PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 7

Case No: DP-2103-B8147 / DP-2206-B9935

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

And

(1) Supernova Pte Ltd
(2) Shopify Commerce Singapore Pte Ltd

… *Organisation*

DECISION

Supernova Pte Ltd & Anor

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2103-B8147/ DP-2206-B9935

6 October 2022

Introduction

1 On 8 October 2020, the Personal Data Protection Commission (the "**Commission**") was notified by Supernova Pte Ltd ("**SNPL**") of a data breach incident of Shopify Inc's database affecting the personal data of certain Singapore-based customers (the "**Incident**"). The Commission commenced investigations to determine whether the circumstances relating to the Incident disclosed any breaches of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

Background

2 Shopify Inc ("**Shopify**") is a company based in Canada that operates an e-commerce platform for online retailers to conduct sales (the "**Platform**"). SNPL is an online retailer that began using the Platform in 2018 to sell its products to customers. Shopify provided payment processing and other services (the "**Services**") to SNPL pursuant to the Shopify Plus Agreement, executed by Shopify and SNPL on 4 December 2018. Shopify Commerce Singapore Pte Ltd ("**Shopify SG**") acted as the

Asia-Pacific data sub-processor of Shopify pursuant to the Shopify Data Processing Addendum to the Shopify Plus Agreement, and its role was confined to collecting customer personal data (including SNPL's) via the Platform and transferring the data out of Singapore to Shopify for both Purchase Processing and Platform Processing.

3 The Platform collected personal data from customers of its online retailers for two broad sets of purposes. First, to facilitate billing, payment and shipping on behalf of the Platform's online retailers ("**Purchase Processing**"). Second, for Shopify's own commercial and administrative purposes. This mainly included the collection of consumer personal data through the Platform's own consumer-facing applications and services e.g. Shop Pay (collectively, "**Platform Processing**"). Granted, for Platform Processing, users of the Platform included customers of merchants who are on the Platform, such as SNPL's customers. Nevertheless, customer personal data was being collected and processed by Shopify for its own purposes, and not on behalf of merchants.

4 On 1 July 2019, the Shopify Plus Agreement (including the Shopify Data Processing Addendum) was assigned to Shopify SG (the "**Assignment**"). At the material time, SNPL had no knowledge of the Assignment as no notice of assignment was required. Consequently, the relationship between the parties was reconfigured in the following manner:

(a) For **Purchase Processing**, Shopify SG became the data intermediary of SNPL, and was responsible for processing personal data on behalf of SNPL.

The flow of SNPL's customer personal data did not change - Shopify SG continued to collect SNPL's customer personal data and transferred this to Shopify to carry out Purchase Processing on its behalf.

(b) For **Platform Processing**, Shopify SG became the data controller of the customer personal data collected through the Platform and its customer-facing applications, including the personal data of the customers of merchants who use the Platform (such as SNPL). In such circumstances, personal data from such users are collected by Shopify SG and processed for its purposes and not on behalf of the merchants. The flow of customer personal data also did not change, as Shopify SG continued to transfer personal data of users of its Platform to Shopify to carry out Platform Processing.

The Incident

5 Between June to September 2020, two Philippines-based service contractors of Shopify that were engaged through a third party, illegally accessed and exfiltrated certain customer personal data stored in Shopify's systems, which had been collected via the Platform for Purchase Processing (the "**Incident**"). This included customer personal data of SNPL. Shopify became aware of this on 15 September 2020 and informed SNPL on 18 September 2020.

6 The customer personal data affected in the Incident included full names, email addresses, billing addresses, shipping addresses, phone numbers, bank identification

numbers, IP addresses, last 4 digits of the customer payment cards, and purchase histories of 23,928 individuals.

Findings and Basis for Determination

7 Neither SNPL nor Shopify SG were responsible for the security of Shopify's systems in Canada holding the personal data affected in the Incident. Nevertheless, both organisations were bound by section 26 of the PDPA.

Transfer limitation obligation under section 26 of the PDPA

8 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 requirements applicable to the aforementioned transfers of personal data from SNPL and Shopify SG to Shopify were those prescribed in Part III of the Personal Data Protection Regulations 2014 ("**PDPR 2014**")[1]. In particular:

(a) Regulation 9(1)(b) of the PDPR 2014 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 the personal data is bound by legally

[1] The PDPR 2014 governs the transfers of personal data prior to 1 February 2021. Transfers of personal data after 1 February 2021 are governed by the Personal Data Protection Regulations 2021.

enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA; and

(b) Regulation 10(1)(b) and 10(1)(c) provide that such legally enforceable obligations include may be imposed on the recipient by contract or binding corporate rules (subject to Regulation 10(2) and 10(3) respectively).

Breach of the Transfer Limitation Obligation by SNPL

9 When SNPL entered into the Shopify Plus Agreement on 4 December 2018, it was aware that by using the Platform its customer personal data would be transferred to Shopify, which was outside Singapore, for Purchase Processing. Shopify was SNPL's data intermediary, whilst Shopify SG was Shopify's data sub-processor as explained in paragraph 2.

10 SNPL (as the data controller of its customers' personal data) had been notified, in the Shopify Plus Agreement, that its customer personal data may be transferred out of Singapore for the purpose of Purchase Processing, and was obligated to comply with the Transfer Limitation Obligation vis-à-vis the personal data collected by Shopify / Shopify SG for Purchase Processing. Section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself. Such obligations include the

Transfer Limitation Obligation. As stated in the Commission's Advisory Guidelines on Key Concepts in the PDPA[2]:

"*Considerations for organisations using data intermediaries*

6.20 Section 4(3) provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself. As such, **it is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA.**

…

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**

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

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 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.**"

(emphasis added)

11 The Transfer Limitation Obligation required SNPL to ensure, prior to transferring customer personal data for processing by Shopify, that Shopify provided a standard of protection to transferred personal data that was comparable to the protection under the PDPA. This obligation did not abate by virtue of the Assignment on 1 July 2019, even though SNPL claimed that it was not made aware of the Assignment. At all times, SNPL was responsible for complying with the Transfer Limitation Obligation for its transfer to Shopify (initially) and Shopify SG (latterly). Even though Shopify SG assumed legal responsibility as SNPL's data intermediary

supposedly without informing SNPL, the flow of SNPL's customer personal data was not altered, as Shopify SG continued to transfer SNPL's customer personal data outside of Singapore (i.e. to Shopify) for Purchase Processing.

12 In connection with this, the onus laid with SNPL to put in place the relevant contractual clauses to ensure the protection of its personal data to a standard comparable to the PDPA. However, investigations revealed that SNPL did not do so. The omission to put in place contractual clauses to ensure such comparable protection began with the start of their commercial arrangement. SNPL stated that, in 2018, it carried out a due diligence assessment of Shopify's approach to data protection before entering into the Shopify Plus Agreement and migrating its online retail activities to the Platform ("**2018 Due Diligence Exercise**"). However, this assessment was inadequate as it failed to ensure that there were binding contractual clauses requiring personal data transferred between them to be protected to a standard comparable to the PDPA.

13 Accordingly, SNPL failed to comply with the Transfer Limitation Obligation.

Breach of the Transfer Limitation Obligation by Shopify SG

14 For the Purchase Processing of customer personal data discussed in the preceding paragraphs, Shopify SG acted as SNPL's data intermediary and was thus not bound by the Transfer Limitation Obligation.

15 However, Shopify SG must also comply with the Transfer Limitation Obligation in relation to the personal data collected for Platform Processing. This is because Shopify SG was processing customer personal data for its own purposes, and was thus the data controller, while Shopify is the data intermediary.

16 In connection with this, investigations revealed that there were no legally binding obligations, in the form of contracts or binding corporate rules within the Shopify group, requiring Shopify to provide PDPA-comparable protection to personal data transferred from Shopify SG to Shopify for processing. While the Shopify Data Processing Addendum makes references to certain data protection legislation applicable to the European Union and the State of California, it did not cover the PDPA. During the course of investigations, Shopify indicated that it would "be putting in place binding corporate rules governing the transfer of merchants' customers' data between group entities" and furnished a draft APAC Cross-Border Whitepaper to the Commission. Whilst this was a step in the right direction, it did not retrospectively allow Shopify SG to regularise its intra-group data transfers to ensure compliance with the Transfer Limitation Obligation at the material time.

17 In view of the foregoing, Shopify SG failed to comply with the Transfer Limitation Obligation in respect of Platform Processing of personal data.

The Deputy Commissioner's Directions

18 In determining what directions (if any) should be given to the organisations pursuant to section 48I of the PDPA, and/or whether the Organisation should be

required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA were considered. In particular, the Commission placed emphasis on the fact that SNPL and Shopify SG had been highly cooperative with the Commission's investigations.

19 On 18 July 2022, SNPL made representations to the Commission requesting for additional time to comply with the above direction. In consideration of SNPL's limitations as a small and medium enterprise, SNPL's deadline to comply with the direction is extended from 60 days to 6 months.

20 Having considered all the relevant factors of this case, SNPL is hereby directed to take the following actions:

(a) SNPL is to put in place within 6 months a process to ensure compliance with the Transfer Limitation Obligation under section 26 of the PDPA in any future engagement of services that may involve the processing of personal data outside of Singapore on behalf of SNPL; and

(b) Shopify SG is to put in place within 60 days a process to ensure compliance with the Transfer Limitation Obligation under section 26 of the PDPA in any future engagement of its services that may involve the processing of personal data outside of Singapore.

21 Specific to SNPL's transfer of personal data for the purpose of Purchase Processing to Shopify in Canada, the following observations may be helpful. The

Association of Southeast Asian Nations ("**ASEAN**") adopted and endorsed the Model Contractual Clauses ("**ASEAN MCCs**"), which are meant to facilitate cross-border transfers of personal data. These provide a standard for business-to-business (B2B) transfers that can be used by enterprises of any scale, but are especially helpful for small and medium enterprises. When using them, businesses may adapt these clauses as necessary for their commercial arrangements.

22 The Commission recognises the ASEAN MCCs as meeting the requirements of the Transfer Limitation Obligation under the PDPA: see PDPC's *Guidance for the Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore* (published 22 January 2021). Using the ASEAN MCCs can ease B2B transfers between Singapore and other jurisdictions such as Canada. In carrying out the directions, SNPL may therefore wish to consider relying on and adapting, as necessary, the ASEAN MCCs.

YEONG ZEE KIN

DEPUTY COMMISSIONER

FOR PERSONAL DATA PROTECTION