Bud Cosmetics Pte Ltd

[2019] SGPDPC 1

Tan Kiat How, Commissioner — Case No DP-1704-B0660

Data Protection – Protection Obligation – Disclosure of personal data – Insufficient security arrangements

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

Data Protection – Openness obligation - Requirement to develop and implement policies and practices and communicate these policies and practices to staff

3 January 2019.

1 On 6 April 2017, the Personal Data Protection Commission (the "**Commission**") received a complaint from an individual (the "**Complainant**") in relation to the publication of a list of approximately 2,300 of the Organisation's members ("**Member List**") containing their personal data on the Internet (the "**Incident**") and commenced investigations thereafter.

2 The Commissioner sets out below its findings and grounds of decision based on the investigations carried out in this matter.

Material Facts

3 The Organisation is an organic and natural skincare retailer specialising in natural skin care brands with retail outlets in Singapore and an online store that it operates and manages at www.budcosmetics.com (the "**Website**"). Since 2007, the Organisation has been collecting customer information for membership registration. At the time of the Incident, all customers who wished to purchase items from the Organisation's Website were required to set up a membership account.

4 As a matter of practice, the Organisation maintained two separate membership databases. The first database was for customers who registered to become members on its Website, which was kept in the SQL database and stored on the host server (the "**Online Database**"), while the second database was for customers who registered in person at the Organisation's retail outlets (the "**Offline Database**").[1] The Offline Database was provided by the Organisation's vendor as part of its point-of-sale system. At all material times, the Online and Offline Databases were not consolidated but were kept and updated separately. Personal data extracted from the Offline Databases was not stored in any folders linked to the Website. The Online Database contained approximately 1,132 members in 2012. At the time of the investigation, the Organisation represented that there were approximately 2,457 registered members on the Online Database.

5 As part of its marketing strategy, the Organisation prepared and sent its customers e-newsletters with information about its products and the latest

[1] At the time of the investigation, the Organisation represented that there were approximately 5,000 registered members on the Offline Database.

promotional offers. A customer mailing list for each e-newsletter was generated by selecting members' email addresses from both the Online and Offline Databases based on certain criteria. When generating this list, the Organisation would only extract email addresses from both the Online and Offline Databases. They would not extract the other types of personal data and combine the records into a masterlist; the Organisation confirmed that apart from the email addresses for the purposes of sending out marketing newsletters, it did not combine the datasets from the Online and Offline databases. To reduce the file size of each e-newsletter, the Organisation intentionally kept the images embedded in the e-newsletters in publicly accessible image folders. Once an e-newsletter was sent out, the customer mailing list for that particular e-newsletter would be kept in an archive folder. The image folders and customer mailing lists were managed and generated by the owner of the Organisation.

6 On or around 6 April 2017, the Complainant, who was a member of the Organisation, discovered a URL link to the Member List in the search results when she conducted a search using her name on the Internet. The Member List contained the following personal data of approximately 2,300 members:

(a) name;

(b) date of birth;

(c) contact number;

(d) email address; and

(e) residential address.

7 The Member List was located in the image folder for an e-newsletter that was sent out in 2012 ("**2012 Image Folder**"). At the time, the 2012 Image

Folder was hosted on SmartyHost Pty Ltd's ("**SmartyHost**") servers based in Australia. However, following a cyberattack incident on SmartyHost's "osCommerce" system in April 2012 ("**2012 Cyberattack Incident**") and unplanned server outages which resulted in website downtime, the Organisation switched web hosting companies in 2013 and engaged Just Host Inc ("**Just Host**"), a United States ("**US**") based company with servers located in Provo, Utah.

8 After it was notified of the Incident, the Organisation deleted the Member List from the 2012 Image Folder as well as the e-newsletter image folders created from 2006 to 2016. The Organisation also sought to improve the security of its Website by activating "Sitelock", an add-on feature offered by Just Host which conducts daily scans of its Website for vulnerabilities and malware.

Cause of the Incident

9 Investigations found that search engines were able to access and index the URL link to the Member List contained in the 2012 Image Folder because the 2012 Image Folder was unsecured. The Organisation represented that, prior to the notification from the Commission, it was unaware of the existence of the Member List, or how it ended up in the 2012 Image Folder. However, it hypothesised that the Member List may have been inserted into the 2012 Image Folder as a result of the 2012 Cyberattack Incident as that was the only known occasion in 2012 where the Organisation had encountered problems with its Website. In the 2012 Cyberattack Incident, hackers exploited a vulnerability in SmartyHost's osCommerce system to send spam emails via the "tell-a-friend" function on the system.

10 Having considered the evidence and findings of the investigation, the Commissioner is not convinced by the Organisation's hypothesis. The vulnerability of the "tell-a-friend" feature does not appear to be in any way connected to the unauthorised extraction of data from the Online Database. More pertinently, the claim that the Incident had occurred in 2012 seems improbable given that the number of members contained in the Member List exceeded the number of online-registered members in 2012 (when they had only approximately 1,132 members). While the Member List could possibly be a combination of 2012-registered members of both the Online and Offline Databases, it is unlikely to be the case as the Organisation had not combined both Databases (save for the combination of email addresses for the mailing list) or linked the Offline Database to the Website such that an exploitation of the "tell-a-friend" feature could have led to the access of the Offline Database.

Findings and Basis for Determination

11 The main issues for determination are:

(a) whether the Organisation complied with its obligations under section 12(a) of the PDPA;

(b) whether the Organisation breached section 24 of the PDPA; and

(c) whether the Organisation complied with its transfer limitation obligation under section 26 of the PDPA.

12 There was no question or dispute that the data disclosed in the Member List was "personal data" as defined in section 2(1) of the PDPA as it was clearly possible to identify an individual from that data.

13 In this regard, although the Member List contained personal data that was collected before the PDPA came into full force on 2 July 2014 ("**Appointed Day**"), as the Organisation continued to use the personal data after the Appointed Day, it was incumbent on the Organisation to take proactive steps to comply with its obligations under the PDPA in respect of not only new personal data that may come into its possession or control but any existing personal data held in its possession or control.[2]

14 As the Commissioner highlighted in *Re Social Metric Pte Ltd* [2017] SGPDPC 17 (at [11]):

> This means that, for example, if there were no security arrangements previously to protect the existing personal data the organisation was holding, the organisation has a positive duty to put in place security arrangements after the Appointed Day. It was not enough for the organisation to leave things *status quo*, if this would not enable the organisation to meet the requirements and standards of the Protection Obligation. As provided in Section 24 of the PDPA, the security arrangements must be "reasonable".
>
> [Emphasis added.]

15 Accordingly, the Organisation was under an obligation to comply with the data protection provisions under the PDPA in respect of both personal data that was collected before and after the Appointed Day.

Whether the Organisation breached section 12(a) of the PDPA

16 Section 12(a) of the PDPA imposes an obligation on organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. Organisations are also

---

[2] See *Re Social Metric Pte Ltd* [2017] SGPDPC 17 at [10].

required to communicate to its staff information about such policies and practices.

17 The Organisation represented that it had a privacy policy on its Website ("**Privacy Policy**") at the time of the Incident. However, the Privacy Policy (which was last updated in December 2006) only notified customers as to how the Organisation will use and process their personal data and did not set out any procedures or practices as to how the Organisation and its employees should handle and protect the personal data in their possession or under their control.

18 In any case, by the Organisation's own admission, prior to being notified by the Commission, the Organisation was under the impression that the PDPA only prohibited organisations from sending marketing messages to Singapore telephone numbers that were registered with the Do Not Call ("**DNC**") Registry. The Organisation confirmed[3] that it did not implement any data protection policies or practices in respect of the personal data in its possession or under its control as it was not aware of its Data Protection Obligations under the PDPA.[4] In response, to questions on the Organisation's data protection policies and practices, the Organisation responded that the questions were "(n)ot applicable as we do not currently have a policy/ procedure document. However, we would appreciate any assistance in drafting such a policy document for our staff".

19 For completeness, the investigations found that the Organisation had begun drafting a new Data Protection Policy prior to the Incident in February 2017, when it claimed to be unaware of its Data Protection Obligations.

---

[3] See the Organisation's response to the Commission's Notice to Produce dated 10 May 2017 at [2.8].

[4] Under Parts III to VI of the PDPA.

However, on balance, the Commissioner accepts the Organisation's representation that it had only drafted the Data Protection Policy because "*during our research of other major local beauty retailer websites we noticed the section on Data Protection Policy section [sic.] on their websites. Hence we thought we should include a similar detailed policy on ours*". The new Data Protection Policy was only implemented after the Incident in June 2017, when the Organisation launched its new Website.

20 In this regard, it is a trite principle of law that ignorance of the law is no excuse. The Organisation's lack of awareness of its obligations under the PDPA cannot excuse its breach of the PDPA and is not a legitimate defence to a breach.[5] It bears repeating that the development and implementation of data protection policies is a fundamental and crucial starting point for organisations to comply with their obligations under the PDPA. As the Commissioner highlighted in *Re Aviva Ltd* [2017] SGPDPC 14 (at [32]):

> Data protection policies and practices developed and implemented by an organisation in accordance with its obligations under section 12 of the PDPA are generally meant to increase awareness and ensure accountability of the organisation's obligations under the PDPA.

21 Data protection training is also an effective and necessary mode of communicating the Organisation's policies and practices and is a key aspect of the Openness Obligation under section 12 of the PDPA.[6] Employees will only be able to protect personal data if they are first able to recognise when a matter requires data protection considerations. In this regard, the Commissioner agrees

---

[5] *M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 (at [16]).

[6] See *Re Habitat for Humanity Singapore Ltd* [2018] SGPDPC 9 (at [14]).

(*cont'd on next page*)

with the following observations in the Joint Guidance Note issued by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia:[7]

> Training and general education on privacy are very important. Our Offices have seen instances where issues were not identified as privacy issues when they should have been. As a result, appropriate steps were not taken to prevent or address privacy breaches. In other cases, we have seen a lack of awareness or appreciation for privacy risks on the part of employees result in the development of products or services that were not compliant with applicable privacy law. In Alberta, human error is the most common cause of reported breaches resulting in a real risk of significant harm to an individual. Examples include: misdirected faxes and mail, e-mail addresses viewable in mass e-mails, inappropriate disposal of documents, and disclosure of passwords.
>
> Employees will be able to better protect privacy when they are able to recognize a matter as one that involves personal information protection.
>
> [Emphasis added.]

22 However, apart from instructing its employees on the requirements under the DNC provisions of the PDPA,[8] the Organisation did not provide any formalised data protection training for its employees. Accordingly, the Commissioner finds that the Organisation had breached section 12(a) of the

---

[7] Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia, Getting Accountability Right with a Privacy Management Program <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/> at p 13.

[8] In this regard, the Organisation represented that it had instructed the members of its sales team to ensure that they require customers to indicate if they want to be contacted by the Organisation when they sign up to be a member and to inform the customer that their data will not be sold or offered to any third party. The Organisation also represented that it only sent text messages via SMS to customers whose numbers were not on the DNC Registry.

PDPA given that at the time of the Incident the Organisation did not develop and implement a data protection policy as necessary for it to meet its obligations under the PDPA.

Whether the Organisation breached section 24 of the PDPA

23 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Member List containing the personal data of the Organisation's online-registered members was located in an image folder that belonged to and was at all material times controlled by the Organisation. Accordingly, the Commissioner finds that the Member List was in the Organisation's possession. The Organisation was also in control of the personal data as it had the ability, right and/or authority to determine what personal data was required to provide its services and the purposes for, and the manner in which it was collected, used and disclosed.[9] Such control was demonstrated when it generated the respective e-newsletter customer mailing lists and when it deleted the Member List upon being notified of the Incident.

24 While the cause of the Incident cannot be determined with certainty after investigations, the fact remains that the Member List was generated and inserted into the 2012 Image Folder. The common law maxim *res ipsa loquitur* applies even though the Organisation showed a clear lack of knowledge of how and

[9] The meaning of control as set out in *AIG Asia Pacific Insurance Pte. Ltd* [2018] SGPDPC 8 at [18].

when this happened. As the Website administrator, the Organisation was responsible for ensuring the security of the Website such as by conducting periodic penetration testing or vulnerability assessments and ensuring that any vulnerabilities are reviewed and promptly fixed to prevent data breaches. However, by the Organisation's own admission, prior to being informed of the Incident, the Organisation never considered the adequacy of the security of its Website or information technology system ("**IT system**") and did not put in place any security arrangements to protect the personal data in its possession or under its control. At the time of the Incident, the Organisation had never conducted any vulnerability scans or penetration tests to ensure that its Website was sufficiently protected.

25 As mentioned above, the Organisation was unaware of its Data Protection Obligations under the PDPA at the time of the Incident and therefore did not have any policies or procedures in place to guide its employees regarding the collection, use and disclosure of personal data in its possession or under its control. Consequently, the Organisation did not implement any checks and controls to prevent or minimise the risk of unauthorised disclosure of personal data. By way of example, the Organisation failed to implement procedures for the generation of Member List, use of Member List for sending e-newsletters and deletion of Member List after e-newsletters have been sent. Given the Organisation's practice of retaining the publicly accessible e-newsletter image folders for extended periods, proper housekeeping should have been conducted to ensure that all publicly accessible folders did not contain extraneous files, including stray copies of Member List.

26 As mentioned in the Guide to Securing Personal Data in Electronic Medium, managing info-communication technology systems security and risks

related to data breaches requires good governance. It is a good practice for organisations to:

> "Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose the data (refer to section 8). If there is a need to retain the data but not in identifiable form, e.g. for performing data analytics, consider anonymising the data." [10]

27 In light of the absence of any security arrangements to protect the personal data from unauthorised disclosure, the Commissioner finds that the Organisation has contravened section 24 of the PDPA.

Whether the Organisation breached section 26 of the PDPA

28 Under section 26 of the PDPA, unless otherwise exempted,[11] 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 regulations issued under the PDPA specify the conditions under which an organisation may transfer personal data outside Singapore.

29 In particular, regulation 9(1) of the Personal Data Protection Regulations 2014 provides that an organisation must take appropriate steps to:

---

[10] Guide to Securing Personal Data in Electronic Medium at [4.1].

[11] A transferring organisation is taken to have satisfied the requirements 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 in the situations set out in regulation 9(3) of the Personal Data Protection Regulations 2014.

(a) ensure that the transferring organisation will comply with the Data Protection Obligations under the PDPA, in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation; and

(b) ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations[12] to provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

30 In this regard, it was not disputed that the Organisation had engaged SmartyHost and Just Host to host its Website and the Online Database. As mentioned above, SmartyHost was based in Australia and Just Host is based in the US. Both companies had servers located outside Singapore.

31 While personal data collected and transferred overseas before the Appointed Day are not subject to the obligations under the PDPA, a substantial portion of the personal data in the Online Database was collected and transferred to Just Host's servers located in the US after the Appointed Day, and are therefore subject to the Transfer Limitation Obligation under the PDPA. Specifically, the number of members in the Online Database had increased from 1,635 members on 29 December 2014 to 2,457 members on 10 April 2017.

32 By engaging the services of Just Host to host its Website and Online Database on its server in the US, the Organisation had effectively transferred personal data outside Singapore. However, as the Organisation was not aware

[12] As defined under regulation 10 of the Personal Data Protection Regulations 2014.

of the transfer limitation requirement under the PDPA, the Organisation admitted that it did not ask or even consider the location of the web hosting company's servers to be a relevant factor when it engaged Just Host to provide web hosting services. The Organisation therefore failed to undertake the most fundamental step of considering whether US federal and state laws provided protection comparable to the PDPA. It is not necessary for the Commissioner to venture any opinion whatsoever on the issue of whether US law provided comparable protection in order to find that the Organisation, having been ignorant of its obligation to do so, had in fact failed to undertake the most fundamental step of considering this issue. This omission is sufficient, *ipso facto*, to put the Organisation in breach of section 26 of the PDPA.

33 Had the Organisation undertaken the fundamental step of considering whether US law provided comparable protection, it could have arrived at two possible conclusions. First, it may decide that there is no further requirement for it to impose any additional safeguards by contract as it concluded that US law provided comparable protection. Second, it may decide that there are areas that US law does not provide comparable protection and it may then impose contractual obligations on Just Host to ensure that it provided a standard of protection comparable to the PDPA in respect of the personal data transferred. Needless to say, the Organisation never reached this set of considerations since it omitted to even undertake the most fundamental step.

34 In this regard, organisations that choose to engage IT vendors that are either located overseas or have servers located outside Singapore are reminded of their obligations under section 26 of the PDPA. If the personal data of individuals have to be transferred from Singapore to the overseas destination, organisations will need to ascertain whether and ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligations to

provide the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

35 Therefore, by the Organisation's own admission, the Commissioner finds that the Organisation failed to discharge its duties under section 26 of the PDPA.

Representations

36 The Organisation made representations for a reduction in the quantum of the financial penalty as set out below at paragraph 38(a) on the basis that the retail industry is facing a financial downturn. The financial information adduced by the Organisation to justify its request did not show any significant drop in income. Having duly considered the matters raised in the representations, the Commissioner has decided to maintain his decision on the quantum of the financial penalty.

The Commissioner's Directions

37 Having found that the SCA is in breach of sections 12(a), 24 and 26 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as it deems fit to ensure compliance with the PDPA.

> (a) to pay a financial penalty of S$11,000 within 30 days from the date of this direction, failing which, interest at a rate specified in the Rules of Court in respect of judgment debts, shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full;

(b) to engage duly qualified personnel to conduct a security audit of its Website and IT system and furnish a schedule stating the scope of risks to be assessed and the time within which a full report of the audit can be provided to the office of the Commissioner within 30 days from the date of this direction;

(c) to develop an IT security policy to guide its employees on the security of personal data on its Website and IT system within 60 days from the date of completion of the above security audit; and

(d) to implement a training policy for employees of the Organisation handling personal data to be trained to be aware of, and to comply with the requirements of the PDPA when handling personal data; and to require all employees to attend such training within 90 days from the date of this direction.

YEONG ZEE KIN
DEPUTY COMMISSIONER
[FOR COMMISSIONER] FOR PERSONAL DATA PROTECTION
