PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 13

Case No. DP-2011-B7423, DP-2011-B7433

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

And

(1) Belden Singapore Private Limited
(2) Grass Valley Singapore Pte Ltd

… *Organisations*

DECISION

Data Protection *– Transfer obligation – Failure to ascertain and ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligations to provide a comparable standard of protection*

Belden Singapore Private Limited & Anor

[2021] SGPDPC 13

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2011-B7423, DP-2011-B7433

12 November 2021

Introduction

1. It is not unusual for a corporate group with a multi-national footprint to conduct cross-border transfers of personal data between its various entities. However, such arrangements also mean that data transferred from an organisation based in Singapore might risk exposure to data breach incidents in another jurisdiction. This is one such incident.

2. On 19 November 2020 and 20 November 2020, Belden Singapore Private Limited ("**Belden Singapore**") and Grass Valley Singapore Pte Ltd ("**GVSPL**") (collectively, the "**Organisations**") notified the Personal Data Protection Commission (the "**Commission**") of a data breach incident whereby an unauthorised third party had gained access to business servers of the Belden Group, and managed to exfiltrate information, including personal data of the employees of the Organisations ("**Incident**").

Facts of the Case

3. The Belden Group is a group of companies involved in the manufacturing of networking, connectivity and cable products. Its various subsidiaries and affiliated companies operate in the Americas, Europe, Middle East, Africa and the Asia Pacific region (the "**Belden entities**"). The overall parent entity, Belden Incorporated ("**Belden Inc.**") is headquartered in St Louis, Missouri, United States. Belden Singapore is part of the Belden Group.

4. As the main Human Resources ("**HR**") functions of Belden Singapore are conducted by Belden Inc., Belden Singapore transfers the personal data of its employees to Belden Inc., which are then stored in Belden Inc.'s servers. The terms on which the various Belden entities transfer and process personal data are governed by the Global Data Transfer Agreement dated 1 September 2020 ("**GDTA**").

5. GVSPL is part of a group of companies (the "**Grass Valley entities**") that were formerly part of the global Belden Group. In July 2020, the Grass Valley entities (including GVSPL) were acquired by another company. Under the terms of the acquisition, Belden Inc. agreed to provide transition services, including administration of its information technology and HR systems for a period of time after the acquisition. Therefore, the personal data of GVSPL's employees (and the employees of other Grass Valley entities) were transferred to Belden Inc. and stored in Belden Inc.'s servers. GVSPL's parent company, Grass Valley USA, LLC ("**GV USA**") (on behalf of its subsidiaries and affiliates, including GVSPL) and Belden Inc. entered into a Data Sharing Agreement dated 18 June 2020 ("**DSA**") to govern the sharing of data (including personal data) between the parties.

6. On 12 November 2020, the Belden Group's information technology team noticed anomalies in its systems. Subsequent investigations revealed that, from September to November 2020, a threat actor had accessed the Belden Group's servers in the USA and other jurisdictions through the use of malicious software at various times and exfiltrated the information and data contained therein. The compromise of GVSPL's Personal Data Sets is

taken to have arisen from the unauthorised access to the Belden Group's servers since there was no evidence of any unauthorised access directly into the systems of the Grass Valley entities.

7. The personal data of 126 individuals related to Belden Singapore (current and former employees as well as non-employees such as suppliers / vendors) and 63 individuals related to GVSPL (current and former employees) were exfiltrated in the Incident (collectively, the "**Personal Data Sets**"). The types of personal data exfiltrated included the following:

(a) Name;
(b) Address;
(c) Email Address;
(d) Telephone Number;
(e) Date of Birth;
(f) Identification Number;
(g) Marital Status;
(h) Photographs;
(i) Salary Information; and
(j) Individual Tax Information.

8. Upon discovery of the Incident, Belden Inc. implemented, or has been in the process of implementing, the following remediation actions:

(a) The following security measures:
    i. Conducted an audit of system administrator accounts to confirm that it was for valid users only
    ii. Reviewed and developed plan to address incident closure activities
    iii. Improved relevancy and frequency of security awareness campaign.

(b) The following short-term and long-term containment actions:

i. Roll out an endpoint security software to all server and client systems
ii. Block command and control IP addresses on perimeter firewalls
iii. Update existing security software definitions
iv. Block access to Mega (cloud storage file hosting service) on firewalls
v. Disallow syncing of data from internal systems to unapproved external cloud storage services
vi. Remove unnecessary accounts from privileged security groups
vii. Rebuild compromised systems
viii. Reboot business-critical systems that cannot be rebuilt
ix. Expedite patching of critical and high severity vulnerabilities
x. Reset passwords for Domains and Enterprise administrators
xi. Reset passwords for all other privileged users
xii. Reset the password for the Kerberos account
xiii. Perform enterprise-wide password reset
xiv. Ensured no direct remote access is available on the systems exposed to the Internet

Findings and Basis for Determination

9. As a preliminary point, Belden Inc. is responsible for maintaining the security and integrity of the Belden Group's systems (including its servers) and implementing the appropriate safeguards. However, the data protection obligations in the Personal Data Protection Act 2012 ("**PDPA**") does not apply to Belden Inc., as it does not process personal data in Singapore. It is further noted that Belden Inc. has made reports to the relevant authorities in the jurisdictions where the compromised servers are located in. Therefore, no findings are made against Belden Inc.

The Transfer Limitation Obligation under section 26 of the PDPA

10. Section 26(1) of the PDPA provides that an organisation shall not transfer any 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 "**Transfer Limitation Obligation**"). The relevant requirements are prescribed in Part III of the Personal Data Protection Regulations 2014 ("**PDPR**")[1] . In particular:

(a) Regulation 9(1)(b) of the PDPR requires an organisation that transfers personal data to a country or territory outside of Singapore to take appropriate steps to ensure that the recipient of personal data 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 that under the PDPA;

(b) Regulation 10(1)(b) of the PDPR provides for contracts to be one such legally enforceable obligation. Regulation 10(2) in turn provides that such contract must require the recipient of the transferred personal data to provide a comparable standard of protection , and must specify the countries and territories to which the personal data may be transferred under the contract; and

(c) Regulation 10(1)(c) of the PDPR provides binding corporate rules to be another such legally enforceable obligations. Regulation 10(3) in turn provides that such binding corporate rules require every recipient to provide a comparable standard of protection , and must specify (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may

[1] As the Incident occurred on or around September 2020, the Personal Data Protection Regulations 2014 apply. However, from 1 February 2021 onwards, the Personal Data Protection Regulations 2021 would apply.

be transferred under the binding corporate rules; and (iii) the rights and obligations provided by the binding corporate rules. Further, such binding corporate rules may only be used by recipients that are related to the transferring organisation.

11. To comply with the Transfer Limitation Obligation in the context of an intra-group transfer where there is centralisation of corporate functions, group members involved in ongoing relationships for regular cross-border transfers of personal data out of Singapore are required to take reasonable steps to ascertain that the overseas transferee has implemented the appropriate policies, practices and / or technical measures to ensure that the transferred personal data is provided with the requisite level of protection. This is no different from an organisation's obligation to carry out the necessary due diligence vis-à-vis the transfer of personal data to an overseas data intermediary, since the overseas transferee is a data intermediary even though they are members within the same group of companies. As stated in the Commission's Advisory Guidelines on Key Concepts in the PDPA[2]:

*"*Overseas transfers of personal data

6.22 Where an organisation engages a data intermediary to process personal data on its behalf and for its purposes, the organisation is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data. This is regardless of whether the personal data is transferred by the organisation to an overseas data intermediary or transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organisation.

6.23 The Transfer Limitation Obligation requires that an organisation ensures that personal data transferred overseas is protected to a standard comparable with the Data Protection Provisions. The onus is on the transferring organisation to

[2] Advisory Guidelines on Key Concepts in the PDPA (Rev 1 February 2021)

> undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure that it is capable of doing so. In undertaking its due diligence, transferring organisations may rely on data intermediaries' extant protection policies and practices, including their assurances of compliance with relevant industry standards or certification."

Whether Belden Singapore complied with the Transfer Limitation Obligation

12. It is determined that Belden Singapore had not complied with the Transfer Limitation Obligation for the reasons explained below.

13. At the material time, Belden Inc. and certain other Belden entities had put in place a binding intra-group contract called the Global Data Transfer Agreement dated 1 September 2020 ("**GDTA**"), which governs the terms on which the various Belden entities transfer personal data to each other.

14. The GDTA contained provisions that required Belden Inc. to provide any personal data transferred from Singapore a comparable standard of protection to that under the PDPA at the time of the Incident. In particular:

(a) Clause 5.2.2 provided that "Where Belden Data and/or Client Data originating in a Non-EEA territory (including in the United Kingdom, if at any time the United Kingdom is not in the EEA or beyond any transition period) (the Originating Territory") are Processed in a territory which is different from the Originating Territory (the "Importing Territory"), then the Data Importer will Process such Belden Data and/or Client Data to a standard consistent with the Applicable Privacy Law(s) of the Originating Territory…"

(b) Clause 19.5.5 of Schedule 5 required the data importer (i.e. Belden Inc.) to ensure that any transfer of personal data to a country or territory outside Singapore is provided a standard of protection that is comparable to the protection under the PDPA.

15. In addition to the above, the GDTA also contained provisions that require the transferee (the "Data Importer") to implement measures aimed at addressing identified security risks to the personal data transferred and assisting the transferor (the "Data Exporter") to comply with the relevant data protection laws. In particular:

(a) Clause 4.1(c)(ii) required the Data Importer to "comply with any requirements arising under any Applicable Privacy Law(s) to protect the Belden and/or Client Data it received including, but not limited to the following:

(A) assistance, taking into account the nature of the Processing, by appropriate technical and organisation measures, insofar as this is possible, to fulfil any obligations the Data Exporter may have to respond to requests from data subjects to exercise their rights under Applicable Privacy Law(s) assistance;

(B) assisting the Data Exporter as necessary to comply with its obligations under Applicable Privacy Law(s) including (without limitation) to conduct a data protection impact assessment and/or to consult with a Supervisory Authority, in each case taking into account the nature of the Processing and the information available to the Data Importer; and

(C) not knowingly performing its obligations under this Agreement in such a way as to cause the Data Exporter to breach any of its obligations under Applicable Privacy Law(s);

(D) ensuring the reliability of any persons it authorises to access the Belden and/or Client Data (including employees, agents and sub-Processors) and ensure that they have undergone appropriate training in the care, protection and handling of Belden and/or Client Data;

(E) it will ensure that any persons authorised to process the Belden and/or Client Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(F) it will maintain appropriate and sufficient technical and organisational security measures to protect such Belden and/or Client Data against a Security Breach. Such measures will include as a minimum the Belden Security Measures; and

(G) it will permit the Data Exporter such access to its premises, computer and other information systems, records, document and agreements as the Data Exporter may reasonably require to satisfy itself that the Data Importer is complying with its obligations under the Agreement; and

(H) it will, at the choice of the Data Exporter, delete or return all Belden and/or Client Data to the Data Exporter after the end of the provision or services relating to processing, unless EU law or any EU Member State law requires storage of the Client Data."

(b) Clause 6 also required the Data Importer to carry out certain measures in the event of a security breach to investigate the breach, mitigate its effects and assist the Data Exporter to fulfill any obligations under the Applicable Privacy Law(s).

16. In this connection, the Belden Group has put in place the following policies and measures concerning the treatment of personal data:

(a) **Data Handling Standard** – Governs the handling of electronic and physical data throughout the Belden Group;

(b) **Personal Data Handling Standard** – Governs the handling of all forms of personal data throughout the Belden Group;

(c) **Data Classification Policy** – Sets the standards for protection of information assets from accidental or unlawful destruction, loss, unauthorised access, modification, compromise, disclosure or other misuse; and

(d) **Record Creation, Retention, Retrieval and Disposal Policy** – Establishes requirements for creating, retaining, retrieving and disposing of records within the Belden Group.

17. Despite the suite of policies and technical measures adopted by the Belden Group, the GDTA and the above policies did not enable Belden Singapore to meet the requirements in Regulation 9(1)(b), read with Regulations 10(1)(b) and 10(2) when the Incident occurred:

(a) The GDTA was not legally binding on Belden Singapore at the material time as Belden Singapore had not acceded to the GDTA. For Belden Singapore to be bound by the GDTA, it must have executed a Deed of Accension under Clause 12.1. However, at the time of the Incident, Belden Singapore had not executed such a Deed of Ascension.

(b) Since the Belden Group opted to structure its data governance architecture around an intra-group contract (i.e. the GDTA), it is trite that the principle of privity of contracts applies, and only the parties to a contract are able to enforce the rights and obligations arising therein. Although the GDTA did, at the time of the Incident, require Belden Inc. to comply with the applicable standards under the PDPA while importing / processing personal data from Singapore (Clause 19.5.5 of Schedule 5), such obligations were not legally enforceable by Belden Singapore. Absent such a mechanism, Belden Singapore had no legal means to ascertain and ensure that the data transferred outside Singapore was afforded the same level of protection as under the PDPA.

(c) Belden Singapore has acknowledged that this was a lapse. It subsequently rectified this oversight by signing a Deed of Accession on 18 June 2021.

(d) Nevertheless, the investigations revealed that, in practice, all the relevant Belden group policies, practices and technical measures mentioned in paragraphs 14 to 16 were implemented in full to ensure that personal data transferred from Singapore are afforded a level of protection comparable to that provided under the PDPA. Therefore, Belden Singapore's breach constituted a lapse in legal formalities rather than a failure to comply with the substance of the Transfer Limitation Obligation.

Whether GVSPL complied with the Transfer Limitation Obligation

18. GVSPL was determined to have complied with the Transfer Limitation Obligation for the reasons explained below.

19. At the material time, GVSPL (as a subsidiary of GV USA) and Belden Inc. was bound by a Data Sharing Agreement dated 18 June 2020 ("**DSA**"), which governed the terms on which GVSPL transferred personal data to Belden Inc. The DSA is in compliance with Regulation 9(1)(b), read with Regulations 10(1)(b) and 10(2) of the PDPR. Clause 10.1 of the DSA provided that, in the case of international transfers of data (including personal data):

> "The Receiving Party shall not process any Data (not permit any Data to be processed) in a territory outside of the European Economic Area ("EEA") unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law[3]. Such measures may include (without limitation); (a) transferring the Data to a recipient in a country that the European Commission has decided provides

[3] Defined to mean "all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU Data Protection Law."

adequate protection for personal data; (b) to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law; (c) to a recipient in the United States that maintains a valid and up-to-date EU-US Privacy Shield certification or (d) to a recipient that has executed standard contractual clauses adopted or approved by the European Commission or by virtue of entering into this Agreement."

20. Whilst Clause 10.1 of the DSA does not mention the PDPA specifically, it does require a Grass Valley entity (including GVSPL) to take measures as are necessary to ensure the transfer is in compliance with the Applicable Data Protection Law, which – in the context of GVSPL – is the PDPA.

21. Additionally, the DSA also contains several provisions aimed at addressing identifiable security risks posed to the transferred personal data as well as ensuring that the Receiving Party assists the Disclosing Party. In particular:

(a) Clause 6.1(c) required the Receiving Party to assist the Disclosing Party as necessary to comply with its obligations under the Applicable Data Protection Law (defined to mean all worldwide data protection and privacy laws and regulations application to the personal data in question) including (but not limited to) conducting any data protection impact assessments, consultation with a supervisory authority and fulfilment of any obligations the Disclosing Party may have to respond to requests from data subjects to exercise their rights under the Applicable Data Protection Law;

(b) Clause 6.1(d) required the Receiving Party to ensure that any persons authorised to process the personal data to have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and

(c) Clause 7.1 provided that the Receiving Party "shall maintain appropriate and sufficient technical and organisational security measures to protect the Data against a Security Incident, taking into account state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of the data subject(s)". Clause 7.2 further stipulates certain actions that the Receiving Party is required to take in the event of a confirmed Security Incident to mitigate the effects of the incident and assist the Disclosing Party to fulfill any obligations under the Applicable Data Protection Law.

22. Finally, the group policies and measures concerning the treatment of personal data enumerated in paragraph 16 also applied to the transfers from GVSPL within the Belden Group.

The Deputy Commissioner's Decision

23. In light of Belden Singapore's breach of the Transfer Limitation Obligation, the Commission is empowered under section 48I of the PDPA to issue Belden Singapore such directions as it deems fit to ensure compliance with the PDPA. This may include directing Belden Singapore to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

24. In considering whether a direction should be given to Belden Singapore in this case, it is noted that:

(a) It was an oversight that Belden Singapore did not sign a Deed of Accession prior to the Incident, and this lapse has been rectified by the signing of the Deed of Ascension.

(b) Belden Singapore's breach of the Transfer Limitation obligation was technical, and a failure of legal formalities that was not substantive in nature. As stated in paragraph 17(d), at the operational level, the suite of Belden group policies, practices and technical measures implemented were sufficient to ensure that personal data transferred from Singapore to Belden Inc. were afforded a level of protection comparable to that provided under the PDPA.

25. Having considered all of the above circumstances, Belden Singapore is administered a warning in respect of its breach of the Transfer Limitation Obligation. No other directions are necessary in view of the remedial actions already taken, namely, Belden Singapore's accession to the GDTA.

YEONG ZEE KIN

DEPUTY COMMISSIONER

FOR PERSONAL DATA PROTECTION