PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 5

Case No. DP-2009-B7011

In the matter of an investigation under section 50(1) of the

Personal Data Protection Act 2012

And

(1) NUInternational Singapore Pte Ltd

(2) Newcastle Research and Innovation Institute Pte Ltd

… *Organisations*

DECISION

---

(1) NUInternational Singapore Pte Ltd; (2) Newcastle Research and Innovation Institute Pte Ltd

[2021] SGPDPC 5

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2009-B7011

23 June 2021

Introduction

1 On 17 September 2020 and 13 November 2020, the Personal Data Protection Commission (the "**Commission**") was notified of a ransomware attack relating to Newcastle Research and Innovation Institute Pte Ltd and NUInternational Singapore Pte Ltd (collectively known as the "**Organisations**") in Singapore (the "**Incident**").

Facts of the case

2 The ransomware infected, on or around 30 August 2020, (a) a database in the United Kingdom, managed by the ultimate parent company of the Organisations (containing 1,083 records of Singapore-based individuals); and (b) a database in Malaysia, hosted by a related company of the Organisations (containing 194 records of Singapore-based individuals). These records containing personal data of the Singapore-based individuals were previously transferred from the Organisations to the ultimate parent company in the United Kingdom and the related company in Malaysia respectively. The Singapore-based individuals were a mix of staff members, undergraduates and/or post-graduate students of the Organisations. Their

personal data (comprising names and user account identifications) were exfiltrated by the threat actor.

Findings and Basis for Determination

3 Section 26(1) of the PDPA stipulates that an organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA (the "**Transfer Limitation Obligation**"). The requirements mentioned in section 26(1) were set out in Regulations 9 and 10 of the **Personal Data Protection Regulations 2014** (which were in force at the time) (the "**Transfer Regulations 2014**"). The Transfer Regulations 2014 was recently amended ("the **Transfer Regulations 2021**"). The ensuing analysis and application of the Transfer Regulations 2014 is equally relevant for the Transfer Regulations 2021, which is *in pari materia* but for some re-numbering of the regulations.

4 The Transfer Regulations 2014 provides for a range of transfer mechanisms to ensure compliance with Section 26(1) of the PDPA, e.g. through legally enforceable obligations under any law, contracts, binding corporate rules or any other legally binding instruments. Within a group of companies, reliance on intra-group agreements and binding corporate rules is common for cross-border data transfers. They provide a flexible system for centralisation of corporate functions and services. The commercial decision would be driven by where these functions are best located, and intra-group agreements and binding corporate rules allow the group to establish a bespoke internal governance system to ensure that personal data is well managed

across the group. The Transfer Regulations 2014 (and 2021) support the adoption of intra-group agreements and binding corporate rules in the following manner.

5 Pursuant to Regulation 9(1)(b), the Organisations could have met the Transfer Limitation Obligation by taking appropriate steps to ensure that the recipients of the transferred personal data in United Kingdom and Malaysia were bound by legally enforceable obligations (in accordance with Regulation 10(1) of the Transfer Regulations 2014) to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA. Regulation 9(1)(b) is now Regulation 10(1) in the Transfer Regulations 2021. Regulation 10(1) of the Transfer Regulations 2014 specifies that such legally enforceable obligations includes any law, a contract that complies with the conditions in Regulation 10(2), or binding corporate rules that meets the conditions set out in Regulation 10(3). These same regulations are now in Regulation 11 in the Transfer Regulations 2021. These regulations support the use of intra-group agreements[1] and binding corporate rules[2].

6 Investigations revealed that the Organisations did not put in place intra-group agreements, binding corporate rules or any other legally binding instrument to ensure that a standard of protection comparable to the PDPA is provided to personal data transferred within the group as required by Regulation 10(1).

7 In its responses to the Commission, the Organisations put forward the argument that they had met the Transfer Limitation Obligation under the PDPA by virtue of the fact that the laws of the United Kingdom applied to the receiving organisations within their group. I do not exclude the possibility that the data protection system that governs the receiving organisation

[1] See *Re Everlast Projects & Others* [2020] SGPDPC 20 at [13].
[2] See *Re Singapore Technologies Engineering Limited* [2020] SGPDPC 21.

may, on a proper analysis, provide comparable protection. However, based on the responses made by the Organisations to the Commission, I am not satisfied that the transferring organisation conducted this analysis and concluded that there would be comparable protection *before the transfer*. After the fact justification will not be accepted.

8 Of the 1,083 Singapore-based individuals whose personal data had been transferred to the ultimate parent company in the United Kingdom, the Organisations mentioned that 44 of these individuals, who were employees, had consented to the transfer of their personal data out of Singapore in their employment contracts. Regulation 9(3)(a) of the Transfer Regulations 2014 did provide for the Transfer Limitation Obligation to be met by obtaining the consent of individuals for the transfer of their data. However, to meet the consent requirement under Regulation 9(3)(a) of the Transfer Regulations 2014, Regulation 9(4) requires the Organisations to provide to the individuals a summary in writing of the extent to which their personal data, when transferred to a foreign country or territory, would be protected to a standard comparable to the PDPA. These requirements are now encapsulated in Regulations 10(2)(a) and 10(3) of the Transfer Regulations 2021. The procedural safeguards established by Regulation 9(3) of the Transfer Regulations 2014 makes the use of consent somewhat more cumbersome, as there is a need for consent to be refreshed whenever reorganisation of the group's internal function leads to a relocation of that function in a different jurisdiction. This also does not enable the Organisations to benefit from the employment management exception to the requirement for consent. Be that as it may, this option is available for organisations that choose to rely on it. However on the evidence, this summary in writing was not provided by the Organisations to the 44 Singapore employees.

The Deputy Commissioner's Directions

9 In view of the foregoing, I therefore find that the Organisations have failed to discharge their Transfer Limitation Obligation under section 26 of the PDPA. The Organisations are directed to do the following within 30 days from the date of this Decision:

(a) put in place intra-group agreements or binding corporate rules for compliance with section 26 of the PDPA in relation to any personal data transferred out of Singapore[3];

(b) if relying on consent, review and make necessary changes to its consent and notification processes for compliance with section 26 of the PDPA and Regulation 10(3) of the Personal Data Protection Regulations 2021 in relation to any personal data transferred out of Singapore; and

(c) inform the Commission of the completion of the above within 7 days of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

[3] Refer to Regulation 11 of Personal Data Protection Regulations 2021, which is applicable at the present time.