Linklaters

May 2016

PDPC Enforcement Actions: Three Lessons for Your Organisation.

On 21 April 2016, Singapore's data privacy regulator, the Personal Data Protection Commission ("**PDPC**") announced that it had taken enforcement actions against 11 organisations for breaching their data protection obligations under the Singapore Personal Data Protection Act 2012 (the "**PDPA**"). These cases involved various contraventions of the PDPA, a majority of which related to unauthorised access or disclosure of personal data.

The PDPC's Grounds of Decision for these cases were also released. The PDPC took a calibrated approach to enforcement action, reflecting its overarching policy that organisations should feel free to continue processing personal data, while taking appropriate actions to keep it secure. Only five organisations were issued with directions (four of which included penalties of up to S$50,000), while the other six were issued with warnings. The severity of the PDPC's directions depended on several factors, including the scale of the breach, remedial actions taken and the organisation's cooperation with the PDPC. Financial penalties were generally imposed on organisations involved in larger scale breaches or on those that were uncooperative with the PDPC.

While there are many lessons organisations can take away from these enforcement actions, the top three learning points we recommend you should address are as follows:

1 Cybersecurity is a critical concern. Early prevention is key.

Of the 11 organisations involved in the PDPC's enforcement actions, five of these fell victim to hacking incidents where personal data held by them were leaked onto public websites. In the course of investigations by the PDPC, it was found that these organisations did not have in place adequate security measures to prevent such hacking.

Some examples of inadequate security measures that the PDPC cited in its Grounds of Decision included:

- omissions to provide password protection or encryption of data;

Contents

1 Cybersecurity is a critical concern. Early prevention is key.. 1

2 Suffering a data breach is not the end of the world. Effective post-breach management can help your case. 2

3 Data intermediaries are separately liable to ensure protection of personal data.... 3

- having “weak” password protection of critical user accounts;
- failure to audit third party service providers assisting with processing of data; and
- not having in place penetration testing software.

On a global scale, large scale hacking incidents have also recently hogged the limelight – the “Panama Papers”, the 2016 Bangladesh Bank hacking heist and the “shame” hacking of the Ashley Madison website are prime examples of the significance of the cybersecurity threat.

In this day and age, it is imperative that organisations put in place adequate security controls on their IT systems and regularly review and update such safeguards. Perhaps as important is the need for organisations to embed a culture of data privacy among their employees. Human error (e.g. accidental or unauthorised disclosure or improper disposal of documents) features as one of the primary causes of data breaches in organisations. The PDPC specifically noted in one of its Grounds of Decision that apart from systems-related shortcomings, investigations disclosed that there were also poor data privacy practices within the organisation investigated. Developing robust internal policies (e.g. security, IT and social media policies), and more importantly embedding a culture of data protection in your organisation, constitute critical prevention steps that will go a considerable way to not only ensuring the personal data that your organisation controls is kept secure, but also potentially saving your organisation significant costs associated with fines, post-breach remedial actions and investigations.

2 Suffering a data breach is not the end of the world. Effective post-breach management can help your case.

In most of the enforcement actions, the PDPC particularly considered the remedial actions, if any, which the errant organisations took to manage the data breaches when deciding what directions (if any) to issue to these organisations. Generally, and perhaps unsurprisingly, the fact that an organisation acted promptly to manage and remedy a data breach was a factor that weighed heavily in its favour.

Effective data breach management will ultimately need to be adapted to the circumstances of the particular breach. Different types and scales of data breaches will call for particular remedial actions to be undertaken.

Examples of remedial action taken by the organisations that the PDPC lauded in its Grounds of Decision included:

- **Prompt notification to affected individuals**: The PDPC took into consideration the fact that K Box Entertainment Group Pte Ltd (“**K Box**”) notified its members of the data breach by way of a letter on the day that it discovered that its members’ personal data had been posted on a public website. Similarly, the Institution of Engineers Singapore (“**IES**”) sent an email notification to all its members

informing them of the hacking activity on its site one day after it discovered the data leak.

- **Implementing additional IT security measures**: The PDPC also noted that IES installed a new intrusion detection system and Secure Sockets Layer certification on its website service following the data leak.
- **Conducting internal investigations/audits**: The PDPC noted that Metro Pte Ltd engaged an external consultant to undertake an internal IT security audit and assessment shortly after it had learnt of the posting of its customers' personal data on a public website. Similarly, IES had instructed its website vendor to conduct a security audit of the website to patch up any vulnerabilities detected.

In 2015, the PDPC issued some guidance on managing data breaches. Our analysis of this guide can be found here.

3 Data intermediaries are separately liable to ensure protection of personal data.

Two of the enforcement actions were against multiple organisations – namely, the primary data owner of the personal data and the third party service provider who processed the organisation's personal data on its behalf pursuant to a contract (i.e., a "data intermediary" for the purposes of the PDPA). Data intermediaries are exempt from complying with most of the PDPA obligations in respect of the personal data they process on behalf of other organisations, with the exception of the protection and retention obligations which they are expected to comply with in full.

The enforcement actions taken by the PDPC last month constitute a clear message to data intermediaries that they will be separately responsible and liable for their own failure to comply with their obligations under the PDPA.

In the K Box case, K Box's data intermediary, Finantech, was found to have failed to put in place the required security measures to provide adequate protection for the personal data in its control, and was fined S$10,000 separately from K Box's fine of S$50,000.

Organisations that act as data intermediaries should therefore be equally mindful of their PDPA obligations. In the same vein, organisations which engage data intermediaries to process personal data on their behalf should also ensure that they undertake an appropriate level of due diligence to assure itself that the data intermediaries they engage are capable of complying with the PDPA's obligations, backed up with the necessary data protection terms and conditions in their contractual arrangements with such data intermediaries (e.g. tailored data protection obligations, notification requirements, preventive steps, remedial measures and potentially contractual indemnities).

Finally, the PDPC also issued new Advisory Guidelines on Enforcement of the Data Protection Provisions on 21 April 2016, which serve to provide more clarity on the PDPC's powers of investigation, and the directions and penalties it can issue to organisations. The Guidelines can be accessed here.

If you require further information or assistance with any of the above, please feel free to contact any of your Linklaters contacts.

Contacts

For further information please contact:

Adrian Fisher
Counsel

(+65) 66925856

adrian.fisher@linklaters.com

Laure de Panafieu
Counsel

(+65) 66925791

laure.de_panafieu@linklaters.com

Joel Cheang
Associate

(+65) 66925877

joel.cheang@linklaters.com

Authors: Adrian Fisher, Laure de Panafieu, Joel Cheang

One George Street #17-01
Singapore 049145

Telephone (+65) 6692 5700
Facsimile (+65) 6692 5708

Linklaters.com