PERSONAL DATA PROTECTION COMMISSION

Case No. DP-1811-B2975

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

(1) MRI Diagnostics Pte Ltd
(2) Clarity Radiology Pte Ltd

SUMMARY OF THE DECISION

1. MRI Diagnostics Pte Ltd ("**NovenaMRI**") operates a medical centre that provides magnetic resonance imaging and X-Ray services to patients. In the course of their business, NovenaMRI subscribed to an internet based teleradiology system ("**System**") provided by Clarity Radiology Pte Ltd ("**Clarity**"). In-turn, Clarity engaged an overseas IT vendor (the "**IT Vendor**") to maintain the System.

2. On 7 November 2018, a patient of NovenaMRI ("**Complainant**") notified the Personal Data Protection Commission (the "**Commission**") about an Excel Spreadsheet containing approximately 600 individual's personal data (including the Complainant's) that was accessible via the internet (the "**Incident**").

3. During the course of investigations, the Commission found two additional Excel Spreadsheets containing similar information as the Excel Spreadsheet reported by the Complainant. A total of approximately 4,099 individuals were affected by the Incident ("**Affected Individuals**"). The Affected Individuals' personal data that was exposed to unauthorised access included their names, NRIC numbers and the type of radiology scans performed (collectively, the "**Personal Data Sets**").

4. The Commission's investigations revealed that the Incident was caused by a lapse in the IT Vendor's processes while carrying out maintenance work on the System. In particular, the IT Vendor had removed access restrictions to a network folder containing the Excel Spreadsheets for the purposes of patching the System, and omitted to reinstate the access restrictions after the patching was completed. Without access restrictions, the Excel Spreadsheets (containing the Personal Data Sets) were indexed by Google's search engines and exposed to unauthorised access.

5. NovenaMRI was an organisation who had collected the Personal Data Sets from its patients, and had control of the Personal Data Sets at all material times.

6. Section 24 of the Personal Data Protection Act ("**PDPA**") requires organisations like NovenaMRI to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or similar risks (the "**Protection Obligation**"). In this regard, the Deputy Commissioner for Personal Data Protection ("**Deputy Commissioner**") finds NovenaMRI in breach of the Protection Obligation because:

    (a) When an organisation engages a vendor to supply, modify and/or maintain its IT system, it is required to provide the vendor with sufficient clarity and specifications on the requirements to protect personal data. This is because even if the vendor was not engaged to process personal data on the organisation's behalf, it may nevertheless handle the personal data incidentally or make decisions that affect the security of the personal data in the course of providing its services. Depending on the circumstances of each case, the organisation should articulate its business requirements concerning the protection of personal data that the IT system will store. This will enable the vendor to assess and recommend the most appropriate and effective method to protect personal data. The organization will then be able

to make a decision with access to the right information. Examples of measures include having clauses in written agreements setting out clearly the vendor's obligations to protect personal data, providing operational guidance and verifying the data protection arrangements implemented by the vendor and/or exercising some form of supervision and oversight over the vendor's activities;

(b) Given the nature of NovenaMRI's business, which entailed being in possession and/or control of personal data of a sensitive nature (e.g. radiology scans and X-Rays), NovenaMRI should also have conducted a proper assessment of its vendor to satisfy itself that the vendor is well-placed to protect the personal data it hosts. For example, NovenaMRI could have obtained documentary evidence that the vendor had complied with industry standards with respect to information security (eg the ISO 27001 standard). However, in this case, there was no evidence that NovenaMRI had conducted proper due diligence of the security standards put in place by Clarity, prior to subscribing to the System that provided cloud-based services, including hosting the Personal Data Sets;

(c) Although NovenaMRI claimed that it had a written agreement with Clarity, it was unable to produce supporting evidence of this. NovenaMRI's claim was also disputed by Clarity, who had admitted that there was no written agreement between the parties. In addition, even after NovenaMRI had engaged Clarity, NovenaMRI did not take any steps to verify if Clarity had implemented any data protection arrangements with respect to the System which hosted the Personal Data Sets.

7. As for Clarity, the contracted services from Clarity to NovenaMRI were to provide an archive for Dicom Images and a Web-based radiology information system with scheduling, registration, billing and client access modules. Essentially, Clarity was a "Software as a Service" provider (or what is commonly known as

"SaaS-provider") who had provided its cloud-based services to NovenaMRI. The provision of such technical solutions or deployment of software integrated into the clinical devices of NovenaMRI did not entail the processing of personal data. As such, Clarity was a vendor of NovenaMRI, and not a "data intermediary" of NovenaMRI. As a vendor, Clarity was not responsible for the protection of the Personal Data Sets under the PDPA in respect of the Incident.

8. However, during the course of investigations, Clarity admitted that it had failed to appoint a data protection officer and had not developed or put in place any data protection policies, as required under Sections 11(3) and 12 of the PDPA. Accordingly, Clarity is in breach of Sections 11(3) and 12 of the PDPA.

9. After considering the circumstances of the case, the Deputy Commissioner's decisions are as follows:

(a) to issue a warning to NovenaMRI for its breach of the Protection Obligation. No further directions are necessary as NovenaMRI has ceased its business relationship with Clarity; and

(b) to direct that Clarity shall, within 30 days from the date of this decision:

i. Appoint a data protection officer;

ii. Develop and implement a data protection policy to comply with its obligations under the PDPA; and

iii. Inform the Commission within 7 days of the completion of each of the above directions.