LHAG Insights

Technology, Media & Telecommunications

G. Vijay Kumar
Partner
TMT
E: vkg@lh-ag.com

Harvey Ng Yih Xiang
Associate
TMT
E: nyx@lh-ag.com

Nicole Shieh E-Lyn
Associate
TMT
E: sel@lh-ag.com

Wee Yun Zhen
Associate
TMT
E: wyz@lh-ag.com

9 MAY 2023

Legal Exposure Of A Company In The Event Of A Data Breach

In our previous article, we discussed measures a company should consider taking in response to a data breach.[1] In this article, we will expand the discourse to the potential liabilities a company may be exposed to, and the measures available to reduce the risks of being held liable in the event of a data breach.

Potential Liabilities under the Personal Data Protection Act 2010 ("PDPA")

Under the PDPA, as a data user, a company is obligated to adopt reasonable measures to safeguard any personal data that is being stored or processed. It is also incumbent upon the company to establish and implement a viable security policy. This policy must include provisions for specific security measures such as anti-virus and anti-malware softwares, as well as access control protocols.[2]

The consequences of a company being held liable for breach of its obligations under the PDPA due to a data

[1]You may access our previous article here: <https://www.lh-ag.com/wp-content/uploads/2023/03/LHAG-Insights-20230321.pdf>

[2]Code of Practice for licensees under the Communications and Multimedia Act 1998

breach is considered severe. The company may be prosecuted and upon conviction be liable to a fine not exceeding RM300,000. Additionally, individuals held responsible for the breach may be liable to imprisonment up to a term not exceeding 2 years.[3]

In the case of *Fei Fah Medical Manufacturing Pte Ltd*,[4] the personal data of users including user IDs and passwords, telephone numbers, and email addresses were exposed publicly on a website following a data breach. The company, despite having engaged an IT firm to oversee the security protocols of their website and servers, was still found to be in breach of the Singapore Personal Data Protection Act 2012 ("**Singapore PDPA**") by the Data Protection Commission of Singapore. This was due to evidence which showed that the company had simply left its responsibilities to the third-party IT firm to implement any security features they deemed fit and thus, the company had limited knowledge of the security measures implemented on its website and servers. As a consequence of the breach, the Data Protection Commission of Singapore ordered the company to pay a fine of SGD 5,000, in addition to other penalties.

A data breach may occur even with the most comprehensive data security systems in place. In such circumstances, in order to reduce the risk of being liable following a data breach, a company should ensure that they have complied with the requirements to implement reasonable security measures as discussed above. In addition, if the company has appointed a third-party IT vendor, the company must nevertheless periodically undertake the necessary verifications to ensure that the IT vendor has complied with the regulatory requirements. The company should also maintain proper records of regular system maintenance, periodic reviews and updates to anti-virus software, penetration testing and any other system security related information as evidence to prove that they have complied with the obligations under the PDPA so as to not be held liable in the event of a data breach.

---

[3] Section 5 of the Personal Data Protection Act 2010
[4] *Fei Fah Medical Manufacturing Pte Ltd* [2016] SGPDPC 3

LH AG ADVOCATES AND SOLICITORS

Potential Liabilities due to claims brought by Customers

When a company is found to be in violation of the PDPA, it will only be subject to the penal sanctions under the PDPA. However, the customers, i.e., victims of a data breach, are not entitled to seek compensation arising from a data breach incident under the PDPA. Nevertheless, customers impacted by a data breach may initiate legal action in the civil courts to seek redress for violations of their privacy.

Though the right to privacy is recognised as a constitutional right under Article 5(1) of the Federal Constitution, the right only protects individuals against acts by the Parliament, Government and/or its agencies. As such, a claim for breach of constitutional right under Article 5(1) of the Federal Constitution cannot be sustained against private companies for data breaches.

However, the affected customers may sue the company in tort under causes of action such as breach of confidence / breach of privacy. To succeed in these claims, the most crucial element to be proven is whether the information disclosed by the data breach was confidential. As such, in the event of a potential claim, companies should seek professional legal advice on what defences may be available to them in law based on the particular facts of the case. If a company is found liable for breach of privacy, the court will award damages to the customer.[5] The amount of damages awarded will depend on the loss suffered by the customer as a consequence of the breach.

Potential Liabilities arising from Ransomware Attacks

In the past, hackers typically acquire personal data through cyberattacks and subsequently sell the stolen data to third parties for financial gain. However, cyber criminals appear to increasingly employ ransomware attacks lately, where they could secure a ransom directly from the affected data users. This is supported by the

[5] *Maslinda bt Ishak v Mohd Tahir bin Osman & Ors* [2009] 6 MLJ 826; *Lee Ewe Poh v Dr Lim Teik Man & Anor* [2011] 1 MLJ 835

latest statistics which indicate a 16% year-on-year rise of detected ransomware attacks in 2022.[6]

In the recent case of *HMI Institute of Health Sciences*,[7] a healthcare training institute in Singapore was the target of a ransomware attack where the cyber attacker encrypted the personal data stored by the institute. The attack denied the institute access to its own files which contained personal data of its customers in the server. A ransom note was subsequently discovered on the affected server. The institute immediately engaged a cybersecurity expert company to conduct an independent assessment of the incident and to recommend the necessary remedial measures. Thereafter, the institute took prompt action to remedy the faults identified by the experts and to prevent a recurrence of the incident.

Despite undertaking prompt remedial measures following the attack, the Singapore Data Protection Commission nevertheless found that the institute was in breach of its statutory duty to take reasonable steps to prevent unauthorised access to personal data in its possession when it failed to secure a remote connection to its server over a period of 4 years, which ultimately resulted in the data breach. The institute was consequently penalised with, amongst others, a fine of SGD 35,000.

This case once again underscores the importance of companies taking reasonable pre-emptive measures to safeguard personal data stored or processed by them as it will be a valid defence against any regulatory actions that may follow from a data breach incident. Remedial or mitigating actions subsequent to a data breach may not be sufficient for a company to absolve itself from liability. This case also serves as a reminder for companies to ensure that they have backed up their data on other servers or to maintain an offline backup of their data, in order to prevent being held ransom by the cyber attackers.

---

[6] Surin Murugiah, 'Ransomware attacks in Malaysia up 16% y-o-y in 2022, says Trend Micro' (Theedgemarkets, 8th March) <https://www.theedgemarkets.com/node/658253> accessed 8 May 2023

[7] *HMI Institute of Health Sciences Pte. Ltd.* [2021] SGPDPC 4

LH AG ADVOCATES AND SOLICITORS

Reasonable Measures a Company may take to comply with the PDPA 2010

In *Giordano Originals (s) Pte Ltd*,[8] the Singapore Personal Data Protection Commission decided that there was no breach of the Singapore PDPA by the company, as the company had taken sufficient pre-emptive measures to protect the personal data, which include the following:

1. Implemented security measures recommended by the Commission Handbook on "How to Guard Against Common Types of Data Breaches";

2. Installed and deployed various endpoint security solutions, which was complemented with real-time system monitoring for Internet traffic abnormalities;

3. Conducted regular periodic system maintenance, reviews and updates such as vulnerability scanning and patching;

4. Ensured that its data was regularly and automatically backed-up; and

5. Encrypted personal data using the current industry-standard RSA algorithm and passphrase.

Conclusion

The personal data of customers are a common target for cyber criminals because it is inherently valuable and vital to the operations of a company. Therefore, companies that process or store personal data must implement up-to-date and proper security measures to prevent data breaches. If a data breach occurs, a company could potentially face statutory penalties as set out in the PDPA, the possibility of legal action initiated by its customers, or the challenge of handling ransom demands.

---

[8] *Giordano Originals (s) Pte Ltd* SGPDPC Case No. DP-2011-B7387

If you have any queries please contact associates **Harvey Ng Yih Xiang** (nyx@lh-ag.com), **Nicole Shieh E-Lyn** (sel@lh-ag.com), **Wee Yun Zhen** (wyz@lh-ag.com) or their team partner, **G. Vijay Kumar** (vkg@lh-ag.com).

Head Office
Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia
Tel: +603 6208 5888
Fax: +603 6201 0122

Johor Office
Suite 21.01
21st Floor, Public Bank Tower
No.19, Jalan Wong Ah Fook
80000 Johor Bahru, Johor
Tel: +607 278 3833
Fax: +607 278 2833

Penang Office
51-12-E, Menara BHL Bank,
Jalan Sultan Ahmad Shah,
10050 Penang
Tel: +604 299 9668
Fax: +604 299 9628

Email
enquiry@lh-ag.com

Website
www.lh-ag.com

Published by the Technology, Media & Telecommunications Practice