PERSONAL DATA PROTECTION COMMISSION

[2017] SGPDPC 15

Case No DP-1612-B0418

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

And

M Stars Movers & Logistics Specialist Pte Ltd

… *Organisation*

GROUNDS OF DECISION

M Stars Movers & Logistics Specialist Pte Ltd

[2017] SGPDPC 15

Yeong Zee Kin, Deputy Commissioner— Case No DP-1612-B0418

15 November 2017

Background

1 This case highlights the risks that organisations face when they fail to develop and implement policies, practices and procedures to protect personal data when communicating with its customers or other individuals through social media.

2 In this matter, a customer (the "**Complainant**") of the Organisation, which provides professional moving services, alleged that the Organisation had disclosed her personal data on its Facebook page without her consent.

3 The findings and grounds of decision based on the investigations carried out in this matter are set out below.

Material Facts

4 Sometime in December 2016, the Complainant engaged the Organisation's professional moving services. The Complainant voluntarily provided her name, mobile number and residential addresses (i.e. the addresses where the items were to be picked up and delivered to) to the Organisation to provide the services.

5 Dissatisfied with the allegedly unsatisfactory services provided by the Organisation, the Complainant left a negative review in a public post on the Organisation's Facebook page. Amongst other things, there was a disagreement as to when the Organisation was required to return the S$100 deposit to the Complainant.

6 The Organisation publicly responded to the Complainant's review in the comment section of the Complainant's post on its Facebook page. In its response, the Organisation identified the Complainant by her English name and surname ("**name**") and residential address (collectively referred to as the "**Personal Data**") and informed the Complainant that she would receive her deposit once she returned the carton boxes that the Organisation had previously provided to her to assist her in moving her belongings.

7 Shortly after the Organisation had disclosed the Complainant's Personal Data on its Facebook page, the Complainant sent the Organisation a private Facebook message requesting the immediate removal of her residential address from the Organisation's Facebook page. The Organisation denied any wrongdoing and refused to remove the Complainant's address from its Facebook page until it was advised to do so by the office of the Commissioner.

8 The Organisation's explanation was that it had disclosed the Complainant's name and residential address in its response to identify the Complainant "*to ensure that [it was] refunding the money of $100 [i.e., the deposit] to the correct person*".

9 The Organisation admitted in the course of the investigations that it was not aware of the Personal Data Protection Act 2012 ("**PDPA**"). Consequently,

it did not appoint a data protection officer ("**DPO**") nor did it implement any data protection policies or guidelines.

Findings and Basis for Determination

10 The issues for determination are:

(a) whether the Organisation had disclosed the Complainant's personal data without consent or authorisation; and

(b) whether the Organisation had complied with its obligations under sections 11 and 12 of the PDPA.

11 The information disclosed by the Organisation is clearly "personal data" within the meaning of section 2(1) of the PDPA as the Complainant could be identified from the information disclosed. The Organisation did not dispute this.

Whether the Organisation had disclosed the Complainant's personal data without consent or authorisation

12 Subject to certain exceptions,[1] in accordance with section 13 read with section 14 of the PDPA, organisations may only collect, use or disclose personal data about an individual with the consent of that individual (the "**Consent Obligation**").

13 An individual may, in some circumstances pursuant to section 15 of the PDPA, be deemed to have consented to the collection, use and disclosure of

1 Pursuant to section 17 of the PDPA read with the Second, Third and Fourth Schedule of the PDPA.

his/her personal data where he/she voluntarily provided the personal data and it is reasonable that he/she would voluntarily provide the data.[2]

14 The Complainant engaged the Organisation to move her belongings to her new home. It is in this context that the Complainant provided her Personal Data to the Organisation; so that the Organisation would know the location from which to pick up the Complainant's belongings and the delivery address. No evidence has been adduced of the Complainant consenting to the disclosure of the Personal Data on the Organisation's public Facebook page. Further, the Deputy Commissioner finds that the Complainant is not deemed to have consented to the said disclosure as the two limbs for making a finding of deemed consent under section 15(1) of the PDPA have not been made out. In this context, it cannot be said that this manner of disclosure of the Complainant's Personal Data by the Organisation in its response to her review on its Facebook page was within the Complainant's reasonable contemplation.

15 The Organisation's explanation that it replied to the Complainant's Facebook post with the Personal Data as it wanted to confirm the identity of the Complainant does not address the reason the Organisation publicly disclosed the Personal Data on its Facebook page. The Organisation's objective of ensuring the identity of the Complainant was not better served by disclosing the Personal Data *publicly* on its Facebook page instead of *privately* communicating with the Complainant directly. There was no legitimate reason for disclosing the Personal Data to third parties. Given the Organisation's admission of its lack of awareness of the PDPA and the obligations it imposes, it is more likely than

2 Section 15 of the PDPA.

not, that the Organisation disclosed the Personal Data simply for convenience without further consideration.

16 It is a trite principle of law that ignorance of the law is no excuse. Thus, the Organisation's lack of awareness of its obligations under the PDPA cannot excuse its breach of the PDPA. The data protection provisions of the PDPA took effect on 2 July 2014[3] after a "sunrise" period of more than a year from 2 January 2013. Since then, organisations have had ample opportunities to develop and implement appropriate policies and practices to comply with the PDPA. In any event, an organisation's lack of awareness of its data protection obligations is not a legitimate defence to a breach.

17 It is apropos to address an issue which commonly arises in the context of an organisation's communications through its commercial social media page. When is it ever acceptable to disclose personal data when an organisation is responding to public comments? It is unlikely that the terms of *ex ante* consent or scope of deemed consent can cover such disclosures.

18 The Deputy Commissioner advises caution in disclosing personal data when responding to public comments. An organisation should not be prevented or hampered from responding to comments about it using the same mode of communications that its interlocutor has selected. In some situations, it may be reasonable or even necessary to disclose personal data in order to advance an explanation. An individual who makes false or exaggerated allegations against an organisation in a public forum may not be able to rely on the PDPA to prevent the organisation from using material and relevant personal data of the individual

---

3 Personal Data Protection Act 2012 (Commencement) Notification 2014.

to explain the organisation's position on the allegations through the same public forum.

19 The following observations may be made in this context about the approach that the Commission adopts. First, the Commission will not engage in weighing allegations and responses on golden scales in order to establish proportionality. The better approach is to act against disclosures that are clearly disproportionate on an objective standard before the Commission intervenes in what is essentially a private dispute (in this case the dispute was the Complainant's alleged dissatisfaction of the services provided by the Organisation). Second, the disclosure may sometimes be justified by exceptions to consent. For example, disclosures in the course of the Organisation's investigations into alleged breaches of agreement or into conduct that may give rise to tortious claims. Disclosures in reliance of exceptions to consent will nevertheless have to be limited in scope in order to achieve the purposes of the applicable exception. Third, even in the absence of consent (whether express or deemed) or an applicable exception, it may nevertheless be objectively reasonable for the Organisation to disclose personal data in response to allegations made against it. Section 11(1) of the PDPA exhorts organisations in discharging its responsibilities under the PDPA to "*consider* what a reasonable person would consider appropriate *in the circumstances*." This requires fact-specific analysis and the burden is on the Organisation to justify that the circumstances were atypical, the disclosure was warranted and its actions were reasonable.

20 In the present case, the Complainant had posted a lengthy complaint on the Organisation's Facebook page, amounting to approximately 500 words. The Organisation responded in three separate posts. Having perused the explanations and considered the context of the disclosure of the Personal Data,

it cannot be said that the disclosure of the Personal Data had any nexus to the allegations and explanations. Hence, the disclosure in its response was clearly disproportionate. The Organisation's response was not made in the context of an *investigation* into a civil dispute (although one patently existed), nor did it fall within any other exception. Finally, the Organisation's disclosure was unwarranted and unreasonable as it was made, more likely than not, for convenience without further consideration (see paragraph 15 above).

21 Given the foregoing, the Deputy Commissioner finds that the disclosure of the Personal Data on the Organisation's Facebook page was made in breach of its Consent Obligation under the PDPA.

Whether the Organisation had complied with its obligations under sections 11 and 12 of the PDPA

22 Section 11(3) of the PDPA requires an organisation to designate one or more individuals (i.e. the DPO) to be responsible for ensuring compliance with the PDPA and section 12(a) of the PDPA requires an organisation to develop and implement policies and practices that are necessary to meet its obligations under the PDPA (collectively, the "**Openness Obligation**").

23 During the investigations, the Organisation admitted that it was not aware of the PDPA and consequently, its data protection obligations[4] under the PDPA. The Organisation also confirmed that, at the material time, it did not implement any data protection policies or practices, nor did it appoint a DPO.

24 In the circumstances, the Deputy Commissioner finds that, by its own admission, the Organisation failed to meet its obligations under sections 11(3)

---

4 Under Parts III to VI of the PDPA.

and 12(a) of the PDPA. In this regard, the Deputy Commissioner repeats his comments made at paragraph 16 above that a lack of awareness of the obligations imposed by the PDPA does not amount to a legitimate defence against a breach by the Organisation.

Data protection policies

25 The Deputy Commissioner takes this opportunity to highlight 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.

26 In this regard, the Deputy Commissioner repeats the Commissioner's guidance in *Re Aviva Ltd* [2017] SGPDPC 14 at paragraph [32] on the role of general data protection policies:

> "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…"

27 At the very basic level, an appropriate data protection policy should be drafted to ensure that it gives a clear understanding within the organisation of its obligations under the PDPA and sets general standards on the handling of personal data which staff are expected to adhere to. To meet these aims, the framers, in developing such policies, have to address their minds to the types of data the organisation handles which may constitute personal data; the manner in, and the purposes for, which it collects, uses and discloses personal data; the parties to, and the circumstances in, which it discloses personal data; and the data protection standards the organisation needs to adopt to meet its obligations under the PDPA.

28 An overarching data protection policy will ensure a consistent minimum data protection standard across an organisation's business practices, procedures and activities (e.g. communications through social media).

29 A general data protection policy is, however, not the be all and end all of data protection. Specific practices, processes, procedures and measures need to be put in place by organisations to protect personal data. In this regard, the Deputy Commissioner agrees with the following comments made by the Office of the Privacy Commissioner of Canada's decision in the case of *Google Inc. WiFi Data Collection*[5] on the necessity to put in place real and effective measures to ensure an organisation's accountability for the personal data it handles:

> "The obligation that organizations must have in place the proper practices, as a matter of accountability, concords with a growing international recognition that the protection of personal information requires real and effective measures. It is this Office's view that organizations need to implement appropriate and effective measures to put into effect the principles and obligations of the Act, including effective compliance and training programs, as an essential part of ensuring that organisations remain accountable for the personal information they collect, use or disclose."

30 Organisations with a social media or other online presence (e.g. social media forums), particularly those that rely on such platforms to communicate with its customers, ought to develop appropriate policies, practices and procedures that amply address the risks of disclosing personal data on social media or other online sites. Together, these policies, practices and procedures should seek to (i) ensure that staff who communicate through an organisation's

---

5 *PIPEDA Report of Findings #2011-001: Google Inc. WiFi Data Collection* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/> at [71].

social media account or similar platforms are aware of the organisation's data protection obligations and the importance and need to protect personal data; (ii) crystallise the organisation's position on the circumstances in which it may be appropriate to disclose personal data on these platforms for example, disclosures for which individuals have already consented to; (iii) ensure that the organisation maintains an appropriate level of control on the content posted on these platforms (e.g. by limiting the number of staff who are allowed to post and placing conditions on these staff such as requiring them to undergo relevant data protection training); (iv) crystallise the organisation's retention rules in respect of posts on such platforms; and (v) provide an avenue to escalate issues or queries to the appropriate function or role within the organisation.

31 A well informed DPO who is familiar with data protection law and practice, should be able to ensure that these policies, practices and procedures are updated to guide members of staff on the appropriate conduct when using such platforms as means of corporate communications, including with customers, and also provide guidance as to when communications commenced on public fora ought to continue in more private channels.

Data protection officer

32 The above paragraph segues appropriately into a discussion of the requirement and role of the DPO.

33 The DPO plays an important role in ensuring that the organisation fulfils its obligations under the PDPA. Recognition of the importance of data protection and the central role performed by a DPO has to come from the very top of an organisation and ought to be part of enterprise risk management frameworks. This will ensure that the board of directors and C-level executives are cognisant of the risks. The DPO ought to be appointed from the ranks of

senior management and be amply empowered to perform the tasks that are assigned to him/her. If not one of the C-level executives, the DPO should have at least a direct line of communication to them. This level of access and empowerment will provide the DPO with the necessary wherewithal to perform his/her role and accomplish his/her functions. The DPO need not – and ought not – be the sole person responsible for data protection within the organisation. Properly implemented, data protection policies will touch most, if not all, parts of an organisation. Every member of staff has a part to play. The DPO is the person within an organisation responsible for implementing the policies and practices, just as the board and C-level executives are ultimately accountable to shareholders and owners for any failure to comply.

34 The responsibilities of a DPO include, but are not limited to:[6]

(a) ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data, including processes and formal procedures to handle queries and/or complaints from the public;

(b) fostering a data protection culture and accountability among employees and communicating personal data protection policies to stakeholders;

(c) handling and managing personal data protection related queries and complaints from the public, including making information about the organisation's data protection policies and practices available on request to the public;

---

6 PDPC, Data Protection Officers at <https://www.pdpc.gov.sg/organisations/data-protection-officers> at para 4.

(d) alerting management to any risks that might arise with regard to personal data; and

(e) liaising with the Commissioner on data protection matters, if necessary.

35 In this regard, the Deputy Commissioner agrees with the position adopted in the Joint Guidance Note[7] on the role and responsibilities of a DPO (or Privacy Officer in the Canadian context) in an organisation:

> "[organizations] must appoint someone who is responsible for the privacy management program. *Whether this person is a C-level executive of a major corporation or the owner/operator of a very small organization, someone must be assigned responsibility for overseeing the organization's compliance with applicable privacy legislation.* Other individuals may be involved in handling personal information, but *the Privacy Officer is the one accountable for structuring, designing and managing the program, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up.* Organizations should expect to dedicate some resources to training the Privacy Officer. The Privacy Officer should establish a program that demonstrates compliance by mapping the program to applicable legislation. It will be important to show how the program is being managed throughout the organization.
>
> The Privacy Officer will play many roles with respect to privacy. S/he will:
>
> - establish and implement program controls;
> - coordinate with other appropriate persons responsible for related disciplines and functions within the organization;
> - be responsible for the ongoing assessment and revision of program controls;
> - represent the organization in the event of a complaint investigation by a privacy commissioner's office; and

---

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/media/gl_acc_201204/> at p. 7.

> - advocate privacy within the organization itself.
>
> This last role is as crucial as the others. Organizations face competing interests and privacy compliance is one program of many. *Privacy, however, is more than a balancing of interests. Privacy should be seen in terms of improving processes, customer relationship management, and reputation. Consequently, the privacy management program's importance must be recognized at all levels.*"
>
> [Emphasis added.]

36 Again, while the quote above is in respect of a Privacy Officer, it is equally applicable in the context of a DPO under the PDPA notwithstanding the differences between privacy and data protection.

37 From the foregoing, it is clear that regardless of the size of an organisation, the DPO plays a vital role in building a robust data protection framework to ensure the organisation's compliance with its obligations under the PDPA.

Directions

38 Having found that the Organisation is in breach of sections 11(3), 12(a) and 13 of the PDPA, the Deputy Commissioner is empowered under section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million.

39 In assessing the breach and determining the directions to be imposed on the Organisation, the Deputy Commissioner took into account the following factors:

(a) the personal data disclosed was limited to the Complainant's name and residential address; and

(b) the Organisation's breach of the Consent Obligation was due to its lack of awareness of the Organisation's obligations under the PDPA.

40 The Deputy Commissioner has decided to issue the following directions to the Organisation:

(a) to put in place a data protection policy and internal guidelines to comply with the provisions of the PDPA within 60 days from the date of this direction;

(b) to appoint a DPO within 30 days from the date of this direction;

(c) to inform the office of the Commissioner of the completion of each of the above directions within 1 week of implementation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION COMMISSION