PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

Media Release

21 April 2016 | For Immediate Release

PDPC takes action against 11 organisations for breaching Data Protection obligations

The Personal Data Protection Commission (PDPC) has taken enforcement actions against several organisations for breaching their data protection obligations under the Personal Data Protection Act (PDPA). Five organisations were issued directions (four of which included financial penalties), while six others were issued warnings.

The PDPC considered the severity of non-compliance of the cases in determining the type of enforcement actions taken. Some of the factors include:

a) Whether the organisation had taken reasonable measures to prevent the data breach;
b) Whether the organisation took steps to identify weaknesses of its system and effectiveness of any remedial actions taken thereafter;
c) Whether the organisation had data protection policies and processes in place;
d) The number of individuals who were affected;
e) The duration of time taken to remedy the breach once it was known;
f) The type of personal data involved;
g) The manner in which the organisation responded to the breach; and
h) The circumstances of the breach.

The PDPC imposed a financial penalty of $50,000 on K Box Entertainment Group Pte Ltd (K Box), a karaoke chain, for not putting in place sufficient security measures to protect the personal data of 317,000 members, for inadequate data protection policies and the absence of a Data Protection Officer (DPO).

The PDPC imposed a financial penalty of $10,000 on Finantech Holdings Pte Ltd, the IT vendor in charge of K Box's content management system (as K Box's data intermediary[1]).

For failing to put in place adequate security measures to protect personal data in its possession that affected 4,000 members, the PDPC imposed a financial penalty of $10,000 on the Institution of Engineers, Singapore. For a similar breach that affected more than 900 customers, a financial penalty of $5,000 was imposed on Fei Fah Medical Manufacturing Pte Ltd, a health supplements supplier.

[1] The PDPA defines a Data Intermediary as "an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation".

For unauthorised disclosure of 37 customers' personal data to four individuals, the PDPC issued directions to Universal Travel Corporation Pte Ltd, a tour agency, to enhance its personal data protection policies.

The PDPC also issued warnings to six organisations for lapses in handling personal data: Challenger Technologies Ltd, an IT retailer, as well as its IT vendor, Xirlynx Innovations; Full House Communications Pte Ltd, a consumer home show organiser; Metro Pte Ltd, a retailer; Singapore Computer Society, an infocomm and digital media professional society; and YesTuition Agency, a tuition agency.

The PDPC may also accept an undertaking that commits the organisation to a particular course of action to improve its compliance with the PDPA. For example, an undertaking may be considered when the organisation is able to achieve the desired level of compliance to the PDPA in a prompt manner without requiring the PDPC to conduct a full investigation.

In the case of Xiaomi Singapore Pte Ltd (Xiaomi), the organisation provided an undertaking to improve its compliance after the PDPC raised concerns about its practice of signing users up to its cloud messaging services by default, without notification. Separately, PDPC found a complaint lodged against Xiaomi for disclosing personal data to third-party marketers without consent to be unsubstantiated.

Details of the cases, including learning points, are listed in **Annex A**.

Since the PDPA came into full effect in July 2014, the PDPC has received 667 complaints. 92% of these complaints were resolved through investigation and facilitation between the respective organisations and individuals. Common complaints include the collection, use and disclosure of personal data without notification or consent, as well as the disclosure of personal data through lack of protection by these organisations.

Mr Leong Keng Thai, Chairman, PDPC, said, "The enforcement actions taken are not to deter the use of personal data for business competitiveness. We recognise that data is essential for innovation in today's economy. The key is to use it responsibly and take appropriate actions to protect it. Both the organisation and its data intermediary, such as IT vendors that provide systems and data management solutions to businesses, are expected to exercise due care and implement adequate security measures."

Annex A – Summary of Facts & Key Learning Points

Annex B – Selected Sections of the PDPA

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

About Personal Data Protection Commission

The PDPC administers the Personal Data Protection Act 2012 (PDPA) in Singapore, which aims to safeguard individuals' personal data against misuse and promote proper management of personal data in organisations. The PDPA enhances Singapore's competitiveness and strengthens our position as a trusted business hub, putting Singapore on par with the growing list of countries with data protection laws. For more information, please visit www.pdpc.gov.sg.

For media queries, please contact:

Ms Deborah Lee
Manager, Communications, Outreach and International
Personal Data Protection Commission
Tel: 6508 7355
E-mail: deborah_lee@pdpc.gov.sg

Mr Kenneth Tan
Manager, Media Relations
Personal Data Protection Commission
Tel: 6211 1600
E-mail: kenneth_tan@pdpc.gov.sg

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ANNEX A – Summary of Facts and Key Learning Points

Organisation: K Box Entertainment Group Pte Ltd (K Box)

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. Members of the public who noticed the leak lodged complaints with the PDPC.

K Box did not ensure that its IT system security was sufficiently robust as security patches were not updated. This allowed external parties to install malware to gain easy access into the system.

There was also no DPO to develop and implement data protection policies, resulting in weak control of access to personal data. For example, unused accounts were not disabled and account-holders used weak passwords consisting of only a single character.

Decision: Breach of section 24 of the PDPA for failing to implement proper and adequate protective measures, resulting in unauthorised disclosure of a large number of personal data. Additionally, the lack of adequate data protection policies, including the absence of a DPO, was considered and it was found that sections 11(3) and 12(a) were also breached.

Actions Taken: Financial penalty of $50,000 was imposed and other directions issued.

Organisation: Finantech Holding Pte Ltd (Finantech)

Finantech was engaged by K Box in August 2007 to develop, host and manage its Content Management System (CMS). As the data intermediary, Finantech did not patch security vulnerabilities in K Box's IT system that held its customers' personal data. Additionally, the password used for the administrator account was simply "admin", which is a weak password that made the administrator account vulnerable to hacks.

Decision: Breach of section 24 of the PDPA for failing to implement proper and adequate protective measures for the personal data in the CMS that it had built and managed for K Box, resulting in unauthorised disclosure of personal data.

Action Taken: Financial penalty of $10,000 was imposed.

Organisation: Institution of Engineers, Singapore (IES)

In October 2014, the PDPC was informed that personal data of users of the IES website had been uploaded on http://pastebin.com. The information was made available through two posts, which revealed the IES members' contact numbers, member IDs and passwords. Through this information, one could potentially access the members' full names, email addresses, residential addresses and other data. The case affected more than 4,000 individuals.

There were security vulnerabilities in IES' IT system that were not patched. In addition, passwords were stored in the clear and not encrypted.

Decision: Breach of section 24 of the PDPA for failing to implement proper and adequate protective measures such as the updating of security patches, resulting in unauthorised disclosure of personal data.

Actions Taken: Financial penalty of $10,000 was imposed and other directions issued.

Organisation: Fei Fah Medical Manufacturing Pte Ltd (Fei Fah)

On 29 September 2014, the PDPC was notified that personal information of Fei Fah's customers had been posted on http://pastebin.com. The information included usernames, passwords, contact numbers and email addresses. More than 900 individuals were affected.

Fei Fah did not ensure that the security measures put in place were sufficient to protect the personal data on its website and server which hosted the database containing its customers' personal data.

Decision: Breach of section 24 of the PDPA for failing to implement proper and adequate protective measures such as adding security measures to protect databases stored online, resulting in unauthorised disclosure of personal data.

Actions Taken: Financial penalty of $5,000 was imposed and other directions issued.

Organisation: Universal Travel Corporation Pte Ltd (UTC)

In March 2015, PDPC received a complaint on wrongful disclosure of personal data by UTC. Four of UTC's customers had requested for information to facilitate their insurance claims relating to changes in flight timings during a particular tour organised by UTC. As there was no clear data protection policy in place, a UTC staff proceeded to share a document that contained the personal data of all 37 customers who had signed up for the same tour without redacting the personal data, such as the name,

nationality, date of birth, passport number and passport expiry date, of the other customers.

Decision: Breach of section 13 for disclosure of personal data without consent. Additionally, the lack of data protection policies was considered and it was found that section 12(a) was also breached.

Action Taken: Directions issued for UTC to inform individuals who had received the passenger list not to disclose the list to other third parties; put in place a data protection policy to comply with the PDPA; and to send UTC employees for training on the obligations of the PDPA.

Organisation: Challenger Technologies Ltd (Challenger)

The PDPC received a complaint in September 2014 that Challenger had sent an individual an email with details of membership that belonged to another customer. Challenger's IT vendor had sent out the email update on its behalf to over 165,000 Challenger members regarding the status of their membership points. However, the emails were sent to the wrong recipients, resulting in each Challenger member receiving the information of another member. Challenger did not have measures in place for its IT vendor to check that the emails were sent to the correct recipients.

The personal data disclosed was limited to the member's name, accumulated points and expiry date. Based on this information alone, the risk of the points being misused was low.

Upon discovering the error, Challenger sent out an apology email to its members the next day, and engaged a training and consultancy firm to help Challenger review its policies and practices to better comply with the PDPA.

Decision: Breach of section 24 of the PDPA for failing to make reasonable security arrangements to prevent unauthorised disclosure of its members' personal data while sending out email communications.

Action Taken: Warning issued.

Organisation: Xirlynx Innovations (Xirlynx)

IT vendor Xirlynx was engaged by Challenger to manage its email communications, among others. Its employee had used an erroneous excel database to send out email updates without conducting checks to ensure that the emails were sent to the correct recipients.

Decision: Breach of section 24 of the PDPA for failing to make reasonable security arrangements to prevent unauthorised disclosure of Challenger members' personal data while sending out email communications.

Action Taken: Warning issued.

Organisation: Full House Communications Pte Ltd (Full House)

On 4 March 2015, PDPC received a complaint regarding the computer system used by Full House to register individuals in lucky draws at a furniture exhibition. The system used a web browser but its auto-fill feature was not disabled. As such, when a user clicked on a field, the system showed the earlier entries (e.g. in the name field, individuals can see a range of names keyed in earlier).

The disclosure of data, however, was limited as the data fields were not linked and details in each field were shown in alphanumeric order. Furthermore, there were members of staff stationed around the lucky draw terminal to monitor the submission, which reduced the risk of individuals collecting the participants' personal data. Full House took prompt remedial actions to rectify the flaw after it was notified of the issue.

Decision: Breach of section 24 of the PDPA for failing to make reasonable security arrangements to prevent unauthorised disclosure of personal data collected from customers.

Action Taken: Warning issued.

Organisation: Metro Pte Ltd (Metro)

In April 2015, PDPC received a complaint that the personal data of 445 of Metro's customers was posted on http://siphon.net in early 2015. This website was set up by a group of security enthusiasts to increase public's awareness on security risks and the risks of compromised/stolen data.

Investigations by PDPC revealed that the data leak was linked to a defacement of Metro's website around February 2014. While Metro had taken steps to patch the defacement then, it failed to detect other well-known and common vulnerabilities which remained unpatched until an internal IT security audit in 2015. Upon notification of the complaint in 2015, Metro took prompt remedial actions to rectify vulnerabilities by instructing its IT vendors to conduct thorough security scans and penetration tests for its external webservers to ensure that its CMS and website application are secure.

Decision: Breach of section 24 of the PDPA for failing to make reasonable security arrangements to prevent unauthorised access to personal data held in Metro's web-facing systems.

Action Taken: Warning issued.

Organisation: Singapore Computer Society (SCS)

The PDPC was notified in March 2015 that an SCS employee had sent out an email to registrants of an event and attached a document containing personal data of the 214 registrants, including their name, SCS identity number, NRIC number, contact number, organisation and designation.

Upon discovery of the mistake, SCS took prompt action to recall the email and also issued an apology to the recipients.

Decision: Breach of section 24 of the PDPA for failing to make reasonable security arrangements to prevent unauthorised disclosure of its registrants' personal data while sending out email communications.

Action Taken: Warning issued.

Organisation: YesTuition Agency (YesTuition)

The PDPC received a complaint on 16 July 2014 that YesTuition, which has a web portal that allows customers to view its tutors' profiles and photos, had used the NRIC numbers of the tutors as the filename for the photos. The images and NRIC numbers of about 30 individuals were accessible from the directory listing on the web portal. As a result, users accessing the profiles of the tutors could view their NRIC numbers. The tutors had not consented to the public disclosure of their NRIC numbers and photos in this manner.

YesTuition took prompt remedial action to remove the NRIC reference after being notified by PDPC.

Decision: Breach of section 13 of the PDPA for disclosing the tutors' personal data on its website without consent.

Action Taken: Warning issued.

Organisation: Xiaomi Singapore Pte Ltd (Xiaomi)

In July 2014, a complaint was lodged that Xiaomi might have disclosed the personal data of its users to telemarketers without consent. There was a subsequent online article by an overseas security firm, F-Secure Corporation, stating that Xiaomi RedMi

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

1S mobile phones were automatically uploading personal data to Xiaomi's server(s) overseas without the knowledge of their users.

The PDPC's investigations found that Xiaomi had not disclosed the personal data of its users to third-party marketers. However, the PDPC had concerns about its practice of signing up some users to its cloud messaging services by default, without notification. In response to that, Xiaomi provided an undertaking to improve its compliance in this area. The PDPC is satisfied that Xiaomi has since completed implementation of measures to improve its compliance and address the areas of concern set out above.

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Key Learning Points:

- **Obligations under PDPA**
    - Be aware that both the organisation and its Data Intermediary (DI) have obligations under the PDPA – vendors who are processing personal data for their clients have to take note of their protection and retention limitation obligations.
    - Engage in close discussion with DIs to ensure that the appropriate level of security is provided for the protection of personal data.
- **Policies and Processes**
    - Appoint a DPO to be responsible for ensuring compliance with the PDPA.
    - Develop and implement personal data protection policies, including the enforcement of password policies among employees with access to personal data, such as using strong passwords and periodically changing passwords, and including sample checks for activities involving mass distribution.
    - Ensure that employees are aware of their role in protecting personal data that is under the organisation's control or in the organisation's possession.
- **Collection, Use and Disclosure**
    - Ensure that individuals are notified on the purpose of the collection, use and/or disclosure of their personal data.
    - Ensure that the use or disclosure of personal data is in line with the purpose it was collected for, and that consent has been obtained from the individuals.
    - Ensure that personal data, in particular those collected using publicly-shared devices, will not be inadvertently disclosed to other individual (e.g. disabling the browser history in online forms).
- **Protection**
    - Ensure that personal data in an organisation's possession or under its control is properly protected, such as:
        - ➢ not relying on default or simple passwords that can be easily guessed;
        - ➢ conducting security audits and tests for IT systems;

  - regularly updating security patches; and
  - disabling accounts that are no longer necessary or in use.

- Ensure that the appropriate level of security is used in a public-facing website or application that collects and stores personal data.

- Ensure that measures are put in place for the sending of mass emails, letters or any other communications to prevent sending to the wrong recipients.

- Password-protect documents containing personal data to reduce risk of unauthorised disclosure when such documents are sent to the wrong recipients.

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ANNEX B – Selected sections of the Personal Data Protection Act (PDPA)

Section 11: Compliance with Act

1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.

(2) An organisation is responsible for personal data in its possession or under its control.

(3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.

(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation.

(5) An organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4).

(6) The designation of an individual by an organisation under subsection (3) shall not relieve the organisation of any of its obligations under this Act.

Section 12: Policies and Practices

An organisation shall —

(a) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act;

(c) communicate to its staff information about the organisation's policies and practices referred to in paragraph (a); and

(d) make information available on request about —

(i) the policies and practices referred to in paragraph (a); and

(ii) the complaint process referred to in paragraph (b).

Section 13: Consent Required

An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —

(a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or

(b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law.

Section 24: Protection of Personal Data

An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.