This decision is subject to final editorial corrections approved by the tribunal and/or redaction pursuant to the publisher's duty in compliance with the law, for publication in LawNet.

Cigna Europe Insurance Company S.A.-N.V.

[2019] SGPDPC 18

Yeong Zee Kin, Deputy Commissioner — Case No DP-1806-B2241

Data protection – Unauthorised disclosure of personal data – Insufficient security arrangements

20 June 2019.

Background

1 Cigna Europe Insurance Company S.A.-N.V. is a company established in Belgium which offers health insurance solutions and coverage in Singapore through a registered branch office (the "**Organisation**"). On 1 June 2018, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident involving the inadvertent disclosure of certain personal data of individuals who had taken up health insurance coverage with the Organisation. The Commission commenced an investigation in order to determine whether the Organisation had failed to comply with its obligations under the Personal Data Protection Act 2012 (the "**PDPA**").

Material Facts

2 The Organisation provides health insurance coverage to employees of its clients and their families who decided to take up such coverage

("**Members**"). In order to provide this health insurance coverage, it collects, uses and processes personal data of the Members.

3 In 2012, the Organisation entered into a services agreement (the "**Services Agreement**") with Cigna European Services (UK) Limited ("**CES**") for the provision of various insurance-related services. CES is a related company of the Organisation within the Cigna group of companies ("**Cigna Group**"). The services provided by CES included the processing of insurance claims (among other services) and this involved activities such as generating and sending claim settlement letters and letters accompanying cheque payments to Members who had made an insurance claim. Such claims were processed through an information technology ("**IT**") system which was operated by CES and used by various companies in the Cigna Group (the "**System**"). In order to make use of the System, the Organisation transferred its Members' personal data to CES and these data were processed in the System.

4 It transpired that, in two separate incidents in January 2017 and May 2018, claims settlement letters intended for certain Members were erroneously sent by CES to other Members. These incidents were due to technical issues affecting the production of the claims settlement letters by CES. In the second incident, the technical issues also affected the production of payment accompanying letters which were sent to some Members. CES initially did not inform the Organisation about the first incident. The Organisation only came to know about the two incidents after the second incident occurred.

Findings and Basis for Determination

5 The cause of the data breach incidents in this case may be traced to the technical issues in the System. As these matters were not within the

Organisation's operational control or even its knowledge prior to May 2018, the Organisation does not bear any direct responsibility under the PDPA for the occurrence of the two incidents.

6 Nevertheless, as the processing of the Members' personal data by CES was pursuant to the Services Agreement between the Organisation and CES, the question arises as to whether the Organisation had in place the appropriate measures to ensure protection of the Members' personal data while the data was stored with and processed by CES. In this regard, section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, disclosure and similar risks.

7 I find that the Organisation had in place the appropriate measures or could rely upon measures established within the Cigna Group to ensure protection of personal data by CES and to monitor CES' compliance. These measures include the following:

(a) The Organisation and CES had entered into the Services Agreement and an Interaffiliate Data Processing and Transfer Agreement in 2012 which required CES to protect personal data transferred to it by the Organisation. For example, various clauses in these agreements required CES:

(i) to protect the confidentiality of the Organisation's customer data;

(ii) to take appropriate and commercially reasonable measures to prevent, *inter alia*, unauthorised access or disclosure of such personal data and to ensure a level of security commensurate with the risks posed by the processing of personal data,

(iii) to comply with a specified set of security safeguards;

(iv) to notify the Organisation of any events that might impact the quality of CES' services and products;

(v) to give the Organisation access to the services for the purpose of reviewing and monitoring the quality of the services and the management of risks; and

(vi) to give the Organisation's internal and external auditors access to the services for the purpose of conducting audits;

(b) There were various internal frameworks, policies and standards which apply to companies within the Cigna Group, including CES. These included, among others, the Cigna Information Protection ("**CIP**") and General Computing Control ("**GCC**") governance frameworks. These frameworks, policies and standards addressed various aspects of IT security (amongst other matters); and

(c) CES was subject to Cigna Group's corporate audit and annual GCC assessment processes which include security and data protection, as well as external audits which may include IT audit reviews.

8 Finally, as regards the causes of the two incidents, the Organisation has informed the Commission that the Cigna Group (including CES, the Organisation and other affected companies within the group) will be improving

its processes in order to prevent a reoccurrence of the incidents. The actions of CES that were directly related to the two incidents took place outside our jurisdiction and were not part of the Commission's present investigation.

Application of section 26(1) of the PDPA to cross-border data transfers

9 As this case concerns personal data which had been transferred from the Organisation (in Singapore) to CES (in the United Kingdom), another question which may arise is whether the transfer meets the requirements of the PDPA. Section 26(1) of the PDPA prohibits organisations from transferring personal data to a country or territory outside Singapore "except in accordance with 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 relevant requirements are prescribed in Part III of the Personal Data Protection Regulations 2014 (the "**PDPR**"). In particular:

(a) Regulation 9(1) of the PDPR requires an organisation (referred to in the PDPR as a "transferring organisation"), before transferring personal data from Singapore to a country or territory outside Singapore, to "take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore … is bound by legally enforceable obligations (in accordance with regulation 10) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the [PDPA]";

(b) Regulation 10(1) provides that legally enforceable obligations (as referred to in regulation 9(1)) includes, among others, a contract in accordance with regulation 10(2); and

(c) Regulation 10(2) provides that a contract referred to in regulation 10(1) must:

(i) "require the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the [PDPA]"; and

(ii) "specify the countries and territories to which the personal data may be transferred under the contract".

10 The effect of the statutory provisions cited in the preceding paragraph is that when a transferring organisation in Singapore and an oversea recipient enter into a contract governing the transfer of personal data from the transferring organisation to the recipient, that contract must meet the two requirements specified in regulation 10(2) of the PDPR in order for the transferring organisation to have complied with section 26(1) of the PDPA. The second of these requirements (reproduced in paragraph 9(c)(ii) above) is self-explanatory. In relation to the first requirement (reproduced in paragraph 9(c)(i) above), the question is whether the contract requires the recipient to provide the appropriate standard of protection to the transferred personal data.

11 As stated in regulation 10(2) (and reproduced above), the standard of protection to the transferred personal data must be at least comparable to the protection under the PDPA. Determining the required standard for a particular contract would first involve considering how the PDPA applies to the personal data while it is in the possession or under the control of the transferring

organisation (i.e. before the transfer to the recipient). The contract should then be drafted to impose comparable obligations on the recipient in respect of the PDPA's nine main data protection obligations (as they are referred to in the Commission's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, in particular, at paragraph 10.2 thereof). These obligations are:

(a) The Openness Obligation (sections 11 and 12 of the PDPA);

(b) The Consent Obligation (sections 13 to 17 of the PDPA);

(c) The Purpose Limitation Obligation (section 18 of the PDPA);

(d) The Notification Obligation (section 19 of the PDPA);

(e) The Access and Correction Obligations (sections 21 and 22 of the PDPA);

(f) The Accuracy Obligation (section 23 of the PDPA);

(g) The Protection Obligation (section 24 of the PDPA);

(h) The Retention Limitation Obligation (section 25 of the PDPA); and

(i) The Transfer Limitation Obligation (section 26 of the PDPA).

12 As a general point, it is not necessary that a contract addresses all nine obligations. This would depend on factors such as the purpose of the transfer, the nature of the relationship between the transferring organisation and the

recipient and the scope of data processing services which the recipient may be providing to the transferring organisation. For example, if the recipient will not be assisting the transferring organisation with the handling of access and correction requests in relation to the transferred personal data, it would not be necessary for the contract to address the requirements of sections 21 and 22 of the PDPA.

13 In the present case, the Protection Obligation (section 24) is relevant to the transfer of personal data from the Organisation to CES. As discussed in the preceding section of this Decision, the Organisation had in place the appropriate security arrangements, including contractual provisions, which met the requirements of section 24 of the PDPA. Those contractual provisions would also meet the requirements of section 26(1) of the PDPA in relation to the Protection Obligation. (As an aside, this position would apply to other organisations in a similar relationship and similar circumstances, that is, where the recipient is a data intermediary of the transferring organisation and is processing personal data on behalf of and for the purposes of the transferring organisation.)

14 As the present case is concerned with the security arrangements put in place by the Organisation and the facts and circumstances of the case do not raise any particular concern as regards other aspects of the Organisation's transfer of personal data to CES, the Commission did not investigate further into the Organisation's compliance with section 26(1). I am satisfied that it is unnecessary to do so and hence make no finding in relation to that section.

Conclusion

15 In light of the above, I find that the Organisation had not contravened its obligations under section 24 of the PDPA.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION