint is withdrawn by the complainant if there are other factors that indicate, in the PDPC's view, that an investigation should be conducted.

Where a complaint relates to a matter that may be reviewed under Section 28(1) of the PDPA, the PDPC will generally conduct a review instead of an investigation unless there appears to be significant non-compliance with Sections 21 and 22 of the PDPA or there are exceptional circumstances. Significant non-compliance may include systemic failures on the part of the organisation; or intentional non-compliance with Sections 21 and 22 of the PDPA.

In addition, the PDPC has clarified that it may, in certain circumstances, commence an investigation of its own motion based on the information that it has received.

Making a complaint to the PDPC

Complainants should note that as a complaint may result in formal action taken by the PDPC against an organisation, complainants may be required to give formal statements and appear before the PDPC in relation to the provision of these statements or other matters within their knowledge.

PDPC's powers when conducting investigations

The PDPC's powers when conducting investigations, which may be exercised by itself or its inspector, are set out in the Ninth Schedule to the PDPA. Broadly, these powers include:

- **the power to require production of documents and information**: paragraph 1 of the Ninth Schedule to the PDPA;
- **the power to enter premises without a warrant**: paragraph 2 of the Ninth Schedule to the PDPA; and
- **the power to enter premises with a warrant**: paragraph 3 of the Ninth Schedule to the PDPA.

The PDPC has clarified that it may use its powers of investigation to obtain from any organisation (including organisations that are not the subject of the PDPC's investigation) any information that the PDPC considers relates to any matter relevant to an investigation.

Under Section 50(3) of the PFDPA, the PDPC may suspend or discontinue an investigation.

Public communications

The PDPC has noted in the Enforcement Guidelines that organisations, before the issuance of any media releases or public disclosure of matters related to the alleged breach, are advised to consider whether the content would hinder the ongoing investigations and to also provide the PDPC with a copy of the materials prior to any media releases or public disclosure of matters.

Direction to secure compliance

The PDPC's power to issue directions to secure an organisation's compliance with the Data Protection Provisions is set out in Section 29 of the PDPA. Directions include, amongst other things, financial penalties.

In considering whether to direct an organisation to pay a financial penalty, the PDPC noted in the Enforcement Guidelines that, while it would objectively determine each case on its own merits and circumstances, the following factors would be considered:

- the seriousness and impact of the organisation's breach;
- the immediacy and effectiveness of corrective actions that the organisation took to address the breach;
- whether the organisation had acted deliberately, wilfully or if the organisation had known or ought to have known of the risk of a serious contravention and failed to take reasonable steps to prevent it; and
- the seriousness of the breach of the Data Protection Provisions and how a reasonable organisation should behave in that particular situation.

In the determination of the quantum of the financial penalty, the PDPC further provided a non-exhaustive list of some aggravating and mitigating factors that it may take into consideration.

The factors which the PDPC may consider to be aggravating factors are:

- the organisation's failure to actively take reasonable steps to resolve the matter with the individual in an effective and prompt manner;
- intentional, repeated and/or ongoing breaches of the Data Protection Provisions by the organisation;
- obstructing the PDPC during the course of its investigations;
- failing to comply with a previous warning or direction from the PDPC; and
- for organisations in the business of handling large volume of sensitive personal data which may cause exceptional damage, injury or hardship to a person if disclosed, the failure to put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data.

The factors which the PDPC may consider to be mitigating factors are:

- the organisation's active and prompt resolution of the matter with the individual;
- the organisation taking reasonable steps to prevent or reduce the harm of a breach;
- the organisation engaging the individual in a meaningful manner and has voluntarily offered a remedy to the individual, and that individual has accepted the remedy;
- the organisation taking immediate steps to notify affected individuals of the breach and reduce the damage caused by a breach; and
- the organisation voluntarily notifying the PDPC of the personal data breach as soon as it learned of the breach, and co-operating with the PDPC in its investigations.

The PDPC's power to publish decisions and directions

Regulations 17, 18 and 19 of the Enforcement Regulations give the PDPC powers to publish decisions and directions.

In the Enforcement Guidelines, the PDPC will generally publish a decision relating to an organisation that is found to have contravened the Data Protection Provisions for reasons of transparency and to allow other organisations to be aware of how the PDPC has applied the PDPA in specific cases and adopt preventive measures to avoid similar situations.

For the avoidance of doubt, non-publication of a decision does not affect the legal validity or effect of the decision.

Further, while it will generally not publish a review decision (as such decisions do not always amount to a finding that an organisation has contravened the Data Protection Provisions), the PDPC has clarified that it may publish a review decision if it is of the view that the review decisions:

- will be of general interest to the public; or

- will provide guidance to individuals and organisations in relation to their respective rights and obligations under the PDPA.

Reconsideration

Section 31 of the PDPA provides that an organisation or individual aggrieved by a decision or direction of the PDPC may apply to the PDPC to reconsider its decision or direction. An application for reconsideration shall be made within 28 days from the issuance of the decision or direction. The reconsideration procedure is set out mainly in Part III of the Enforcement Regulations.

Broadly, the reconsideration procedure will involve the following steps:

- **Upon receiving a reconsideration application**: the PDPC will serve on the respondent a copy of the application, any accompanying documents that have been provided by the applicant, and a notice requiring a written response from the respondent if the respondent wishes to submit an explanation or reply to the matters raised in the application.

- **If the respondent submits a response**: where appropriate, the PDPC may serve a copy of the response and any accompanying documents to the applicant; and invite the applicant to submit a response to the respondent's reply.

- **If the respondent fails to submit a response**: the PDPC will make its decision based on the information and documents obtained by the PDPC.

The PDPC has clarified that the typical time frame that an organisation or an applicant may submit a response will generally be within 14 days.

The PDPC has further clarified that it will generally allow an applicant to withdraw a reconsideration application unless the PDPC considers that there is sufficient reason, based on the information and documents provided to the PDPC prior to the applicant's request to withdraw his application, for the PDPC to reconsider the contested decision.

Appeals

The right to appeal from a direction or decision made by the PDPC is set forth under Section 34 of the PDPA and the appeal will generally be heard by a Data Protection Appeal Committee (Section 33 of the PDPA). Subsequently, the right to appeal against, or with respect to a decision or direction made by the Data Protection Appeal Committee, may be made to the High Court under Section 35. A decision of the High Court may be further appealed to the Court of Appeal following the Rules of Court.

Right to appeal in relation to reconsideration applications

Section 34(2) of the PDPA provides that where an application for reconsideration has been made under Section 31 of the PDPA, every appeal in respect of the same decision or direction shall be deemed to be withdrawn.

In this regard, the PDPC has clarified that an appellant whose appeal is deemed to be withdrawn may make an application for reconsideration to the PDPC, and the PDPC shall consider such applications concurrently with other applications for reconsideration in respect of the same matter.

Alternatively, the appellant may await the outcome of the PDPC's reconsideration of its decision or direction, and consider whether to make an appeal against the PDPC's decision upon reconsideration.

Right to appeal to the High Court

Section 35(1) provides that an appeal against, or with respect to the decision made by the Data Protection Appeal Committee to the High Court can only be made on two grounds:

- on a point of law; or

- as to the amount of a financial penalty.

In hearing the appeal, under Section 35(3) of the PDPA, the High Court may:

- confirm, modify or reverse the decision or direction of the Data Protection Appeal Committee; and

- make such further or other order, including (without limitation) orders as to costs.

Rights of Private Action

Generally, as the PDPC is not empowered to grant relief to a complainant, persons who suffer loss or damage as a result of a contravention of the PDPA may commence civil proceedings against an organisation.

In commencing civil proceedings for relief under Section 32(1), the PDPC has noted that a party is required to comply with Rules of Court, Order 105, Rule 12, which provides that:

- an individual is required to serve a copy of the writ or originating summons to the PDPC not later than seven days after service of the writ or originating summons on the defendant; and

- an individual who is granted a judgment or order by a court under section 32(1) is required to transmit a copy of the judgment or order to the PDPC within three days after the date of the judgment or order.

Following Section 32(3), a court hearing an action under Section 32(1) of the PDPA may grant any or all of the following relief:

- an injunction or declaration;

- damages; or

- such other relief as the court thinks fit.

PART 2: PDPC TAKES ACTION AGAINST 11 ORGANISATIONS FOR BREACHING DATA PROTECTION OBLIGATIONS

The PDPC has taken enforcement actions against 11 organisations for breaching their data protection obligations. Accordingly, five organisations were issued directions (four of which include financial penalties), while six others were issued warnings. As discussed above, Section 29 of the PDPA provides, among other things, that if the PDPC is satisfied that an organisation is not complying with the Data Protection Provisions under the PDPA, the PDPC may give the organisation such directions as the PDPC thinks fit in the circumstances to ensure compliance with the Data Protection Provisions. Such directions may include the imposition of financial penalties on organisations.

The following paragraphs aim to discuss the material facts in detail, and in particular, highlight the PDPC's assessment for each decision.

K Box and Finantech

Material facts:
In September 2014, a list containing the personal data of 317,000 K Box members was found to have been leaked and uploaded on http://pastebin.com, a website which allows members of the public to post and share text online publicly. The data included names, contact numbers and residential addresses.

PDPC's findings:
The PDPC found that K Box breached Section 24 of the PDPA as it failed to make reasonable security arrangements to protect the members' personal data:

(i) K Box did not ensure that security patches were updated and/or to conduct audits of the security of its database and system, which allowed external parties to install malware to gain easy access into its system that held its customers' personal data;

(ii) K Box failed to enforce its password policy by permitting the use of weak passwords;

(iii) K Box did not disable unused accounts;

(iv) Emails containing large volume of personal data were sent without any password-protection or encryption; and

(v) K Box failed to ensure that Finantech, the third party IT vendor engaged by K Box to develop K Box's Content Management System, had undertaken adequate measures to protect members' personal data.

In addition, K Box has not complied with Sections 11 and 12 of the PDPA as it did not appoint a Data Protection Officer ("**DPO**") to develop and implement data protection policies.

The PDPC also determined that Finantech is a data intermediary of K Box as K Box employees had restricted access to the information of members, and K Box relied on Finantech to extract and send them members' personal data. As the data intermediary, Finantech had breached Section 24 of the PDPA as it did not patch security vulnerabilities in K Box's IT system, and the administrator account had a weak password which made the administrator account vulnerable to hacks.

In deciding the type of enforcement action to be taken against K Box, the PDPC took into consideration the following six factors, that:

(i) the **remedial actions undertaken by K Box were fair and prompt** when they discovered the data breach in September 2014;

(ii) most of the remedial actions were taken either in September or November 2014;

(iii) the PDPC **found no evidence to suggest that the data breach was due to actions taken by K Box staff**;

(iv) **a fairly large amount of personal data** (approximately "317,000" K Box members or more) **had been disclosed as a result of the lack of security**. The personal data comprising their full names, contact numbers, email addresses, residential addresses, contact numbers, gender, profession, date of birth, and member number were sensitive data because it could have led to identify theft;

(v) **K Box (as the primary data owner) had disregarded its obligations under the PDPA**. K Box had ample opportunities to put in place reasonable security measures from 2 January 2013 to 2 July 2014 but it did not do so. K Box had also failed to appoint a DPO or put in place privacy policies as late as April 2015. K Box also did not implement data protection terms and conditions in its contract with Finantech, and did not instruct Finantech (as the main data processor of K Box members' personal data) to protect personal data; and

(vi) **K Box was not forthcoming in providing information during the investigation**. They had only provided bare facts in their responses during the investigations, which did not facilitate the PDPC's investigations.

Accordingly, the PDPC decided to issue the following directions to K Box:

(i) pay a financial penalty of $50,000 within 30 days from the date of the PDPC's direction; and

(ii) appoint a DPO within 30 days from the date of the PDPC's direction (if K Box has not already done so).

In deciding the type of enforcement action to be taken against Finantech, the PDPC took into consideration the following five factors, that:

(i) the **remedial actions undertaken by Finantech were fair and prompt** when they discovered the data breach in September 2014;

(ii) Most of the remedial actions were taken either in September or November 2014;

(iii) **A fairly large amount of personal data had been put at risk as a result of the lack of security;**

(iv) **Finantech (as the data intermediary) had disregarded its obligations under the PDPA.** Finantech had ample opportunities to put in place reasonable security measures from 2 January 2013 to 2 July 2014 but it did not do so. There was no evidence to show that Finantech had advised K Box on the reasonable security measures that it ought to implement to protect personal data held by the system; and

(v) Finantech **appeared not to be forthcoming in providing information during the investigation**. Finantech's

responses to the Notices to Require Production of Documents and Information under the Ninth Schedule of the PDPA were only provided almost seven months after the NTPs were first issued in October 2014. This delayed the investigation process.

Accordingly, the PDPC directed Finantech to pay a financial penalty of $10,000 within 30 days from the date of the PDPC's direction.

IES

Material facts:
The PDPC was informed that the personal data of users of the IES website had been posted on http://pastebin.com. More than 4,000 individuals' contact numbers, member IDs and passwords were released.

PDPC's findings:
The PDPC found that the member IDs and passwords released constituted personal data as any member of the public could have used this information to log into the accounts of IES members and access personal data relating to the members stored on the IES website. This personal data was under the control of IES as the two IT vendors engaged, ReadySpace and Forecepts, did not own or administer the website.

IES had failed to implement reasonable security arrangements (Section 24 of the PDPA) despite the hosting of the website's server in a secure site and in a dedicated server; the performance of software updates; and the authorisation of only four individuals and Forecepts to extract the list of user IDs and passwords. It was apparent to the PDPC that:

(i) the website had not provided for the encrypted storage of member passwords;

(ii) no audit had been conducted on ReadySpace's hosting services and/or the security of the website prior to the data leak;

(iii) IES had not conducted any penetration testing on the website and was not aware of penetration testing software; and

(iv) while IES represented that it had made phone calls to ReadySpace and Forecepts to inform them about the PDPA, there was no indication that IES had otherwise given instructions to its vendors to make security arrangements so as to ensure that personal data stored in the website would be protected in compliance with IES's obligations under the PDPA.

The PDPC further found that while IES may have had firewall and anti-virus software in place prior to the data leak, IES had made insufficient effort to inquire into and/or ensure the security of personal data stored on the website, thus, resulting in numerous security vulnerabilities.

In deciding the type of enforcement action to be taken against IES, the PDPC took into consideration the following four factors, that:

(i) **IES was cooperative and forthcoming** throughout the PDPC's investigation;

(ii) **IES promptly took measures following its discovery of the data leak** (e.g., disabling the members' portal on the website; changing the passwords for all IES members' accounts, and resetting of the passwords for its administrator accounts in the member portal; sending an email notification informing the members about the hacking activity; and removing the telephone numbers and addresses of IES members previously stored on the database on the website);

(iii) **IES took additional security measures following the data leak** (e.g., instructed Forecepts to conduct of a security audit of the website and to patch up any vulnerabilities detected; conduct a monthly audit on the website upon completion of the security hardening process; installation of a new intrusion detection system; installation of Secure Sockets Layer certification in the website's server); and

(iv) **any vulnerabilities identified have been patched** by Forecepts.

Accordingly, the PDPC decided to issue the following directions to IES:

(i) IES shall within 60 days from the date of the PDPC's direction:

- conduct a further vulnerability scan of the Site; and
- patch all vulnerabilities identified by such scan;

(ii) IES shall, in addition, submit to the PDPC by no later than 14 days after the conduct of the abovementioned vulnerability scan, a written update providing details on:

- the results of the vulnerability scan; and
- the measures that were taken by IES to patch all vulnerabilities identified by the vulnerability scan; and

(iii) IES shall pay a financial penalty of S$10,000.00 within 30 days from the date of the PDPC's direction.

Fei Fah

Material facts:
Fei Fah had the personal data of its customers, which included the customers' usernames, passwords, contact numbers and email addresses, posted on http://pastebin.com. More than 900 individuals were affected. After being alerted of the leak via PDPC's notice dated 1 October 2014, Fei Fah sent email notifications to all affected individuals informing them of the data leak. In addition, Fei Fah took steps to instruct its Hong Kong-based data intermediary IT Factory to remove all data collecting functions from its website. However, as these instructions failed to be carried out by IT Factory, new data continued to be collected via the website until 30 July 2015, when the PDPC alerted Fei Fah to the fact that its website still retained its data collecting functions.

PDPC's findings:
The PDPC found that the information leaked constituted personal data despite the encoded passwords, as the passwords were encoded with a commonly used crytographic hash function, which could be deciphered easily. The usernames and decoded passwords could be used to access the personal details of the members. Additionally, Fei Fah possessed and/or controlled the personal data of its customers.

Fei Fah had failed to implement reasonable security arrangements (Section 24 of the PDPA) in respect of personal data relating to users of its website as it:

(i) was unable to provide any information about the security arrangements that it had put in place to protect its website or the server where the database of personal data collected was hosted;

(ii) was unable to provide details nor evidence of the firewalls within the administration control panel;

(iii) made little effort to inquire into and/or ensure the security of personal data stored on the website; and

(iv) appeared to have little knowledge as to whether there were security measures implemented on its website or the server where the database of personal data collected was hosted.

In deciding the type of enforcement action to be taken against Fei Fah, the PDPC took into consideration the following two factors, that:

(i) Fei Fah had been **neither cooperative nor forthcoming in its responses** to the Notices to Require Production of Documents and Information under the Ninth Schedule to the PDPA ("**NTPs**") issued by the PDPC as part of its investigations. The PDPC noted that Fei Fah had **provided incomplete responses** to the first and second NTPs and initially ignored the third NTP issued by the PDPC. Fei Fah also **took between three weeks to a month to respond** to each NTP; and

(ii) although Fei Fah took steps to instruct its Hong Kong-based data intermediary IT Factory to implement remedial actions to address the data leak following its discovery on 1 October 2014, it **did not**

ensure that its instructions were carried out by its data intermediary. IT Factory only implemented remedial actions to address the data leak on 30 July 2015, more than ten months after Fei Fah first discovered the data leak. This undue delay in implementing the remedial actions suggests a continuing indifference by Fei Fah to make reasonable security arrangements.

Accordingly, the PDPC decided to issue the following directions to Fei Fah:

(i) Fei Fah shall within 120 days from the date of the PDPC's direction:

- implement a new website to replace the Site;
- conduct a web application vulnerability scan of the new website; and
- patch all vulnerabilities identified by such scan;

(ii) Fei Fah shall, in addition, submit to the PDPC by no later than 14 days after patching all vulnerabilities identified by the abovementioned vulnerability scan, a written update providing details on:

- the results of the vulnerability scan; and
- the measures that were taken by Fei Fah to patch all vulnerabilities identified by the vulnerability scan; and

(iii) Fei Fah shall pay a financial penalty of S$5,000.00 within 30 days from the date of the PDPC's direction.

Challenger and Xirlynx

Material facts:
A third party IT vendor, Xirlynx, was engaged by Challenger to manage and execute its email campaigns. Xirlynx erroneously sent emails containing the personal data of members of Challenger's ValueClub programme to other members of the programme, who were the wrong recipients. Nevertheless, the personal data disclosed was limited to the member's name, accumulated points and expiry date. The risk of the points being misused because of this disclosure was low.

PDPC's findings:
The PDPC found that Xirlynx was a data intermediary of Challenger as Xirlynx had processed personal data on behalf of Challenger and Challenger clearly relied on Xirlynx to process its members' personal data. As such, Challenger has the same obligations under the PDPA in respect of Xirlynx's processing of personal data.

Xirlynx was in breach of Section 24 of the PDPA as it has failed to make reasonable security arrangements:

(i) Xirlynx had caused an Excel column containing a list of Valueclub members' names, and an Excel column containing a list of the members' email addresses, to be mismatched. The occurrence of the data breach was prima facie an indication that Xirlynx had not fulfilled its responsibility to ensure that processing of the member database was done in the correct manner.

(ii) Xirlynx did not conduct sample proof-reading, which was a reasonable security arrangement given the nature of the services it provided. Sample proof-reading would likely have either averted the data leak or greatly reduced the number of individuals affected.

Correspondingly, the PDPC found that Challenger was also in breach of Section 24 of the PDPA. Challenger had neglected to exercise control over Xirlynx's workflow in the processing of Challenger's ValueClub membership database and have left it to Xirlynx to implement measures required to protect the personal data Xirlynx processed and, until the data breach occurred, had not considered what requirements it would want to implement to ensure that the personal data was appropriately protected.

In deciding the type of enforcement action to be taken against Challenger and Xirlynx, the PDPC took into consideration the following four factors, that:

(i) the **personal data leaked was limited** (i.e., the names, membership expiry dates and accumulated ValueClub programme points) and are not of a sensitive nature;

(ii) the **personal data leaked could not be used by the individuals who had received them to profiteer or benefit from them**, and was unlikely to lead to any harm or loss to the individuals concerned;

(iii) both Challenger and Xirlynx had been **cooperative** with the PDPC and were **forthcoming in their responses to the PDPC** during the investigation; and

(iv) Challenger had **taken several proactive steps to remedy the breach** (e.g., engaging a new IT vendor and hiring the services of a data protection consultant).

Accordingly, the PDPC decided to issue a warning to both Challenger and Xirlynx.

UTC

Material facts:

On request by four of its customers to furnish formal documentation confirming the cancellation of their transit flight to Sofia, UTC sent by email to these customers the formal confirmation together with the passenger list The passenger list that was sent contained the personal data (e.g., name, nationality, date of birth, passport number, passport expiry date and passenger name record) of all 37 of the customers who had signed up for the same tour. These details were not masked or redacted when it was sent by UTC.

PDPC's findings:

The PDPC found that UTC had breached Section 13 of the PDPA as it had not sought for or obtained any of the 37 passenger's consent. No such deemed consent can be imputed on the facts. Additionally, UTC had breached Section 20 of the PDPA as it had not informed of the purposes for which it was disclosing the passengers' personal data. These purposes did not include the purpose of allowing another passenger to process his/her insurance claim.

The exception to the requirement of consent is provided for in paragraph 1(a) of the Fourth Schedule of the PDPA. Paragraph 1(a) of the Fourth Schedule provides that consent would not be required if "*the disclosure is necessary for any purpose which is clearly in the interests of the individual [and] if consent for its disclosure cannot be obtained in a timely way*". The PDPC found that the exception did not apply for the following reasons:

(i) "interests of the individual" refers to the interests of the data subject and disclosing the personal data of other passengers to a fellow passenger for the purpose of enabling that passenger to make a claim against his travel insurance policy for himself cannot be said to be in the interest of any one or all of the other passengers;

(ii) it was not obvious to the PDPC that in order to make an insurance claim, details of all other affected passengers had to be disclosed; and

(iii) there is nothing to suggest that consent for disclosure could not be secured from the passengers in the list in a timely manner, or that there was urgency in the matter which warranted the consent from the other passengers to be dispensed with.

As such, it was found that UTC was in breach of Sections 13 and 20 of the PDPA. In addition, since the purposes could not be purposes that a reasonable person would consider appropriate in the circumstances, UTC was also in breach of Section 18 of the PDPA.

Furthermore, given that UTC had not put in place data protection policies to ensure compliance with the PDPA at the material time when the data breach transpired, UTC was in breach of Section 12(a) of the PDPA.

In deciding the type of enforcement action to be taken against UTC, the PDPC took into consideration the following five factors, that:

(i) the **disclosures were made to a limited number of persons** and **to their personal email addresses**;

(ii) the **personal data that was disclosed was in relation to limited individuals**;

(iii) the **disclosures were not due to a systemic issue that could result in further disclosures** to be made or further harm to be caused;

(iv) the **disclosures appear to be caused by the lack of awareness** on UTC's employees' part of data protection obligations; and

(v) the **disclosures were bona fide mistakes** made by UTC's employees who were seeking to assist the passengers with their insurance claims, and **not one where there was a wilful disregard for the provisions in the PDPA**.

Accordingly, the PDPC decided to issue the following directions to UTC:

(i) to put in place within 3 months a data protection policy and internal guidelines to comply with the provisions of the PDPA and, in particular, to prevent future recurrences of the breaches that has occurred in this matter;

(ii) to inform within 2 weeks the individuals who received the passenger list not to disclose the list to other third parties;

(iii) for all employees of the UTC handling personal data to attend a training course on the obligations under the PDPA and the UTC's data protection policies within 6 months from the date of this decision; and

(iv) to inform the PDPC of the completion of each of the above within 1 week.

Full House

Material facts:
In obtaining information for registration for a lucky draw organised by Full House at a furniture fair, Full House enabled the auto-fill function for the computerised forms on the laptops at the redemption counter. The personal data displayed in the drop-down boxes included the individual's name, identity card number, contact number and email address.

PDPC's findings:

The PDPC found that Full House was in breach of their obligation under Section 24 of the PDPA as it had enabled the auto-fill function, which permitted a user to have access to the personal data of other individual(s) that was stored on the laptops. Even if the information found within a particular drop-down box were not listed in chronological order, the PDPC noted that the information by themselves or collectively, amounted to personal data. Furthermore, there are certain instances where a link could be drawn between the information across various drop boxes (e.g., an email address containing part of the individual's name could be linked to the full name of the individual and hence identify the individual). The presence of staff around the laptops made no difference in preventing an individual from accessing the personal data stored on the system, though it helped to ensure that individuals do not take photographs of the laptop screens. As such, the PDPC found that Full House breached Section 24 of the PDPA.

In deciding the type of enforcement action to be taken against Full House, the PDPC took into consideration the following two factors:

(i) the **impact of the breach is limited**, since, in the given circumstances, a user would have had limited time to observe and collect personal data in the drop-down boxes; and

(ii) Full House **took action shortly after the complaint was made** to stop the use of the drop-down boxes and to arrange for its staff to fill in the forms themselves.

Accordingly, the PDPC decided to issue a warning against Full House.

Metro

Material facts:
In March 2015, it was discovered that the names, personal email addresses, NRIC numbers, personal mobile phone numbers, dates of birth and Facebook user IDs of 445 of Metro's customers were disclosed on http://siph9n.net ("**the Siph0n**

website"). Investigations by PDPC revealed that the data leak was linked to the hacking of Metro's corporate website in 2014. Metro's IT support partners, Grey Digital and Vodien Internet Solutions Pte Ltd, carried out investigations, but were unable to determine the cause of the hacking incidents. Metro has since taken steps to improve on its web security following the hacking incidents. Upon notification of the complaint in 2015, Metro instructed Grey Digital to remove any user information from the server of the hacked website and also engaged KPMG Singapore to carry out an assessment and audit of the security of its systems.

PDPC's findings:
The PDPC found that Metro had failed to implement reasonable security arrangements and has breached Section 24 of the PDPA. Despite Metro and/or Grey Digital act of taking steps to improve the security of Metro's website and system following the hacking incidents, the KPMG report found, amongst other things, that there was at least one significant issue which was indicative of a failure to implement reasonable security arrangements – the SQL injection vulnerability. The SQL injection vulnerability is a common and well-documented form of vulnerability that ought to have been reasonably anticipated, identified and rectified by Metro at an early stage.

The PDPC also noted that since Metro had collected and stored the personal data from its users or customers in the web servers and web applications, any vulnerability in these platforms would pose a real risk to the security of the personal data that was collected. The fact that there were a number of issues with the security of Metro's IT system, particularly, the SQL injection vulnerability, indicated to the PDPC that web security was lacking. As such, the PDPC found that Metro was in breach of Section 24 of the PDPA.

In deciding the type of enforcement action to be taken against Metro, the PDPC took into consideration the following two factors, that:

(i) Metro had **taken action to strengthen the security of its website** (e.g., engaging KPMG to undertake an internal IT security audit and assessment after learning of the posting of its customer's personal data on the Siph0n website). However, the PDPC also noted that Metro's actions (after the hacking incidents in February 2014) did not enable it to detect and address at least one significant security lapse until several months later (i.e., after May 2015); and

(ii) the data leak that gave rise to the complaint took place before July 2014 and there is **no evidence that there has been a data breach to date**, notwithstanding Metro's failure to make reasonable security arrangements.

Accordingly, the PDPC decided to issue a warning against Metro.

SCS

Material facts:
Prior to an event jointly organised and conducted by SCS and the Infocomm Development Authority of Singapore, an employee of SCS sent out event confirmation emails to 214 registrants of the event, of which a copy of the registration list (with information such as the registrant's full names, NRIC numbers, contact numbers, email addresses, organisation and designation information) for the event was attached. Upon being notified of the disclosure of the registration list by some registrants, SCS promptly recalled the email and sent an official email apology to the registrants who had raised concerns over the incident.

PDPC's findings:
The primary concern was whether SCS had implemented reasonable security arrangements (Section 24 of the PDPA) to prevent unauthorised disclosure of information. Even though SCS having to obtain consent from the registrants (Section 13 of the PDPA) appears to be a secondary concern, the PDPC noted that this case would be more properly considered from the perspective of whether SCS had implemented reasonable security arrangements. Nevertheless, moving forward, the PDPC has clarified that other cases may require an examination of both Sections 13 and 24 of the PDPA.

The PDPC found that SCS was in breach of Section 24 of the PDPA as the poor data handling practices (e.g., the registration list was not protected by a password) by SCS did not include

sufficient security arrangements to the standard required under Section 24 of the PDPA.

In deciding the type of enforcement action to be taken against SCS, the PDPC took into consideration the following three factors, that:

(i) a **significant part of the personal data disclosed** was **business contact information**;

(ii) SCS **took prompt action to recall the emails** even though this action did not result in a complete recall of all the emails; and

(iii) SCS **informed the PDPC of the data breach voluntarily** and was **cooperative** during the investigation.

Accordingly, the PDPC decided to issue a warning against SCS.

Yestuition

Material facts:
Yestuition, which has a web portal that allows customers to view its tutors' profile and photos, published images of its tutors that were named using the tutors' respective NRIC numbers. These images were made publicly discoverable and accessible via a directory listing on one of the pages of Yestuition's website, and approximately 30 individuals were in the directory listing.

PDPC's findings:
The PDPC found that Yestuition was in breach of Section 13 of the PDPA as it did not obtain the tutor's consent for the disclosure of their NRIC numbers and images to members of the public. Such a disclosure also ran counter to the terms of Yestuition's Privacy Policy.

In deciding the type of enforcement action to be taken against Yestuition, the PDPC took into consideration the following two factors, that:

(i) Yestuition **took proactive steps to restrict access to the page once it was made aware of the issue**, and **changed its practice** of using its tutors' NRIC numbers as the file names of their images; and

(ii) Yestuition had been **cooperative with the PDPC** and **forthcoming in its responses** to the PDPC during the investigation.

Consequently, the PDPC decided to issue a warning against Yestuition.

Xiaomi Singapore Pte. Ltd ("Xiaomi")

In the PDPC's media release entitled "PDPC takes action against 11 organisations for breaching Data Protection obligations", the PDPC has stated that it may accept an undertaking that commits an organisation to a particular course of action to achieve the desired level of compliance with the PDPA. For instance, an undertaking may be considered when an organisation is able to improve its compliance with the PDPA promptly without requiring the PDPC to conduct a full investigation.

And it is for illustration purposes that the PDPC cited the case of Xiaomi. In response to the PDPC raising concerns about its practice of signing users up to its cloud messaging services by default, Xiaomi provided an undertaking to the PDPC to improve its compliance in accordance with the PDPA.

CONCLUDING REMARKS

Since the PDPA came into full force in July 2014, the PDPC has received a total of 667 complaints, 92% of which were resolved through investigation and facilitation between the respective organisations and individuals.

Notably, the Chairman of the PDPC stated that the enforcement actions that were taken against the 11 organisations were not to deter the use of personal data for business competitiveness. The PDPC continues to recognise the indispensable nature of data, especially when data is essential for innovation in today's economy. As such, both the organisation and its data intermediaries (such as IT vendors that provide systems and data management solutions to businesses) would be expected to: (i) use data responsibly; (ii) take appropriate actions to protect data; (iii) exercise due care; and (iv) implement adequate data security measures.

Given that the PDPA has already been in full force for almost two years, organisations should by now be aware of the PDPC's approach against breaches of the Data Protection Provisions and in particular, take the Decisions as learning points.

Finally, we would highlight that the Enforcement Guidelines should be read in conjunction with the other Advisory Guidelines issued by the PDPC from time to time.

If you have any questions or comments on this article, please contact:

Lim Chong Kin
Director
Head, Telecommunications, Media & Technology
T: +65 6531 4110
E: chongkin.lim@drewnapier.com

Charmian Aw
Director
T: +65 6531 2235
E: charmian.aw@drewnapier.com

Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906