Singapore Law Review
Juris Illuminae Vol 9 (2017/18)

SUGGESTIONS ON THE RELEVANCE OF THE ORGANIZATION'S SIZE TO SECTION 11 OF SINGAPORE'S PERSONAL DATA PROTECTION ACT

FOO EE YEONG DANIEL

I. INTRODUCTION

Singapore's *Personal Data Protection Act*[1] [*PDPA*] has been in effect since four years ago,[2] and serves to balance the protection of individuals' personal data with the 'need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances'.[3] Since then, the Personal Data Protection Commission [*PDPC*], with the help of public consultations,[4] has continually revisited and augmented[5] the PDPA's various advisory guidelines.[6]

The PDPA stipulates various obligations, which organisations should fulfil based on 'what a reasonable person would consider appropriate in the circumstances', as per section 11(1) of the Act (the "reasonableness test"). This standard of reasonableness underpins the standard of compliance

---

[1] *Personal Data Protection Act* (No. 26 of 2012).

[2] According to the Personal Data Protection Commission of Singapore, "Legislation and Guidelines", online: <https://www.pdpc.gov.sg/legislation-and-guidelines>, '[t]he PDPA took effect in phases starting with the provisions relating to the formation of the PDPA on 2 January 2013. Provisions relating to the DNC Registry came into effect on 2 January 2014 and the main data protection rules on 2 July 2014.'

[3] *Supra* note 1 at s 3.

[4] A useful repository of these consultation papers may be found at the Personal Data Protection Commission of Singapore, "Public Consultations", online: <https://www.pdpc.gov.sg/legislation-and-guidelines/public consultations>.

[5] *Singapore Parliamentary Debates, Official Report*, vol 93 (10 March 2015) (Assoc Prof Dr Yaacob Ibrahim).

[6] *Supra* note 1 at s 49(1), which states that the 'Commission may, from time to time, issue written advisory guidelines indicating the manner in which the Commission will interpret the provisions of this Act'.

for all obligations under the PDPA,[7] and the Advisory Guidelines on Key Concepts in the PDPA[8] [the *Guidelines*] clarifies that this applies to *all* private organisations[9] as defined in section 2, regardless of their size.

This article aims to explore the relevance of an organisation's size to the PDPA's reasonableness test, and submits that the former should be considered as a factor in applying the latter. This may be done, for instance, by providing for it in the Guidelines.

II. MINIMAL SCOPE FOR SIZE IN THE PDPA'S REASONABLENESS TEST

Currently, the size of the organisation appears to be contemplated only by the Protection Obligation – when determining whether reasonable security arrangements have been made to prevent unauthorised handling of personal data under section 24 of the PDPA. This is seen from the Guidelines, which provide only general guidance for compliance[10] and mention the size of the organisation only once: as a factor in risk assessment exercises determining whether information security arrangements are adequate.[11] Otherwise, the PDPA legislation and jurisprudence do not feature the size of the organisation in applying the reasonableness test for any other obligation. There does not appear to be any debate on this issue; one can only guess that the drafters of the PDPA believed that fulfilling these other obligations was more important than the strain of compliance on organisations and/or that the obligations were generally undemanding for organisations that already had strong data protection practices. In any case, the PDPA prevents organisations from invoking their small size to unjustifiably exempt themselves from obligations to protect personal data.

---

[7] These may be broadly labelled as the Consent Obligation, Purpose Limitation Obligation, Notification Obligation, Access and Correction Obligation, Accuracy Obligation, Protection Obligation, Retention Limitation Obligation, Transfer Limitation Obligation and Openness Obligation. This article will look at only a few of these obligations, mostly for illustrative purposes.

[8] Personal Data Protection Commission of Singapore, "Advisory Guidelines on Key Concepts in the PDPA" (revised 27 July 2017).

[9] *Ibid* at 6.3.

[10] Personal Data Protection Commission of Singapore, "Introduction to the Guidelines" at para 3.3.

[11] *Supra* note 8 at 17.4(a).

Instead, the reasonableness of measures appears to turn on the impact on the individual whose personal data is mishandled and the compliance measures themselves. For example, the Accuracy Obligation under section 23 considers, *inter alia*, the nature of the personal data,[12] as well as the impact on the relevant individual should the data be inaccurate.[13] Another example is the Notification Obligation under section 20, which considers the 'circumstances and manner in which [the organisation] will be collecting the personal data',[14] the 'frequency at which the personal data will be collected'[15] and 'the channel through which the notification is provided'.[16] The size of the organisation does not appear to feature in the reasonableness test for any of the obligations under the PDPA, except for in the Protection Obligation.

III. ORGANIZATIONAL SIZE SHOULD BE A FACTOR

As a result of the above, the reasonableness test arguably fails to take into account the resource-scarce reality of many small organisations when determining whether they have discharged their obligations to a 'reasonable' standard under the PDPA. One example is where an organisation transfers personal data to its parent company overseas, and has to fulfil its Transfer Limitation Obligation under section 26 of the PDPA. The Guidelines suggest that the organisation reviews the corporate rules binding both organisations and assesses that they comply with these regulations, as well as that the data protection is 'comparable to the standard under the PDPA'.[17] This envisages studying rules, designing and executing appropriate transfers, as well as deciding whether corporate practices sufficiently comply with legislation – all difficult processes that require a certain amount of manpower or at least expertise that small organisations will not be as privy to as large ones. Except for in the Protection Obligation, the PDPA's current reasonableness test essentially demands the same standard of compliance from the sole proprietor as that from the large,

[12] *Ibid* at 16.4(a).
[13] *Ibid* at 16.4(e).
[14] *Ibid* at 14.10(a).
[15] *Ibid* at 14.10(c).
[16] *Ibid* at 14.10(d).
[17] *Ibid* at 19.4.

multinational company. This raises issues of resource inequality and disadvantage to small organisations, for which sustainability is already a challenge without the PDPA.

Considering the organisation's size when applying the reasonableness test would better accord with the plain meaning of 'reasonableness'. It appears unreasonable, in the barest and most layman sense of the word, to expect small organisations to comply with the PDPA as rigorously as large organisations. Then-President of the Singapore Chinese Chamber of Commerce and Industry, Mr Teo Siong Seng, emphasised during the Second Reading of the Personal Data Protection Bill that small organisations would struggle more with manpower, time-related and even consultancy costs of compliance with the PDPA.[18] SMEs have since reportedly had to grapple with 'overburdened staff'[19] and five-figure costs on 'new procedures, staff training and the upgrading of technology]'.[20] In particular, the obligation to 'develop and implement policies and practices that are necessary' to comply with the PDPA, as per section 12(a) of the Act, is manifestly more difficult for small organisations than it is for large ones. Taking into account an organisation's size would achieve better approximations of what a 'reasonable person would consider appropriate in the circumstances'. This would in turn produce more practical benefits: guiding the PDPC to achieve fairer adjudicative outcomes – ensuring that small organisations are not penalised for failing to take compliance measures beyond their means.

Further, having regard for the size of the organisation would better achieve the PDPA's purpose of mitigating compliance costs.[21] Organisations should save costs when implementing essential PDPA-compliant processes, as doing so guards against actionable, personal data breaches 'under other statutes, at common law and equity'.[22] This helps organisations save costs on litigation and

---

[18] *Parliamentary Debates Singapore: Official Report*, vol 89 (15 October 2012) (Nominated Member, Mr Teo Siong Seng). Mr Teo spoke as then-President of the Singapore Chinese Chamber of Commerce and Industry, 'representing 4,000 corporate members and 145 trade associations from a great diversity of trades, industries and service providers'.

[19] The Straits Times, "Privacy Act shows confusion", online: < http://www.todayonline.com/commentary/privacy-act-sows-confusion>.

[20] The Straits Times, "Early childhood educator simplifies personal data protection requirements", online: <http://www.straitstimes.com/business/companies-markets/early-childhood-educator-simplifies-personal-data-protection-requirements>.

[21] *Singapore Parliamentary Debates, Official Report*, vol 89 (15 October 2012) (Minister for Communications and Information, Associate Professor Dr Yaacob Ibrahim).

[22] Hannah YeeFen Lim, *Data Protection in the Practical Context: Strategies and Techniques* (Singapore: Academy Publishing, 2017) at 1.2.

compensation, which would be greater than the costs incurred for compliance with the PDPA. However, as the PDPA's reasonableness test now apparently does not accommodate the inherent differences between small and large organisations, small organisations may find themselves tending toward the safest practices or 'best solution[s]' adopted by large organisations, which may be too costly for them.[23] Recognising that the size of the organisation should affect what is considered 'reasonable' compliance would give a green light to small organisations and their consultants (if they can afford any) to exercise latitude in adopting more cost-efficient practices that would still comply with the PDPA.[24]

Considering the organisation's size would also better achieve the PDPA's purpose of enhancing Singapore's business competitiveness.[25] Holding small organisations to the same standard of 'reasonableness' as large organisations in complying with the PDPA has deleterious effects on the former's operations.[26] This is because compliance with the PDPA requires a large amount of time, cost and effort that could otherwise be invested productively into the organisation's operations.[27] Such resource-demanding measures include studying the PDPA, appointing a Personal Data Officer,[28] developing policies and practices for compliance[29] that must be then communicated to staff,[30] as well as training staff to receive and respond to PDPA-related inquiries and complaints.[31] This has arguably even worse consequences for small social service organisations, which already struggle to make the most of their resources to perform their charitable works. Imposing the reasonableness test for compliance – without considering their sizes – risks impeding the good work of these organisations and generally inhibiting the progress of Singapore's social service sector

---

[23] *Supra* note 19.

[24] It is interesting to note that organisations are already advised to consider their size in deciding appropriate audit processes, as per Alat Sheela, *Role Of Audit In Your Organisation's Personal Data Protection Act 2012 Compliance Programme, Personal Data Protection Digest* (Singapore: Academy Publishing, 2017) at 10. It is submitted that this should be the case for all forms of compliance practices.

[25] *Supra* note 22.

[26] This was recently alluded to in *Parliamentary Debates Singapore: Official Report*, vol 94 (6 March 2017) (Member of Parliament, Mr Saktiandi Supaat): the need to protect personal data has made it 'more difficult' for businesses to 'use data innovatively and optimize business opportunities'.

[27] *Supra* note 19.

[28] This is an extension of the PDPA's obligations; *supra* note 1 at s 11(3).

[29] *Ibid* at s 12(a).

[30] *Ibid* at s 12(c).

[31] *Ibid* at s 12(b).

– a result that is normatively undesirable. A reasonableness test that accounts for the organisation's size would encourage small organisations to consider practices that are less operationally disruptive than those that large organisations adopt but would still comply with the PDPA. Such would not only facilitate the Act's aim of business productivity and competitiveness, but also the socially desirable aims of various social service organisations.

IV. THE DANGERS OF CONSIDERING ORGANIZATIONAL SIZE

The dangers of considering an organisation's size in applying the reasonableness test may be observed from the effects of Australia's *Privacy Act 1988* [*APA*],[32] which makes exemptions for small businesses.[33] This 'small business exemption' has been heavily criticised, and the Australian Law Reform Commission even recommended its repeal in 2008.[34] In particular, it has been argued that organisational size is unrelated to the risk of personal data breach; such depends instead on the nature of the data, its handling and the organisation's operations.[35] There have been concerns that the APA may be abused by small organisations, which are given a statutory backdoor to misuse personal data in the name of cost-effectiveness.[36]

Including the organisation's size as only a *factor* in the PDPA's reasonableness test would be an appropriately moderate approach that mitigates the risk of completely exempting small, rogue organisations. In fact, as suggested, the organisation's size could be mentioned as a factor only in the Guidelines. Since the Guidelines are 'advisory' and 'do not constitute legal advice',[37] this would mitigate the risk of giving small organisations *carte blanche* to breach the PDPA – holding small organisations to baseline standards of compliance. The non-conclusive status of a 'factor', as well as the non-binding nature of the Guidelines, also collectively preserve the PDPC's ability to find PDPA breaches regardless of the organisation's size. The only difference would be that the PDPC

---

[32] *Privacy Act 1988* (Cth).
[33] *Ibid* at s 6C.
[34] See Recommendation 39-1 in Australian Law Reform Commission, "Australian Privacy Law and Practice Report 108" at p 53.
[35] *Ibid* at 39.26.
[36] A more detailed analysis of the *Privacy Act 1988*'s 'small business exemption' may be found in *Supra* note 35.
[37] *Supra* note 10 at 3.1.

should be persuaded to weigh the small size of the organisation as one of many factors in deciding whether there is a breach of the Act.

V. MOVING FORWARD: CHALLENGES IN DEFINING 'SIZE'

In sum, an organisation's size should be considered as a factor in the PDPA's reasonableness test as such better accords with the plain meaning of 'reasonableness', as well as better achieves the Act's purposes of enhancing Singapore's business competitiveness while managing compliance costs.

Having explored the legal and normative justifications of incorporating the organisation's size as a factor in the PDPA's reasonableness test, this article notes that defining 'size' has proven and can expected to be tricky. The APA's definition of a 'small business' may be used as a case study. It sets out what would and would not qualify for the exemption, and has two significant features: first, it pegs 'size' primarily to the organisation's annual turnover.[38] Second, it adopts a binary view of what would be 'small' and not. Suggestions have been made to raise the APA's turnover threshold, to account for inflation.[39] There have also been suggestions to base the definition instead on specific levels of risk,[40] or simply the number of employees in the organisation.[41] Each of these has attracted its criticisms.

Thus, careful thought should be given as to what definition of 'size' would be a suitable factor in the PDPA's 'reasonableness' test, considering the Act's aim of promoting business competitiveness and data protection while moderating compliance costs. These, as well as other matters related to how the size of the organisation may or should affect its compliance obligations, should also be further considered.

---

[38] *Supra* note 32 at s 6D.
[39] *Supra* note 34 at 39.124.
[40] As determined by the type of data and number of individuals about whom data is held; *Ibid* at 39.126.
[41] *Ibid* at 39.129.