Social Metric Pte Ltd

[2017] SGPDPC 17

Tan Kiat How, Commissioner — Case No DP-160-A712; DP-1604-A713

Data Protection – Protection obligation – Disclosure of personal data – Insufficient technical and administrative security arrangements

Data Protection – Data Protection Provisions coming into force and effect

Data Protection – Obligations of organisation and data intermediary – Data intermediary taking on the role and responsibilities of an organisation

Data Protection – Retention limitation obligation – Purpose for which the personal data was collected is no longer served by retaining the data – Retention is no longer necessary for legal or business purposes

27 November 2017.

Background

1 This case involves a company which, as part of its social media marketing campaigns conducted for and on behalf of its clients, created webpages containing the personal data of its clients' customers; and subsequently failed to remove those webpages from the world wide web, even after the social media marketing campaigns were over.

2 A complaint was made to the Personal Data Protection Commission ("**PDPC**") regarding the unauthorised disclosure of personal data on these webpages on the world wide web. The Commissioner undertook an investigation into the matter, and the Commissioner sets out his findings and decision on the matter below.

Material Facts and Documents

3 Social Metric is a digital marketing agency that provides social media marketing services. As part of these services, Social Metric would collect personal data of its clients' customers for various purposes, for example, as a form of customer engagement, or to analyse the customer demographics, amongst other things.

4 For the webpages in question, Social Metric had created nine webpages (the "**Webpages**") for various social media contests that Social Metric conducted for and on behalf of its clients. These Webpages were found on Social Metric's website at https://www.socialmetric.com (the "**Website**"). The Webpages consisted of tables that listed out various particulars of individuals. They were created for internal administrative and client use.

5 The personal data in these nine Webpages included individuals' names; email addresses; contact numbers; employers; occupations; date and time of registration; and other miscellaneous information including, "places to visit" (eg states in Australia), "activities" (outdoor sports), and "purpose" (eg personal growth). In particular, two out of the nine Webpages also contained the personal data (name and age) of about 155 children. The Commissioner's investigations disclosed that such personal data was provided by the individuals directly (ie by the individual sending his or her personal data to Social Metric through Facebook's private message function), and were not obtained from publicly available sources.

6 Based on the date and time of registration of the nine Webpages, it was observed that all the personal data contained therein, except for two individuals, were collected and disclosed before the Personal Data Protection Act 2012 ("**PDPA**") came into full force on 2 July 2014 ("**Appointed Day**"). In respect

of the two individuals, the personal data of one of the individuals (name, email address, contact number) was disclosed on 24 December 2014, while the personal data of the other individual (name and email address) was disclosed on 15 September 2015.

7 Social Metric was first informed by the Complainant of the unintended disclosure of personal data on the nine Webpages on 27 April 2016. Following the complaint made by the Complainant to the PDPC, the PDPC had also informed Social Metric about the disclosure on the Webpages in May 2016. After being informed about the Webpages, Social Metric took down three out of the nine Webpages. However, at the time of the Commissioner's investigation, six out of the nine Webpages were still available on the world wide web. These remaining six Webpages contained the personal data of approximately 558 individuals. As at 11 July 2016, all the Webpages have been taken down. The personal data was therefore left on the Webpages for a period of at least 2 months since the time that Social Metric had first been informed of the personal data that was held on its Website until they were all completely taken down. By the Commissioner's estimate, given that some of the marketing campaigns had ended by the Appointed Day, some of the personal data would have been left on the Webpages for more than two years after the respective events.

Commissioner's Findings and Basis for Determination

Issues for Determination

8 Based on the facts, there were two main issues for determination before the Commissioner:

(a) what were Social Metric's obligations under the PDPA with respect to the personal data found on the Webpages that were exposed on the internet;

(b) whether Social Metric complied with these obligations. Specifically,

(i) whether Social Metric complied with its Retention Limitation Obligation under section 25 of the PDPA when it retained the personal data of its clients' customers even after the social media marketing campaigns were over; and

(ii) whether Social Metric has complied with its Protection Obligation under section 24 of the PDPA, given the unauthorised disclosure of personal data on the Webpages.

(a) Social Metric's obligations under the PDPA

i. How did the Data Protection Provisions of the PDPA apply to Social Metric?

9 As the Webpages were created before the Data Protection Provisions of the PDPA (ie Parts III to VI of the PDPA) came into force on the Appointed Day, it is necessary to examine how Social Metric came to take on these obligations under the PDPA in respect of the Webpages.

10 *Before the Appointed Day*, the Data Protection Provisions of the PDPA were not in force, and hence, Social Metric was not subject to these provisions in relation to the personal data that it had processed for its clients' social marketing campaigns. *After the Appointed Day*, the Data Protection Provisions under the PDPA came into force, and at such time, it became incumbent on an organisation (as in this case, Social Metric) to take proactive steps to comply

with these obligations under the PDPA in respect of the *existing* personal data held in their possession or control, as well as any *new* personal data that it may come into possession or control with.

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".

12 What has just been described about the PDPA obligations coming into operation and applying after the Appointed Day is to be contrasted with the 'grandfathering' provision under section 19 of the PDPA, which also applies to personal data held by an organisation before the Appointed Day. In essence, section 19 of the PDPA allows an organisation to continue to *use* (but not disclose) personal data that was collected before the Appointed Day for such purposes for which the personal data was collected, without having to obtain consent under the Data Protection Provisions. As mentioned in *Re Comfort Transportation Pte Ltd and another* [2016] SGPDPC 17, personal data collected before the Appointed Day as business contact information could continue to be used *after* the Appointed Day as such. Notwithstanding the grandfathering of the purpose for usage, the organisation would have to still comply with the rest of the Data Protection Provisions.

13 From the above analysis, therefore, Social Metric has the obligation to comply with the Data Protection Provisions under the PDPA in respect of the existing personal data that were held on its Website.

ii. In what capacity did Social Metric take on such obligations under the PDPA?

14 In order to determine what obligations apply to Social Metric under the PDPA, it is apposite to consider the capacity that Social Metric was in when it was carrying out the data processing activities on the personal data of its clients' customers – ie as a data intermediary or an organisation. This is because different sets of obligations and responsibilities may apply depending on the capacity that Social Metric is in.

15 Under the PDPA, when an organisation carries out data processing activities on behalf of another, the organisation is considered a data intermediary. The PDPA obligations that would apply to a data intermediary pursuant to section 4(2) of the PDPA are limited to two obligations – the Protection Obligation and Retention Limitation Obligation. In comparison, an "organisation" under the PDPA, for which the data intermediary is performing the data processing, would be subject to the full range of obligations under the PDPA. This is so, even though the organisation may have engaged a data intermediary to implement the necessary data protection measures for the organisation. Section 4(3) of the PDPA provides that "*an organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for purposes by a data intermediary as if the personal data were processed by the organisation itself*".

16 Beyond the different sets of obligations that may apply to an organisation or data intermediary, there may also be different responsibilities that an organisation or data intermediary may undertake under the PDPA. As explained in *Re Smiling Orchid (S) Pte Ltd and others* [2016] SGPDPC 19, in a situation where the data processing activities are carried out by the organisation's external vendor, the organisation has a supervisory or general

role for the protection of the personal data, while the data intermediary has a more direct and specific role in the protection of personal data arising from its direct possession of or control over the personal data. This means that the organisation can still be liable for a data breach for failing to meet its responsibility, even though its data intermediary was found to have its own responsibility, and vice versa.

17 In this case, at the point of collection of personal data, Social Metric was carrying out the collection on behalf of its clients for the marketing campaigns, and was thus acting as a data intermediary for its clients. Next, with regard to Social Metric posting the personal data of its clients' customers on the Website, that, too, was done in the capacity as a data intermediary. The Website was put up for the purposes of the marketing campaigns of Social Metric's clients. It was when the marketing campaigns had ended, and Social Metric had held on to the personal data (which was still posted on the Website) for a longer period than was *reasonable*, that Social Metric can no longer be considered a data intermediary in relation to such activities.

18 There are two main reasons for this position. First, the social marketing campaigns were already over, and both Social Metric and its clients had no further purpose in retaining the personal data on the Website. Social Metric cannot be said to be "*[processing] personal data on behalf of*" its clients by the protracted retention of the personal data on its Website. Indeed, as mentioned above, based on the Commissioner's estimate, some of the personal data was kept on its Website for more than two years. Accordingly, at some point in time, Social Metric was no longer a data intermediary within the definition of this term under the PDPA. Instead, Social Metric was now acting on its own accord in relation to the personal data that it held, and had taken on the full responsibility of protecting such personal data. Second, Social Metric had a

standard operating procedure ("**SOP**") to dispose of the personal data after the marketing campaigns in its contract for service with its clients had ended. As far as the clients were concerned, it was reasonable to expect Social Metric to carry out the disposal upon the completion of the marketing campaigns, and there was no evidence that Social Metric's clients were aware that Social Metric had failed to dispose of the personal data. In the premises, it would not be logical nor fair if the PDPA imposes a continuing obligation on Social Metric's clients to protect the personal data. Since Social Metric had failed to carry out what it was supposed to do (ie to dispose of the personal data after the marketing campaigns), it bears the risk for whatever happens to the personal data that was held in its hands after the marketing campaigns were over.

19 Social Metric had therefore assumed the full data protection responsibilities of an "organisation" under the PDPA after the end of the marketing campaigns. This is a position that has been adopted by foreign data protection authorities as well.

iii. Foreign authorities on the issue of a data intermediary taking on responsibilities of an organisation

20 The foreign data protection authorities have taken the position that a data processor, which was originally engaged to perform data processing activities for or on behalf of a data controller, could subsequently take on the data protection responsibilities of a data controller under certain circumstances, for example, where the data processor uses the personal data for its own unauthorised purposes, or for additional purposes not envisaged by the data controller, or for its own benefit.

21 According to the guidance issued by the UK's Information Commissioner's Office, *Data controllers and data processors: what the*

difference is and what the governance implications are ("**ICO guidance**"), a data processor may become a data controller in its own right, albeit to a limited extent, when, for example, the processor breaks the agreement with its data controller. The ICO guidance provides that:[1]

> "65. A data processor will have access to the personal data held by the controller or controllers it provides its services to but it cannot have any of its own data controller responsibilities for that data. **However, in certain situations this may change and it will become a data controller in its own right if only to a limited extent.**
>
> …
>
> 67. **If a data processor breaks the agreement with its data controller, for example by using the data for its own unauthorised purposes, then it will also take on its own data controller responsibilities.** This includes the duty under the first data protection principle to process, including to obtain, personal data fairly and lawfully. Where a data processor takes the personal data the controller has entrusted it with but breaks the terms of its contract by using the data for its own purposes, it is likely to be in breach of the first principle and the ICO could take enforcement action against it…"
>
> [Emphasis added.]

22 Similarly, in the EU, the European Commission has issued *Opinion 1/2010 on the concepts of "controller" and "processor"* which describes a scenario where a data processor which conducts marketing activities may be considered to be a data controller and become subject to data protection obligations:[2]

---

1 U.K., Information Commissioner's Office, Data controllers and data processors: what the difference is and what the governance implications are (6 May 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> at paras. [65], [67].

2 E.U., European Commission, Art. 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (16 Feb 2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> at p.14.

> "In these cases - where there is a good definition of purposes, but little or even no guidance on technical and organizational means - the means should represent a reasonable way of achieving the purpose(s) and the data controller should be fully informed about the means used. **Would a contractor have an influence on the purpose and carry out the processing (also) for its own benefit, for example by using personal data received with a view to generate added-value services, it would be a controller (or possibly a joint controller) for another processing activity and therefore subject to all the obligations of the applicable data protection law**.
>
> > Example No. 3: Company referred to as data processor but acting as controller
> >
> > Company MarketinZ provides services of promotional advertisement and direct marketing to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for the purpose of promoting products of other customers. **This decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this processing operation.** The question of the lawfulness of this processing will still be assessed in the light of other Articles (6-8)."
>
> [Emphasis added.]

23 This means that where a data processor has an influence on the purpose of the processing, and carries out a separate processing activity which is different from the purpose that the data controller envisaged or which is for the data processor's own benefit, then the data processor could be considered a data controller for that separate processing activity.

24 Whilst Singapore does not have the concept of a "data controller" or a "data processor" in its data protection regime, these terms taken from the UK's Data Protection Act 1988 and the EU Directive 95/46/EC do bear similarities to the concept of "organisation" and "data intermediary" respectively in the PDPA.

As such, the Commissioner is of the view that the general principles mentioned above are useful and supportive of the position that the Commissioner has taken.

(b) In this case, Social Metric's compliance with its Retention Limitation and Protection Obligations comes into focus

25 Accordingly, while Social Metric had initially held the *de facto* role of a data intermediary (before the Appointed Day) during the marketing campaigns, Social Metric had subsequently taken on the role of an "organisation" when it held on to the personal data on its Website after the marketing campaigns with its clients were over.

26 In this case, the pertinent issues relate to Social Metric's compliance with its Protection and Retention Limitation Obligations. This is because the nature of the breach and the subject of complaint in this case relate to (a) Social Metric's failure to protect the personal data on the Webpages from unauthorised access; and (b) Social Metric's failure to remove personal data of its clients' customers from its Website in accordance with its SOP or a reasonable period thereafter justifiable for legal or business purposes ("**the tail period**"). *These are obligations that are common between Social Metric as data intermediary or as organisation*. Had the period of retention been shorter, and Social Metric stayed as a data intermediary, its alleged misconduct would have been analysed as breaches of the Retention Limitation and Protection Obligations *qua* data intermediary. Where in this case, a considerable period has passed, and the data intermediary has morphed into an organisation, it is not meaningful to split hairs and analyse *part* of the period in which Social Metric had held on to the data as a breach of a data intermediary's Retention Limitation and Protection Obligations while analysing the *rest* of this period as a breach of an organisation's Retention Limitation and Protection Obligations. With the effluxion of time that Social Metric had held on to the data, there was nothing

to separate Social Metric's responsibilities under the Retention Limitation and Protection Obligations from that of a data intermediary or an organisation – Social Metric ultimately took on the role and responsibility as an "organisation" under the PDPA for the protection of personal data. The entire period in excess of "the tail period" should be analysed as a breach of an organisation's Retention Limitation and Protection Obligations.

27 We turn now to the assessment of whether or not Social Metric has complied with its Retention Limitation and Protection Obligations.

i. Whether Social Metric has complied with the Retention Limitation Obligation

28 Under the Retention Limitation Obligation, an organisation is obliged to cease retaining its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that: (a) the purpose for which the personal data was collected is no longer served by retaining the data; and (b) retention is no longer necessary for legal or business purposes. As limbs (a) and (b) of section 25 of the PDPA are conjunctive, this means that if the organisation still has purposes for retaining the personal data under *either* limb (a) or limb (b) of section 25 of the PDPA, the organisation is allowed to retain such personal data.

29 On the facts of this case, Social Metric held on to the personal data even though the marketing campaigns were over. Under limb (a) of section 25 of the PDPA, the purpose for which the personal data was collected was no longer being served by retention of the personal data. Additionally, based on the evidence in this matter, there was nothing to indicate that Social Metric had any legal or business purpose under limb (b) of section 25 of the PDPA for keeping the personal data either. Since the purpose of retention as a data intermediary

was no longer valid, retention as an organisation is all the more indefensible. Accordingly, Social Metric has failed to show that it had any purpose for retaining personal data pursuant to limbs (a) and (b) of section 25 of the PDPA, and it is therefore in breach of section 25 of the PDPA.

ii. Whether Social Metric has complied with the Protection Obligation

30 As explained above at paragraphs 25 to 26 above, Social Metric has an obligation to protect personal data under the Protection Obligation as an *organisation* under the PDPA (pursuant to Section 24 of the PDPA). Social Metric had taken on the role of an "organisation" when it held on to the personal data on its Website after the marketing campaigns with its clients were over, and it was in such a capacity that it had the duty to protect the personal data in its possession or control after the Protection Obligation came into force on the Appointed Day.

31 The Commissioner finds that Social Metric failed to comply with its Protection Obligation. Social Metric had failed to limit access to the Webpages, and had left the personal data on the Webpages exposed to the world wide web. There were no security or access controls on the Website or on any of the Webpages, such as a password protection. Any member of the public could have accessed the personal data of the clients' customers through the Webpages.

32 This case is analogous to the case *Re Propnex Realty Pte Ltd* [2017] SGPDPC 1, where it was found that the organisation failed to properly protect personal data as it did not have any security controls or restrictions (ie proper authentication system) to prevent access from the world wide web over the webpages that were stored on the server. Similar to *Re Propnex Realty Pte Ltd*, therefore, the present case may be characterised as one which Social Metric had

failed in its Protection Obligation to put in the necessary controls to prevent access to personal data held on its Webpages. It was not one where, for example, the organisation had intentionally disclosed personal data on its website. In those cases, the Commissioner may look into the further issues of whether the organisation was in breach of its Consent and Notification Obligations for disclosing personal data without consent and/or notification. This is illustrated by the case of *Re My Digital Lock Pte Ltd* [2016] SGPDPC 20.

33 Additionally, not only did Social Metric fail to put in the necessary security measures upon the PDPA coming into full force on 2 July 2014 (ie the Appointed Day), this had carried on well after 2 July 2014. As mentioned earlier at paragraph 6, there were two instances where Social Metric had uploaded personal data of the two individuals on the Webpages in December 2014 and September 2015 respectively. Social Metric's prolonged failure to put in place the necessary security measures was inexplicable and a flagrant breach of its Protection Obligation under the PDPA.

34 Social Metric alleged that the reason why the customers' personal data was publicly accessible online was due to oversight or forgetfulness on its part. These are not valid excuses.

35 In consideration of the above, Social Metric, in allowing the Webpages containing personal data to be made publicly available and failing to implement reasonable security arrangements over the Webpages, was in breach of the Protection Obligation.

The Commissioner's Directions

36 Pursuant to section 29 of the PDPA, the Commissioner is empowered to give Social Metric such directions as it deems fit to ensure Social Metric's

compliance with the PDPA. This may include directing Social Metric to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

37 In assessing the breach and determining the directions to be imposed to Social Metric in this case, the Commissioner took into account the following factors:

(a) the fact that personal data (names and ages) of about 155 children were disclosed;

(b) Social Metric did not take prompt remedial actions after being informed of the data breach by the Commissioner;

(c) Social Metric had, on more than on occasion, informed the Commissioner that the personal data in question had been deleted when this was not the case; and

(d) Social Metric was generally uncooperative throughout the investigation process. Social Metric demonstrated its uncooperative attitude by making unsubstantiated claims such as informing the Commissioner that the data breach was a result of an external hack, and that it had engaged freelance developers located in the Philippines to set up and maintain the Website without providing any evidence of their claims. In addition, Social Metric also caused multiple delays in the investigation process when it repeatedly missed the Commissioner's deadlines to reply.

38 Having completed its investigation and assessment of this matter, the Commissioner is satisfied that Social Metric was in breach of the Protection

Obligation and the Retention Limitation Obligation under sections 24 and 25 of the PDPA respectively.

39 In consideration of the relevant facts and circumstances of the present case, the Commissioner hereby directs Social Metric to:

(a) scan and confirm that its Website no longer stores publicly accessible personal data that is not supposed to be disclosed to the public; and

(b) pay a financial penalty of S$18,000 within 30 days from the date of the Commissioner's direction, failing which, interest, at the rate specified in the Rules of Court in respect of judgment debts, shall be payable on the outstanding amount of such financial penalty.

40 The Commissioner emphasises that he takes a very serious view of any instance of non-compliance with the PDPA, and he urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. The Commissioner will not hesitate to take the appropriate enforcement action against the organisation(s) accordingly.
