CNPUPDATE

cnplaw
KNOWING ▪ THINKING ▪ SOLVING
Across Asia

600 North Bridge Road
#13-01 Parkview Square
Singapore 188778

T: +65 6323 8383
F: +65 6323 8282
contact@cnplaw.com

www.cnplaw.com

Fine of $1,000,000 imposed on SingHealth and IHiS for breach of Personal Data Protection Act

In a Grounds of Decision ("SingHealth-IHiS Decision") released on 15 January 2019, the Personal Data Protection Commission ("PDPC") meted out its largest fines to date to Singapore Health Services Pte. Ltd. ("SingHealth") and Integrated Health Information Systems Pte. Ltd. ("IHiS"), in the amounts of $250,000 and $750,000 respectively for their involvement in the largest data breach incident since the Personal Data Protection Act ("PDPA") came into force in 2014.

In June-July 2018, personal data of more than 1.5 million of SingHealth's patients and outpatients were accessed and copied following an attack on its system by unknown perpetrators. IHiS, the central national IT agency for the public healthcare sector, was primarily responsible for cybersecurity of SingHealth's systems.

The PDPC considered the technical security measures and incident response policies in detail and, having regard to the "highly sensitive and confidential" nature of the medical records that could cause an individual embarrassment if made known, found that both SingHealth and IHiS breached Section 24 of the PDPA in failing to implement reasonable security measures to protect personal data.

The maximum financial penalty the PDPC could have imposed was $1 million on each of SingHealth and IHiS. The PDPC noted that it would have imposed the maximum fine on IHiS instead of $750,000 if not for the mitigating factors that IHiS had voluntarily and unequivocally admitted to liability, cooperated during the investigation, took immediate effective remedial action and that it was a victim of a "skilled and sophisticated threat actor".

In meting out the $250,000 fine to SingHealth, the PDPC cited the same mitigating factors as it did for IHiS and also noted SingHealth's constraints since it was a matter of policy that IT functions and capabilities needed to be centralised in IHiS. While the latter factor is unlikely to be relevant in other fact scenarios in the private sector, organisations should be aware of the need to manage data that is held by a data intermediary. The PDPC has stated in various earlier decisions, and reiterated in the SingHealth-IHiS Decision, that there should be a contract setting out "the obligations and responsibilities of a data intermediary to protect the organisation's personal data and the parties' respective roles, obligations, and responsibilities to protect the personal data."[1] It is clear that a data controller's duty to take reasonable steps to protect personal data from unauthorised use and disclosure is not discharged by merely outsourcing the data to a third-party service provider.

This SingHealth-IHiS Decision reinforces the growing importance and emphasis on cybersecurity, and organisations should carefully consider the strength of their safeguards, technical and otherwise, against unauthorised access to personal data in their care.

[1] Paragraph 59, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision—SingHealth-IHiS—150119.pdf

cnplaw
KNOWING ▪ THINKING ▪ SOLVING
Across Asia

600 North Bridge Road
#13-01 Parkview Square
Singapore 188778

T: +65 6323 8383
F: +65 6323 8282
contact@cnplaw.com

www.cnplaw.com

Author:

Mr Stephen Soh and Ms Lorraine Liew

For further information on the above, please contact our Data Protection and Security Team.