[2021] PDP Digest

PERSONAL DATA PROTECTION DIGEST

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

PERSONAL DATA PROTECTION DIGEST

Editor

Yeong Zee Kin

Deputy Editors

Chen Su-Anne

Lee Ti-Ting

Amogh Chakravarti

Editorial Assistant

Yeo Wei Cheang

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

2022

CITATION
This volume may be cited as:
[2021] PDP Digest

Published by Academy Publishing

Academy Publishing is a division of the Singapore Academy of Law ("SAL").

SAL is the promotion and development agency for Singapore's legal industry. Its vision is to make Singapore the legal hub of Asia. It aims to drive legal excellence through developing thought leadership, world-class infrastructure and legal solutions. It does this by building up the intellectual capital of the legal profession by enhancing legal knowledge, raising the international profile of Singapore law, promoting Singapore as a centre for dispute resolution and improving the efficiency of legal practice through the use of technology. More information can be found at www.sal.org.sg.

Publicity & Engagement
Personal Data Protection Commission
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438
E-mail: info@pdpc.gov.sg
www.pdpc.gov.sg

MCI (P) 053/02/2022

FOREWORD

BY THE PERSONAL DATA PROTECTION COMMISSIONER

Change is inevitable, and the law must keep up. In the 2018 edition of the Personal Data Protection Digest ("Digest"), we highlighted the need for data protection laws to keep pace with changes and advancements in technology, business, and societal expectations. That comment has since borne fruit in the latest amendments to the Personal Data Protection Act ("PDPA") which came into effect on 1 February 2021.

The latest amendments – made in consultation with industry stakeholders and the public – reflect our sharpened resolve for the PDPA to strike the right balance between incentivising organisations to innovate with data, and ensuring that they do so responsibly.

New exceptions have been introduced to empower organisations to perform research, improve business processes, and perform other legitimate uses. At the same time, with a new mandatory Data Breach Notification Obligation and enhanced financial penalties, organisations will be held to a higher standard of accountability for their data use. The new Data Portability Obligation will also grant individuals greater autonomy over their personal data and spur innovative competition amongst service providers. The Personal Data Protection Commission will continue to engage with industry and the public to promote responsible data use as the fuel for Singapore's digital economy.

This year's edition of the Digest compiles perspectives from data protection practitioners on a variety of topics relating to the latest amendments to the PDPA, as well as other topics broadly on (a) the regulation of data collection, use and disclosure; (b) the data protection responsibilities of organisations; and (c) the obligations owed by organisations to data subjects. The contributors have shared practical guidance on PDPA compliance, and we hope that you find their insights useful.

I thank the authors for their contributors to this year's Digest, and look forward to a new and exciting decade ahead for the PDPA.

Lew Chuen Hong

Commissioner

Singapore

CONTENTS

	Page
Foreword by the Personal Data Protection Commissioner, Lew Chuen Hong	iii
Regulation of Data Collection, Use and Disclosure	
Fostering Data Sharing and Innovation Whilst Maintaining Legal Safeguards *LIM Sui Yin, Jeffrey*	1
Dawn of a New Age for the Notification Obligation *Jansen AW* and *TING Chun Yen*	16
Consent Granted but Impractical to Withdraw – Considerations in the Digital Economy *LIM Tat* and *HENG Chiew Khoon*	30
The Public Availability Exception *Benjamin WONG*	41
Review of Decisions Relating to the Regulation of Data Collection, Use and Disclosure *Benjamin WONG*	52
Organisations' Data Protection Responsibilities	
Achieving Accountability through Data Protection by Design *Steve TAN* and *Justin LEE*	59
Personal Accountability under the Personal Data Protection Act: Past and Present *Lanx GOH* and *Joshua KOW*	69
Cross That Breach When We Get There? Designing Pre-emptive Measures to Manage Potential Cross-border Data Incidents under the Personal Data Protection Act *Nick CHIAM Zhi Wen* and *LEE Jia Juinn, Kenji*	85
Welcoming the Mandatory Data Breach Notification Regime: A Comparative Analysis and Observations from Practice *LIM Chong Kin* and *Charis SEOW*	109

Page

The Data Breach Notification Obligation and Case Studies for Financial Institutions and Employers
Alexander YAP Wei-Ming, *Eugene HO Yizhe*, *TAN Zhi Feng*, *Christine TEE Hui Min* and *Jean CHAN* 126

Effecting Voluntary Statutory Undertakings in Singapore – Remediation Rather Than Reprimand
Bryan TAN 144

Navigating Cross-border Data Transfer Laws in 2021
Charmian AW, *Cynthia O'DONOGHUE*, *Aselle IBRAIMOVA*, *Amy YIN* and *Catherine JING* 155

Utility of a Structured Framework in Assessing Financial Penalties under the Personal Data Protection Act
Kabir SINGH, *LOW Xide* and *John WU Bangguo* 177

The Vital Role of the Data Protection Officer
CHUA Ying-Hong 193

Obligations Owed to Data Subjects

Individuals' Rights under the Amended Personal Data Protection Act: Balancing Individual Control and Organisational Accountability
David N ALFRED and *Janice LEE* 205

Data Portability: The Singapore Approach and a Comparative Study of Selected Jurisdictions
Amira Nabila BUDIYANO and *Jonathan KAO* 219

Data Litigation: Practical and Legal Difficulties in the Right of Private Action
Janice GOH, *Sarah HEW* and *TAN Tian Yi* 251

Whistle-blowing Systems: Balancing Legitimate Corporate Governance Interests and Data Subject Rights
Carren THUNG 265

FOSTERING DATA SHARING AND INNOVATION WHILST MAINTAINING LEGAL SAFEGUARDS*

LIM Sui Yin, Jeffrey
LLB (Hons) (Bristol University);
Advocate and Solicitor (Singapore); Barrister-at-law (England & Wales)

I. Introduction

1 By now, most people would have heard of the pithy saying "data is the new oil", and perhaps just as many have heard of how that is a poor analogy. To add further strain to this ill-fated analogy, one might rhetorically ask: *If data is the new oil, then where are the supply chains, the refineries, the brokerage systems, the marketplaces and distribution systems?*

2 The comparison between oil and data, including personal data, indeed misses many of the nuances around data as a resource, as an asset, and as a springboard to securing a competitive advantage or innovation. But the rhetorical question above does raise an interesting perspective and question: namely, is it possible to envision an economy and business ecosystem built on data sharing, and, if so, what are the structures that are necessary to achieve this?

3 Despite the clear differences between a commodity like oil, and a resource like personal data, there are analogies that can be drawn if one chooses to squint hard enough. For example, just as crude oil must be refined, data also needs to be refined. The processes[1] can include

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

1 The topic is broadly detailed in many publicly accessible articles, and fuller discussion is not within the scope of this article. However, a useful and basic introduction to data cleansing and transformation can be found at Tableau, "Guide to Data Cleaning: Definition, Benefits, Components, and How to Clean Your Data" <https://www.tableau.com/learn/articles/what-is-data-cleaning> (accessed November 2021); Fakhitah Ridzuan & Wan Mohd Nazmee Wan Zainon, "The Fifth Information Systems International Conference 2019: A Review on Data Cleansing Methods for Big Data" (2019)

(*continued on next page*)

"cleansing" (*eg*, removing errors, fixing or dealing with missing data, removing duplicates, *etc*) or "transforming" the data (*eg*, reworking the structure of data from one schema to another, *etc*). Indeed, these "refining" services are part of a burgeoning industry as businesses undertake digital transformation or look to find new business insights from the data that they have.

4 Of course, unlike oil, dinosaurs are no longer around to register a complaint with a regulator over how the product of their fossils are used after their extraction from the ground. Data subjects, on the other hand, have rights over their personal data under the Personal Data Protection Act 2012[2] ("PDPA") and rightly so, since the harm to a data subject arising from breaches, unregulated use and other conduct could be substantial. Additionally, the loss in terms of commercial, reputational and legal damage that could result from data breaches is one reason why businesses would be cautious about undertaking data refinement or exploiting the personal data they have to improve their bottom line.

5 But does regulation inhibit innovation, or does it in fact create a framework for growing the opportunities for innovation? This article will examine how the PDPA has been adapted to address growing opportunities for innovation within organisations and across corporate groups.

6 In addition, beyond the perspective of individual organisations or their corporate groups, this article will also review how data sharing within a business community or ecosystem might be facilitated through regulatory adaptation. This article will explore this point by looking at efforts in other territories to identify what the structures for community/ecosystem data sharing might look like, and what a legal regime to facilitate such an open data sharing ecosystem might cover.

II. Is regulation a shackle on innovation?

7 The view that regulations need to be adapted to encourage innovation has been stated about data protection laws in other jurisdictions. For example, in the context of the European Union's ("EU's") General Data

---

161 *Procedia Computer Science* 731; and Tim M Schendzielorz, "A Guide to Data Transformation" *Analytics Vidhya* (15 January 2020).

2 Act 26 of 2012.

Protection Regulation ("GDPR"), it has been argued[3] that innovations in artificial intelligence ("AI") applications rely on access and repurposing of data and that the EU GDPR does not position the EU well for such innovation, as the quote below states:

> The GDPR has had a number of unintended negative consequences for the EU's competitiveness in AI. Indeed, it has become clear that because the GDPR was initially drafted in 2014, before awareness of machine learning was widespread, policymakers did not properly consider its impact on AI. In many ways, it would have been better to have delayed the GDPR process by a year or two, as that would have given drafters more insight into the algorithmic economy. Nevertheless, *this oversight has made the GDPR unfit for the emerging algorithmic economy. In particular, the GDPR has created artificial scarcity of data by making it more difficult for organizations to collect and share data. In addition, it has made it more difficult for companies to use AI applications that automate decision-making regarding individuals using personal information. As a result, the GDPR has put the EU at a competitive disadvantage in the development and use of AI.* [emphasis added]

8 A differently nuanced view, however, might be that data protection laws act not as mere hindrances on the exploitation of personal data but rather to set rules of engagement for organisations to collaborate with each other. After all, if there are rules that can be relied on by parties hoping to exchange their data, then those rules might well help increase (if not be a substitute for) the trust needed to ensure that the data can be shared.

9 This thinking can be illustrated by looking at a theory about one of the roles of contract law, *ie*, that its role is premised on facilitating trust between parties who do not have a relationship of trust in order to move forward in a collaboration. Like any theory, there are different perspectives that can be taken on this point, but the thesis that parties rely on contracts as a way to bridge a trust gap has merit.[4]

10 This is a utilitarian perspective to contract law, namely that parties to a *private* arrangement (or private treaty) can approach each other and facilitate more complex and riskier exchanges of promises in the confidence

---

3 Eline Chivot & Daniel Castro, "The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy" *Center for Data Innovation* (13 May 2019).

4 This article is indebted to the insightful discussion in Anthony J Bellia, "Promises, Trust, and Contract Law" (2002) 47 Am J Juris 25.

that these promises will be honoured. After all, if Party A can show that Party B promised it would not abuse personal data entrusted to it, Party A might be able to manage its stakeholders' expectations and/or objections over Party A's engagement with Party B.

11 But this perspective need not be confined to contract law and indeed, whether it is trust law, property law, or other laws, the fact is that social and economic interactions are arguably facilitated and bolstered by laws generally. The general expectation that laws will be enforced and that the rule of law will apply are key assumptions and the basis on which individuals can indeed be placed into interactions that would not otherwise have happened due to the absence of trust.

12 This is no different for data protection law. Consumers trust that data privacy statements and consent restrictions will be honoured, and so they disclose their data to organisations.[5] Organisations will, in turn, look to data protection law and the consents and policies in place as a point of reference for what they can and cannot do with the personal data they receive. In this way, an organisation sharing data with another would do so knowing that it is not only contract law but also the PDPA that could create risks for a counterparty who wishes to renege on a promise concerning how it would handle personal data entrusted to it.

13 Additionally, the manner and means that an organisation would look to share data would be shaped by the rules under the PDPA. Unlike contracts, which are private treaties, the PDPA impacts the conduct of persons outside the bilateral or even multilateral contractual arrangements, since these only apply to contractual counterparties (or identified third-party beneficiaries in legal systems which permit the conferment of benefit to non-contracting third parties).[6] An example of this would be how the PDPA approaches unauthorised re-identification from anonymised data.

---

5 Indeed, even where there is no data privacy law *per se*, the idea that a privacy statement should not be deceptive has been one of the theories of liability that the Federal Trade Commission in the US uses to pursue actions involving consumer harms arising from misuse of personal data, under the unfair and deceptive acts and practices (or UDAP) rules under § 5 of the Federal Trade Commission Act of 1914.

6 As in the case of the Contracts (Rights of Third Parties) Act (Cap 53B, 2002 Rev Ed).

Whilst a disclosing party to a contract might well impose contractual prohibitions against unauthorised re-identification on the receiving party (and this could well be followed up with robust contractual provisions and audit rights to verify compliance), such contractual prohibitions pale in comparison and ability to restrain such unauthorised activity through the risk of criminal penalties and prosecution under s 48F of the PDPA. As prohibited conduct under criminal provisions, the prohibition applies whether or not a rogue employee of the receiving party was himself or herself a party to the contract, and subsequent recipients/individuals do not need to be under back-to-back contractual obligations for that prohibition to apply.

14 This suggests that there is a role for legislatures to play in order to use data or facilitate data sharing for innovation. Contractual and private arrangements between parties certainly do have their role, but legislatures and regulators play a role that private actors cannot – namely, to broaden or adapt laws to give further legislative frameworks to enhance data sharing.

15 For the sake of analysis, one could classify such adaptations of laws to be targeted at two levels: first, rules used to enhance opportunities to innovate within each organisation (or their groups) ("Internal Data Innovation Uses"); and second, rules to enhance or promote data sharing as part of the larger economy – *ie*, through fostering data sharing in a business ecosystem or community ("Community Data Sharing Uses").

III. Targeted adaptation of laws: Recent changes to the Personal Data Protection Act

16 With respect to Internal Data Innovation Uses, organisations or their corporate groups apply the personal data they have for use cases for their own business needs. In order to facilitate this through legal frameworks, the law will need to adjust rules that give organisations a regulatory pathway to pursue use cases for personal data in a way that is responsible and minimises harm. It can also encompass arrangements where the organisation shares personal data with service providers so as to access skill sets and resources which it could not feasibly have or, at least, not adequately deploy in-house.

17 In this regard, the PDPA has welcomed adaptations including:

(a) the explicit recognition of the business improvement exception ("the BIP exception") to the consent obligation,[7] which covers:[8]

(i) "[i]mproving, enhancing or developing new goods or services";

(ii) "[i]mproving, enhancing or developing new methods or processes for business operations in relation to the organisation's goods and services";

(iii) "[l]earning or understanding [the] behaviour and preferences of individuals (including groups or individuals segmented by profile)"; or

(iv) "[i]dentifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals";

(b) the expansion of the deemed consent framework to include a new process to include deemed consent by notification[9] ("DCN route").

18 Both the BIP exception and DCN route present organisations with pathways to execute data analytics and other operations against personal data which can be used to innovate and enhance their businesses, leveraging the possibility of business insight from the personal data that has been collected through their operations.

19 They are also carefully calibrated adaptations. The BIP exception and DCN route each are complemented by stakeholder-interest-balancing provisions.

---

7 Personal Data Protection Act 2012 (Act 26 of 2012) First Schedule, Part 5; Second Schedule, Part 2, Div 2. See also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 12.71–12.83.

8 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 12.71(a)–12.71(d).

9 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A; for further reading, see Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 12.23–12.26.

20 The BIP exception, for example, is not a "back door" through which the repurposing of personal data for marketing purposes can be achieved.[10] There are threshold requirements before the pathway becomes available,[11] including obligations to enter into contractual and other arrangements such as binding corporate rules for data sharing between group companies.

21 The DCN route is similarly a balanced adaptation to the PDPA, with provisions requiring the execution of an assessment to determine (a) that specific thresholds as to adverse effect are not crossed;[12] (b) that specific measures to bring the use case to the data subject's attention are achieved;[13] and (c) the ability to identify and implement measures to eliminate, reduce or mitigate adverse effects.[14]

22 In short, these are pathways that foster innovation with a framework to address risk. This laying down of a framework helps to reduce uncertainty or unstructured risk taking. Significantly, the provisions for BIP also provide a framework for business improvement and cover data sharing within a group of companies[15] as well, which is a recognition of how they collaborate and share data across business divisions.

23 Whilst not strictly a recent amendment to the PDPA, the *Guide to Managing Data Intermediaries*[16] is a fuller statement of the ways in which organisations are expected to address the handling of data intermediaries, including those who could be engaged to process personal data such as data cleansing or transformation.

---

10 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.78.

11 Namely, the business improvement purpose cannot reasonably be achieved without the use of the personal data in an individually identifiable form, and the use of the personal data for this purpose does not have any adverse effect on the individual to whom the personal data relates: Personal Data Protection Act 2012 (Act 26 of 2012) First Schedule, Part 5, para 3.

12 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A(4)(*a*).

13 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A(4)(*b*).

14 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A(5).

15 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.73.

16 Issued September 2020.

24 Other options include regulatory sandboxes, which could also open options for organisations to experiment in different business models or use cases for the personal data that they have. These provide opportunities for organisations to push an innovative use case or model concerning the use of personal data within relaxed (albeit temporarily) regulatory standards.

IV. Facilitating Community Data Sharing

25 Turning to Community Data Sharing, the focus is now on adaptions to the law that provide a regulatory pathway to data sharing between differently owned businesses so as to access new data use case opportunities and provide new options to data subjects.

26 On this, it should be noted:

(a) In the case of the data subject, the premise of Community Data Sharing is that the individual can gain access to more service providers and receive benefits from more competition for their monetary spend and for permissions to use their data.

(b) In the case of the organisations, the case for Community Data Sharing is premised on the notion that businesses want access to more data and are prepared to contribute the personal data that it has gained (in a safe and lawful way) as the price of gaining access to this wider data.

27 In this area, one can point to the enacted but (as at the time of the writing of this article) as-yet-in-force data portability provisions[17] ("Portability Provisions") which were rules promulgated which have been expressly adapted to give data subjects greater control over their personal data.[18] In particular, the public consultation document ("Portability Consult") of 22 May 2019 is explicit about how the intent of the new Portability Provisions is to give individuals the right to facilitate access to

17 The recently enacted Part VIB of the Personal Data Protection Act 2012 (Act 26 of 2012), not yet in force at the time of the writing of this article.

18 See, broadly, Personal Data Protection Commission, *Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions* (22 May 2019).

other service providers.[19] As a concept, data portability is not a novel matter; it has precedents in other legal systems and this is a common premise in enacting such provisions.

28 Under the Portability Provisions, data sharing across differently owned businesses is driven by the data subject, where the objective of the data sharing is to provide the consumer with greater choice, and foster competition. Where it might also foster innovation is where the portability request creates an opportunity for a business to apply personal data collected for one use case to be used for another.

29 The fact that the data subject is driving the request means that the would-be innovating business would have to establish the relationship with the data subject, convince him or her of the potential value of the new use case, and then procure that data subject's mandate to implement the data portability operation.

30 The data subject may be at the centre of this, but it is not hard to see an infrastructure and business model that could develop around the data subject's decisions. "Data Portability-as-a-service" operators could be envisioned – a layer of intermediaries whose business is to facilitate the transfer of personal data between service providers. One could also envision service providers whose business is to help build up aggregations of data that can be, subject to the data subject's mandate, perhaps working off a data-as-a-service model[20] or becoming a hub by which insights could be built.[21]

31 If open data sharing is widely embraced, a network effect of having more data points and an intermediary economy involving accredited service providers qualified against licensing or codes of conduct can emerge.

---

19 Personal Data Protection Commission, *Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions* (22 May 2019) at para 1.4.

20 For a quick definition of data-as-a-service, see Techopedia, "Data as a Service (DaaS)" (last updated 12 May 2017) <https://www.techopedia.com/definition/28560/data-as-a-service-daas> (accessed November 2021).

21 For a discussion of how data as a service might be employed to cleanse or transform data, see Keerthipriyan, "Data as a Service" *Walmart Global Tech* (13 November 2020).

32 Broader initiatives that move into open data sharing models could potentially pave the way for the development of supply chains, infrastructure, business and commercial models that facilitate the exchange of data in a structured and accountable manner to realise the economic effects of open data sharing. In short, it could boost the establishment of data-as-the-new-oil supply chains, refineries, brokerage systems, marketplaces and distribution systems for insight, or access to data that was mentioned at the start of this article – *ie*, a full business ecosystem built on the premise that data, including personal data, can be lawfully and securely harnessed by businesses across any industry for the benefit of data subjects and businesses alike.

33 To use a colloquialism, this is not "pie-in-the-sky" thinking. Other communities in the world have attempted to articulate this vision of data sharing, and there is good learning to be had from looking at how these attempts have fared, if only to be informed of the issues that need to be addressed. An example of how this has been undertaken is in the context of developments in the EU.

V. Attempts at developing the European Union data space and data sharing

34 For instruction, one also can look, as a starting point, at the proposals for the development of a European data space as part of the European Strategy for Data,[22] where it was stated that:

> The aim is to create *a single European data space – a genuine single market for data*, open to data from across the world – where *personal as well as non-personal data*, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, …. *It should be a space where EU law can be enforced effectively*, and *where all data-driven products and services comply with the relevant norms of the EU's single market*. To this end, the EU should *combine fit-for-purpose legislation and governance to ensure availability of data,*

22 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* (COM/2020/66 final) (18 February 2020).

> *with investments in standards, tools and infrastructures as well as competences for handling data*. [emphasis added]

35 Indeed, the need for "fit-for-purpose" legislation was affirmed as part of a public consultation on the European Strategy for Data which was conducted from 19 February 2020 to 31 May 2020.[23] Among notable findings, the policy premise emerging from the findings was that governments would take the lead to facilitate data sharing by promoting interoperability, tools/platforms for sharing and fair commercial terms for data sharing; encouraging data sharing in the public interest (or data altruism); and providing funding for this data sharing. There was an acknowledgment that data scarcity exists in the European digital space.

36 To that end, the draft Data Governance Act[24] ("DGovA") is an attempt to fill this need, and its notable features include the following:

> (a) *Government-to-business ("G2B") (public sector) data sharing* is meant to apply to data not covered by the Open Data Directive,[25] which addresses G2B data sharing in respect of public sector data. The excluded data is data which is not accessible due to commercial and statistical confidentiality and data for which third parties have intellectual property rights.
>
> (b) *It envisages a class of trusted data intermediaries* whose business is to facilitate the exchange of data. *Specific categories of such intermediaries* may also apply (*eg*, service providers that focus on personal data). These would be subject to certification as a means of regulating their activities – these would be certified via a self-notification to authorities of their entering the data intermediary space, with subsequent monitoring for continued certification thereafter. *Other participants include data co-operatives*, which are meant to strengthen the position of individuals.

---

23 European Commission, *Summary Report on the Open Public Consultation on the European Strategy for Data* (24 July 2020).

24 Draft as at March 2021: *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance* (COM(2020) 767 final) (25 November 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767> (accessed December 2021).

25 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

(c) *It promotes public data sharing for no gain (data altruism)*,[26] but there would be a registration system – *ie*, organisations which seek to support data altruism could be registered as such (data altruism organisations or "DAOs") for recognition within the EU. DAOs are to be not-for-profit entities. DAOs can collect information but this would, under the EU GDPR, be via consent of the data subjects or through permissions to grant access to data-by-data holders.

(d) *It is meant to be "fully" compliant with the EU GDPR*, and respect data subject rights – *ie*, it is meant to be consistent with (and not clash with) the EU GDPR. It is also meant to work alongside proprietary intellectual property ("IP") rights in data, *ie*, it will not change the law on IP rights as to databases.[27]

(e) *An expert group known as the European Data Innovation Board* is to be established to develop best practices by EU member states on data sharing.

(f) *Competition law concepts and principles* are meant to apply – *eg*, requiring public sector bodies to comply with competition law when applying principles for reuse of data held, and applying prohibitions against renewing pre-DGovA exclusivity agreements between data holders and data re-users, ensuring that terms imposed on reuse of data are limited to only what is necessary to preserve the rights of third parties.

(g) *Safeguards* such as anonymisation of personal data in appropriate cases are to be implemented, and protection of IP or trade secrets and

---

26 "Data altruism" is a term meant to cover activity where individuals or companies make data voluntarily available for reuse, without compensation, for the common good, such as for scientific research or improving public services. The draft Data Governance Act proposes a registration and monitoring regime for organisations that facilitate data altruism. They will need to operate under certain conditions – *eg*, not-for-profit basis, legal independence (such as in respect of corporate control), transparency obligations, *etc*.

27 In this regard, it should be noted that the EU Database Directive (Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases) introduced proprietary law giving copyright over mere data, a position not adopted in some other legal systems.

commercially sensitive data are to be in place, with differentiated rules for more sensitive data (*eg*, health data).

37 The initial draft of the DGovA was reviewed, and issues were raised concerning its alignment with the principles and concepts of the EU GDPR. The opinions of the European Data Protection Board and European Data Protection Supervisor, jointly expressed,[28] pointed out areas of tension and conflict with the EU GDPR.

38 A full discussion of these tensions would merit a fuller examination in a separate article, but as a broad summary, the objections included that the DGovA would create the risk of establishing a parallel set of rules concerning the handling of personal data which would be inconsistent with the EU GDPR, and that safeguards and disciplines long established under the EU GDPR ought not to be lowered or compromised in the name of promoting a European data space.

39 It is instructive, however, that the DGovA anticipates a particular structure: licensed or accredited intermediaries and DAOs, the application of best practice conduct and codes, *etc*. There are parallels too in the case of the Australian Consumer Data Right[29] ("AU CDR"), where some similarities can be found.[30]

40 Additionally, besides fit-for-purpose legislation, other components to foster Community Data Sharing include developing data sharing solutions at the technological and operational levels. In this regard, Community Data Sharing requires an articulated framework by which organisations can establish common standards or protocols concerning the sharing of data, whether this is a matter of managing application programming interfaces

28 European Data Protection Board, EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Version 1.1, 9 June 2021).

29 References as to the structures in place, and the rules and processes can be found at the Consumer Data Right website <https://www.cdr.gov.au/>.

30 A fuller examination of the Australian Consumer Data Right framework is beyond the scope of this article but a detailed review and good read on these developments can be found in Emma Leong, "Open Banking: The Changing Nature of Regulating Banking Data – A Case Study of Australia and Singapore" (2020) 35(3) BFLR 443.

across databases and systems or standards over data minimisation or data anonymisation.

41 Perhaps some of this work can be gleaned from the progress at the EU level where multi-EU member state initiatives in GAIA-X have made headway in addressing these other issues. GAIA-X is a data sharing structure that envisions a decentralised and federated data space which conforms to a homogeneous system or set of standards for an open data sharing infrastructure.[31] The collaborations in a project like GAIA-X include a wide spectrum of industry participants,[32] and arguably, the broader the traction, the greater network effect in the utility of such a platform for data exchange.

42 Notably, GAIA-X requires that organisations apply certain standards and criteria – it is an implicit price of admission to the network. Once organisations meet the criteria for GAIA-X, they may obtain independent certification, and this can provide a basis and framework under which organisations can enter into data sharing arrangements which are aligned with EU law, and facilitate investment in projects within the European digital single market.

43 There are doubts and questions, to be sure. Would data subjects contribute their personal data out of purely altruistic purposes? Would organisations share what they consider to be "crown jewels" in the form of personal data collected through their operations? How real would the benefits be? No easy answers are available for these issues.

44 It is notable though, that a proposition for data sharing can be framed as a mutually beneficial arrangement, where private interests can be served

---

31 The reader is encouraged to visit the site for GAIA-X, and a useful link can be found at GAIA-X, "FAQs on the GAIA-X Project" <https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/FAQ/faq-projekt-gaia-x.html> (accessed November 2021).

32 According to a report: "Founding members of GAIA-X include 22 companies from a cross-section of industries: Amadeus, Atos, Beckhoff, Bosch, BMW, DE-CIX, Deutsche Telekom, Docaposte, EDF, Fraunhofer, German Edge Cloud, Institut Mines Telecom, International Data Spaces Association, Orange, 3DS Outscale, OVHcloud, PlusServer, Safran, SAP, Scaleway, and Siemens." See Liam Tung, "Meet GAIA-X: This Is Europe's Bid to Get Cloud Independence from US and China Giants" *ZDNet* (8 June 2020).

effectively (whether to assist consumers in getting more out of their interactions using their data, or businesses getting access to reservoirs of data not otherwise available without burdensome investment).

45 Nevertheless, DGovA, GAIA-X and the AU CDR all present useful precedents to learn from. The chief value, it is submitted, lies in determining how far the articulation of a proposed ecosystem and rules set needs to go in order to facilitate Community Data Sharing. These examples could provide useful examples of what structures for community/ecosystem data sharing might look like, and what routes or options to adapt the legal regime (whether by modifications to the PDPA itself or by complementary and harmonised new legislation) might be available.

VI. Conclusion

46 This article began by asking what appeared to be a rhetorical question that emphasised or reinforced the incompatibility of an analogy drawn between data and oil. Having discussed the nuances around data sharing, it is not hard, however, to envision how that comparison might help draw out some vision of where data sharing, and an economy or business ecosystem buffeted by data sharing, could develop further.

47 Indeed, with the right legislative approaches[33] and adaptations to data sharing, and with effective platform standards and solutions to implement and operationalise data sharing, it is possible to see a future where open data sharing across the economy becomes a measured, regulated and healthily managed phenomenon which produces economic benefits to a wider range of stakeholders including both businesses and consumers alike.

---

33 Like the Australian Consumer Data Right, though, it might be useful to take a measured, sector-by-sector approach, perhaps beginning with industries which are regulated (and thus having businesses which are experienced and practiced in compliance thinking).

DAWN OF A NEW AGE FOR THE NOTIFICATION OBLIGATION[*]

Jansen AW[†]
LLB (National University of Singapore); Advocate and Solicitor (Singapore); CIPP/E, CIPP/A, CIPM, FIP

TING Chun Yen[‡]
LLB (Monash University); Advocate and Solicitor (Singapore)

I. Introduction

1 In a move to accommodate modern commercial arrangements and to support data use for business innovation in an increasingly digital economy,[1] the recent amendments to the Personal Data Protection Act 2012[2] ("PDPA") which have come into effect on 1 February 2021 bring about promising developments to the data protection landscape in Singapore. In addition to increasing the recognised exceptions to consent under the PDPA, a key amendment is the expansion of the categories of deemed consent under the PDPA to include not only deemed consent by contractual necessity but also deemed consent by way of notification of the purpose for data processing. With these changes, the Notification Obligation under the PDPA gains new meaning and features more significantly than before.

2 Under the Notification Obligation, organisations are required to inform individuals of the purposes for which their personal data will be collected, used and disclosed before such data can be collected for such purposes. If individuals were not previously informed of any new

---

* Any views expressed in this article are the authors' personal views and should not be taken to represent the views of their employer/law firm. All errors remain the authors' own.

† Partner, Donaldson & Burkinshaw LLP.

‡ Senior Associate, Donaldson & Burkinshaw LLP.

1 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

2 Act 26 of 2012.

purpose(s) for use or disclosure of personal data, the organisation is required to inform the individual of such new purpose(s) before the use or disclosure for that purpose.[3] Organisations must also be acutely aware as to when their use and disclosure of personal data falls within the scope of its previously informed purposes, or falls under a different purpose where consent has yet to be obtained.

3 Strict compliance with the Notification Obligation, however, carries with it the rise in consent fatigue, especially in the digital age where there are increasing newfound purposes in the use of personal data.[4] With the sheer volume of data needed and collected, and the speed of such data collection, organisations find themselves having to repeatedly engage with consumers to notify them of new purposes of data use and to obtain consent. The problem is exacerbated when organisations provide customers with lengthy data protection policies and notices, or seek to prepare broadly worded notices that do not allow individuals to properly ascertain or comprehend the purposes for which their data is collected. Conversely, individuals are not able to provide meaningful consent for the collection, use and disclosure of their personal data.[5] This could undermine the very premise of obtaining consent itself.

4 Some solutions to obtaining meaningful consent include innovative ways of ensuring notification, such as providing consumers with just-in-time notifications or adopting dynamic consent, especially when more sensitive types of data such as health-related data are involved.[6] Such means of notification help to break down information to more granular choices, providing for a more interactive interface allowing users to easily modify and tailor consent suited to their specific preferences, thereby allowing for more meaningful consent.

---

3 Personal Data Protection Act (Act 26 of 2012) ss 20(1)(*a*) and 20(1)(*b*). See also s 20(1)(*c*).

4 Chester Toh & Tan Jen Lee, "With Personal Data Comes Great Responsibility" *The Business Times* (6 March 2019).

5 Ministry of Communications and Information and the Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection (Amendment) Bill* (14 May 2020) at para 4.

6 Personal Data Protection Commission, *Guide to Notification* at p 21 <https://www.pdpc.gov.sg/help-and-resources/2019/09/guide-to-notification> (accessed November 2021).

5 In conjunction to these solutions, the new deemed consent by notification provisions also pave the way forward for obtaining consent. Under the new s 15A of the PDPA, a further category of deemed consent is introduced whereby organisations can deem that individuals have consented to the collection, use or disclosure of personal data for a purpose that they had been notified of and they have not taken any action to opt out of the collection, use or disclosure of their personal data. Individuals have to take steps to actively opt out of such deemed consent if they do not wish for their data to be collected, used or disclosed for the new purpose. The safeguards in place are that organisations are to carry out an assessment of the likely adverse effects on the individual, and identify measures to eliminate, reduce the likelihood of or mitigate the adverse effects identified.[7]

6 This article will consider the interplay of the deemed consent by notification provisions with the existing Notification Obligation under the PDPA and examine how these provisions seek to strike a delicate balance between encouraging data innovation and ensuring adequate protection of one's personal data. Ultimately, a shift towards an approach premised on accountability would help to strengthen consumer trust and business reputation as well as increase organisational competitiveness. This in turn will also give organisations greater assurance in using data for its legitimate business purposes having the requisite safeguards in place.

II. Delving into the "new" Notification Obligation of deemed consent by notification

7 The main facets of the expanded category of deemed consent by notification place the responsibility on organisations to conduct a risk and impact assessment of the "likely adverse effect" to the individual, as well as to take appropriate measures to ensure adequate notification is provided together with a reasonable opt-out period. These aspects will be considered in turn.

7 Personal Data Protection Act 2012 (Act 26 of 2012) ss 15A(2) and 15A(4).

A. Effective and adequate notification

8 As the name suggests, the requirement of notification features heavily in the new category of deemed consent by notification. Organisations must take reasonable steps to ensure that the notification they provide to their customers is adequate. This includes bringing to the attention of the individual the organisation's intention to collect, use or disclose the personal data, and the purpose for which the personal data will be collected, used or disclosed. Individuals must also be notified of and provided a reasonable period and a reasonable manner by which they may notify the organisation that they do not consent to the organisation's proposed collection, use or disclosure of the personal data.[8]

9 In ensuring that individuals are duly notified for the purposes of deeming consent, the considerations when applying the Notification Obligation remain relevant. Organisations should consider the following:

(a) **The information and details to be included in the notification**. Organisations must take reasonable steps to bring to the attention of individuals the purpose for which their personal data will be collected used or disclosed. The purpose has to be framed with the appropriate level of detail for individuals to determine the reasons and manner in which the organisation will be collecting, using or disclosing their personal data.[9] An organisation need not specify every activity it will undertake in relation to collecting, using or disclosing personal data, but should inform the individual of its objectives or reasons in relation to such personal data.[10] A yardstick may be to consider whether stating the purpose with greater specificity would help or hinder the individual understanding the purpose(s) for which his personal data would be collected, used or disclosed.[11]

---

8 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A(4)(*b*).

9 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A(4)(*b*)(ii); Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 14.15.

10 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 8.2.

11 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 14.15 and 14.16.

(b) **The mode, manner and form of the notification**. In order to ensure that the notification is effective in bringing to the individual's attention the proposed collection, use or disclosure of his personal data, the organisation should consider the usual mode of communication between the individual and the organisation. Direct modes of notification are recommended as a default to minimise the risk that individuals do not see the notification.[12] When direct communication channels such as mail, e-mail messages, telephone calls or SMS (subject to the Do Not Call provisions) are available, these can be an effective means for organisations to notify individuals. If mobile apps are used by the organisation, push notifications may be possible, but this would require app users to opt in to receiving such notifications. Notices on dashboards or in-app notifications or messages in mobile apps may be a possible alternative. In considering the mode of notification, the demographic of customers may also be a relevant consideration. If the demographic of users is the elderly and/or persons less adept with mobile apps or mobile notifications, direct forms of notification may be more suitable. It is also relevant to consider the number of individuals to be notified. Where the organisation intends to reach out to a large scale of individuals, other forms of mass communication channels may be considered, such as notification through the organisation's social media channels and notification through printed or other news media.

(c) **Timing of the notification**. The timing of such notification becomes particularly relevant when organisations seek to rely on deemed consent by notification. Organisations have to provide individuals with the notification ahead of the collection, use and disclosure in order to ensure a reasonable period for the individual to opt out of such consent. The reasonableness of the opt-out period and the opt-out method employed also becomes relevant. The length of an opt-out period would depend on the particular service provided and the nature and frequency of interaction with the individual. The Personal Data Protection Commission ("PDPC") *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[13] ("Advisory

12 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) Annex B.

13 Revised 1 October 2021.

> Guidelines") suggest pegging the length of the opt-out period to the frequency of the individual's interaction with the organisation. If this is on a daily basis, a shorter opt-out period may be reasonable. However, if the individual interacts with the organisation on a monthly basis, the opt-out period should not be shorter than a month. If the method for opting out is easily accessible, such as via a direct hyperlink from the notification, this may justify a shorter opt-out period.[14]

10 It may also be relevant to consider the time taken for an organisation to process an opt-out request. Internal deadlines and checks should be put in place within the organisation to ensure that no opt-out request is missed prior to the processing of personal data under this new category of deemed consent.

B. Assessment of likely adverse effect(s) and mitigating measures

11 The *raison d'être* behind the deemed consent by notification provisions could be said to facilitate easier access to personal data for business or other legitimate purposes, whilst ensuring sufficient protection for the individual by only allowing personal data to be processed if there is no likely adverse effect to the individual. To give effect to this, organisations are required to conduct a detailed assessment of the likely adverse effects that the proposed collection, use or disclosure of personal data is likely to have on the individual and seek to eliminate or mitigate them. Organisations would by now already be familiar with conducting Data Protection Impact Assessments ("DPIAs"), where the organisation identifies, assesses and addresses personal data protection risks based on their particular functions, needs and processes.[15] It may be useful for an organisation to adapt its existing DPIA to be used for its assessment under the deemed consent by notification provisions.

12 In conducting an assessment to rely on the deemed consent by notification provisions, organisations have to assess *all* reasonably

---

14 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.23(c).

15 Personal Data Protection Commission, *Guide to Data Protection Impact Assessments* (1 November 2017; revised 14 September 2021).

foreseeable risks to and adverse effects on the individual resulting from the intended collection, use or disclosure.[16] This would include the financial, social, physical and psychological effects on the individual.

13 Some considerations in conducting the assessment include:

(a) **The impact of collection, use or disclosure of the personal data on the individual**. This would involve an assessment of the severity and likelihood of any adverse effect that can arise from the collection, use or disclosure of personal data.[17] The more severe and material the adverse effect, the more the stringent mitigating measures that must be available and implemented, without which organisations should not be allowed to deem consent.

(b) **The nature and type of personal data**. Organisations should consider the sensitivity of the personal data that is sought to be collected, used and/or disclosed. If the intended purpose deals with the processing of sensitive personal data such as healthcare records or financial information, the potential adverse effect to individuals would be higher,[18] and more rigorous mitigating measures would be required if the organisation intends to deem consent.

(c) **The demographic of individuals**. When individuals belong to a vulnerable segment of the population such as minors, and individuals with physical or mental disabilities or special needs, the adverse effects may be more severe.[19] If so, more stringent measures ought to be put in place if consent is to be deemed simply by way of notification.

(d) **The extent of data to be collected, used or disclosed**. Organisations should consider how extensive the collection, use or disclosure of an individual's personal data will be, and how such data is intended to be collected, used or disclosed.[20] For accountability,

16 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(a).

17 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(a).

18 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(b).

19 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(b).

20 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(c).

organisations should not collect more data than is reasonably necessary to achieve the said purpose, as more data collected can pose a higher risk and consequently greater adverse effect. If extensive personal data is needed for an organisation's purposes, in such circumstances, it may be better for the organisation to seek express consent from the individual rather than rely on the deemed consent provisions.

(e) **Reasonableness of the purpose of collection, use or disclosure of personal data**. When using or disclosing personal data for a secondary purpose, organisations should consider the primary purpose for which the data was collected. This may affect the reasonableness of using or disclosing the personal data for this new purpose.[21]

(f) **Predictions or decisions arising from the data**. It would also be pertinent to consider whether the predictions or decisions that may arise from the collection, use or disclosure of the personal data are likely to cause physical harm, harassment, serious alarm or distress to an individual. If such predictions or decisions may result in an individual being excluded, discriminated against, defamed or harmed in any way, this could result in severe adverse effects to the individual.[22]

14 After considering all adverse effects, organisations also need to consider the measures that can be taken to mitigate, eliminate or reduce the likelihood of the adverse effect. To this end, it would also be relevant to consider the practicality of implementing these mitigating measures as well as resource costs. It would be pointless for organisations to have flawless policies and protocols in place, without the expertise or manpower to execute these policies.

15 Having regard to the likely adverse effects and the mitigating measures put into place, the organisation then assesses the likely residual adverse effects to the individual. It should only proceed further if there is no residual adverse effect arising from relying on deemed consent by notification provisions.

---

21 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(d).

22 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.69(e).

III. Applying the "new" Notification Obligation

16 The expanded deemed consent provisions are likely to assist organisations in streamlining their processes and practices. The PDPC notes that these provisions would be useful particularly when an organisation wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the personal data for, and it is unable to rely on any exceptions to consent for the intended secondary use.[23]

17 A possible application of the new provisions would be by companies looking to expand their range of services provided to customers, building on the personal data that they have already collected from their customers. For instance, mobile apps such as health or wellness apps collecting user data of daily lifestyle patterns may be able to rely on the expanded deemed consent provisions to also use such data to offer further services such as tailored exercise regimes or personalised food plans. There would be no likely adverse effect to propose such further services, since users would still have to provide their express consent to participate after reviewing the proposed plan. Notification would likely be effective through the mobile app itself. However, as there may be inactive users of the apps, notification by way of e-mail or through social media channels may also be used in conjunction.[24]

18 It may also be possible for organisations to rely on these provisions to enhance their existing services. Drawing from the example in the PDPC's Advisory Guidelines, if a company records calls and collects voice data of customers through its call centre, and subsequently wishes to use such voice data for an additional form of authentication purposes for the customer's account, the company may be able to rely on deemed consent for the latter purpose. As this is an additional form of authentication increasing security, there is no likely adverse effect on the customer in using his personal data for this additional purpose. Depending on the organisation's interactions with its customers, if customers are regularly notified by e-mail, the company can e-mail its customers notifying them of the intended use of

---

23 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.23.

24 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at pp 47–48.

their voice data. A hyperlink may also be provided in the e-mail for customers who wish to opt out.[25]

19 Organisations may also be able to rely on the deemed consent by notification provisions to disclose personal data of their customers to their business partners or related companies for further development of customised products. For instance, a hotel chain may be able to rely on these provisions to share personal data of its members with a travel website company to develop online travel resources and customised travel packages. In this case, there may be no likely adverse effect to its members. The hotel chain can provide notification in the usual manner which it connects with its members, such as by way of e-mail.[26]

20 In applying these provisions, organisations must also be mindful that adequate and effective notification must be given to customers beforehand, and adequate time must be allowed for customers to opt out. This is observed from the example in the PDPC's Advisory Guidelines. If an event company organising an exhibition wishes to deploy sensors to collect facial and movement data to analyse the exhibits visited and the duration spent by each visitor and wishes to rely on the deemed consent provisions, it would not be sufficient to notify attendees simply by a placing a notice at the exhibition venue. The organisation must ensure that attendees are provided with a reasonable period of time to opt out from the collection of their data for this purpose.[27]

IV. Expanded deemed consent by notification *versus* the new legitimate interests exception

21 It is also apposite to consider the new legitimate interests exception, which bears similarity to the deemed consent by notification provisions. Under the legitimate interests exception, an organisation can collect, use or disclose personal data in circumstances where it conducts an assessment and is satisfied that the collection, use or disclosure is in the legitimate interests

25 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at pp 49–50.

26 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at p 49.

27 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at p 50.

of the organisation or other persons (including other organisations), and the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. An openness requirement is also imposed, where the organisation has to disclose its reliance on the legitimate interests exception.[28]

22 To rely on the legitimate interests exception, the organisation must first be able to identify and articulate with sufficient clarity the situation or purpose that qualifies as a "legitimate interest". This is unlike the deemed consent by notification provisions which do not impose any threshold and standard in relation to the purpose in which the intended collection, use and/or disclosure relates to.

23 The heart of both the legitimate interests exception and the deemed consent by notification provisions involves the application of a risk and impact assessment. The considerations in assessing "adverse effect" are similar for both the deemed consent by notification provisions and the legitimate interests exception. However, the legitimate interests exception is framed slightly differently as it involves a balancing test:

> (a) The organisation must first identify the expected benefits of collection, use and/or disclosure of the data.
> (b) Next, the organisation should assess whether there is any likely adverse effect to the individual after applying measures to mitigate the adverse effect.
> (c) The organisation then should consider whether the identified legitimate interests outweigh the residual adverse effect.[29]

24 To this end, the deemed consent by notification provisions are held to a more stringent standard – the organisation can only deem consent if there is no residual adverse effect arising from relying on the deemed consent by notification provisions. This would likely be to balance against the broad circumstances and purposes that the deemed consent by notification provisions may be applicable, as explained above.[30]

---

28 Personal Data Protection Act 2012 (Act 26 of 2012) First Schedule, Part 3.

29 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) Annex C.

30 See para 11 above.

25 There are also other exceptions to consent that organisations may seek to rely on, including the research exception or the business improvement exception. In particular, given the potential breadth of "business improvement" purposes,[31] many purposes that fail to fall within the deemed consent by notification exceptions may purportedly still fall within the business improvement exception on the premise of "improving, enhancing or developing new goods or services".[32] Again, this is not without safeguards. In order to rely on the business improvement exception, organisations will need to ensure that the business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form, and the organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.[33]

26 A similar thread across all these provisions is that organisations are now pushed to think not only of their business purposes but also of the interests of their customers. They now have to conduct a cost-benefit and risk-benefit analysis when processing data to consider the benefits of easier access of processing personal data, weighed against the potential harm that may befall the data subject. In the event of any doubt, it may be best to err on the side of caution and to obtain consent in the traditional way.

V. Accountability as the core of the Notification Obligation

27 It remains to be seen how the new deemed consent by notification provisions will fare when put into practice, and how organisations will leverage on these provisions to streamline their policies and processes as well as justify innovative uses of data.[34] The assessment checklist released by the PDPC is a helpful step-by-step guide and provides a minimal benchmark for organisations to refer to and rely on in performing their risk

31 "Relevant purposes" is defined in para 1(2) under Part 5 of the First Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012).

32 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 12.73 and 12.74.

33 Personal Data Protection Act 2012 (Act 26 of 2012) First Schedule, Part 5.

34 Koh See Khiang, "Notes from the Asia-Pacific Region, 13 Nov 2020" *IAPP* (12 November 2020).

assessments.[35] It is also notable that the PDPC has made clear that it is not mandatory for organisations to adhere strictly to the checklist, and organisations have the latitude to conduct their own assessment to justify their reliance on the deemed consent by notification provisions. This is a recognition by the PDPC that there is no one-size-fits-all method to identify, assess, or address all data protection risks.[36] Organisations should adopt an assessment methodology and format that best allows them to determine the likely adverse effects and mitigating measures, having regard to their specific business and operational needs, as well as their company's individual circumstances.

28 It also remains to be seen how the PDPC would approach organisations' assessments, especially if the PDPC ultimately disagrees with an organisation's notification method, the adverse effects identified, proposed mitigating measure(s) and assessment outcome. For one, it may be practically impossible for organisations to identify *all* likely adverse effects on the individual. To this end, the PDPC has indicated that in determining whether the measures implemented to eliminate or mitigate the likely adverse effects identified are appropriate, it would adopt a commercially reasonable standard.[37]

29 What is clear is that organisations are not given a *carte blanche* to collect, use or disclose personal data.[38] Organisations now bear the onus to ensure and implement accountability measures when relying on the deemed consent by notification provisions. Organisations now have to be even more deliberate and mindful in how they collect, use and disclose personal data. DPIAs become even more essential in an organisation's processes, which in any event makes for good business practice. While some organisations may consider carrying out such risk assessments to be an increase in compliance

35 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) Annex B.

36 See also Personal Data Protection Commission, Guide to Data Protection Impact Assessments (published 1 November 2017; revised 14 September 2021) at para 8.2.

37 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.66.

38 Wilson Ang *et al*, "Singapore's Public Consultation on proposed changes to the Singapore Personal Data Protection Act" *Data Protection Report* (21 May 2020).

costs, requiring organisations to regularly perform such risk assessments could be a positive move to push organisations to be accountable to their relevant stakeholders on how they manage personal data.

30 In this light, it is also recommended that in approaching the "new" Notification Obligation, organisations ought not to force-fit its intended collection, use and disclosure of personal data into the expanded deemed consent provisions or the exceptions to consent under the PDPA. In the spirit of accountability, even if organisations are able to rely on these expanded provisions or exceptions, it may be worthwhile to nonetheless provide fair notice to its customers and stakeholders, as a matter of prudency or based on good practice. Ultimately, such accountability will help to foster greater trust with the public, enhance business competitiveness and provide greater assurance to their customers, all of which are necessary elements for organisations to thrive in today's growing digital economy.

VI. Concluding thoughts

31 Obtaining consent by way of notification is not new. Jurisdictions such as Australia and New Zealand already adopt a notification-based approach towards consent. These jurisdictions also do not include a requirement for a risk or adverse impact assessment.

32 In contrast, the "new" Notification Obligation in Singapore is carefully customised and has taken a form that is tailored to Singapore's needs. The uniquely Singaporean take on the Notification Obligation allows for a careful balance of the interests of companies and individuals. On the one hand, companies are allowed to carry out more data processing activities without being unduly hindered and put off by excessive consent-taking. On the other hand, the obligation for companies to carry out comprehensive adverse impact assessments helps to ensure that the personal data of individuals still remains adequately protected. This must be a win-win situation for all.

CONSENT GRANTED BUT IMPRACTICAL TO WITHDRAW – CONSIDERATIONS IN THE DIGITAL ECONOMY*

LIM Tat†
LLB (Hons) (National University of Singapore),
MBA, LLM (National University of Singapore),
MSc (Construction Law & Arbitration) (With Merit) (King's College London, University of London and National University of Singapore)

HENG Chiew Khoon‡
B Eng (National University of Singapore);
CIPM, CIPP/A

I. Introduction

1 The Personal Data Protection Act 2012[1] ("PDPA") establishes a data protection law that articulates protection via "obligations", *ie*, acts or courses of action to which an "organisation" (as defined in the PDPA) is legally bound to perform, including the discharge of duties or commitments to which compliance to the Act is required. Chief among obligations is the principle of consent; individuals must consent or be deemed to have consented before collection, use or disclosure of personal data is permitted. In addition, consent is considered valid only when

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Founding Partner, Aequitas Law LLP. Lim Tat was called to the Singapore Bar in 1989 and is a Fellow of the Chartered Institute of Arbitrators (UK) and Distinguished Fellow of the International Academy of Mediators (US).

‡ Data Protection Manager, Aequitas Law LLP. Heng Chiew Khoon is an independent data protection consultant and practising data protection officer with certifications from the International Association of Privacy Professionals.

1 Act 26 of 2012.

individuals are notified and informed on the purpose for the personal data collection.[2]

2 The PDPA can be considered as a "consent-first" law, that is, consent to collection, use or disclosure of personal data is always required, unless there is an exception to the need for consent.[3] In contrast, the European Union's General Data Protection Regulation[4] ("GDPR") treats consent as the correct lawful basis only if no alternative is available.[5]

3 The PDPA provisions allow for individuals to withdraw consent and to be informed of the likely consequences of such withdrawal.[6] Also of significance is the range of exceptions to consent: when data collection is required or authorised under the PDPA or other laws, legitimate interests, evaluative purposes and introduced in the enhanced PDPA;[7] and deemed consent by contractual necessity and notification.[8]

4 This article examines how a combination of the weakening of consent effectiveness and its reduced relevance in the workings of a digital economy contributes to the possibly irrelevance of consent withdrawal by individuals and the impracticality of such withdrawal incurring severe consequences.

---

2 Personal Data Protection Act 2012 (Act 26 of 2012) ss 13(*a*), 14 and 20.

3 Lyn Boxall, "Exceptional Exceptions to Consent" *Data Protection Excellence Network* (24 June 2020).

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").

5 United Kingdom Information Commissioner's Office, "When Is Consent Appropriate?" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/> (accessed 28 July 2021); GDPR Arts 6(1) and 9(2).

6 Personal Data Protection Act 2012 (Act 26 of 2012) s 16.

7 Personal Data Protection Commission, "Enhanced PDPA for Businesses" <https://www.pdpc.gov.sg/Enhanced-PDPA-for-Businesses> (accessed 1 July 2021).

8 Personal Data Protection Act 2012 (Act 26 of 2012) s 15A(4)(*a*).

II. The digital economy and its impact on consent

A. Personal Data Protection Act and the advent of the digital economy

5 The digital economy refers to the production and consumption of goods and services together with the supply of money based on information and communication technology ("ICT"), increasingly perceived as conducting business through markets utilising the Internet and the World Wide Web. Also referred to as the "Internet economy", "new economy", or "web economy", it encompasses everyday online interconnectedness among people, businesses, devices, data and processes using the Internet, mobile devices and the Internet of things.[9]

6 Given that one of the PDPA's goals is to address the increasing use of personal data in the face of rapid technological advancements and deeper complexities associated with the digital economy,[10] it may be said that the PDPA does not attempt to accentuate the role of consent in Singapore's data protection model, instead adopting a balancing approach incorporating necessity, reasonableness and fairness not secured by the Consent Obligation.[11]

7 Increasing the emphasis on the Protection and Accountability obligations may prove a better strategy to encourage outcomes where more effort and resources are put in place to build trust and safeguards within organisations. In 2017, the Personal Data Protection Commission ("PDPC") proposed to reduce the significance of consent partly because of

---

9 See Wikipedia, "Digital Economy" <https://en.wikipedia.org/wiki/Digital_economy> (accessed 1 July 2021).

10 Commissioner of the Personal Data Protection Commission, Tan Kiat How, mentioned at the Personal Data Protection Seminar 2017 (27 July 2017):

> The Digital Economy provides exciting opportunities for businesses and workers. We have seen the rise of platforms in domains such as e-commerce, social media and e-payments, and the growth of vibrant digital ecosystems around these platforms. In these ecosystems, data is the currency of exchange and the basis on which enterprises innovate business models, products and services. Trust is a key lubricant that enables the entire system to function.

11 Yip Man, "Personal Data Protection Act 2012: Understanding the Consent Obligation" [2017] PDP Digest 266.

its inconvenience to the practice of personal data analytics,[12] reducing its role to "where seeking consent is practical" by developing "parallel bases for collecting, using and disclosing personal data".[13] Instead "greater responsibility would be placed on organisations to demonstrate accountability in ensuring the protection of personal data and safeguarding the interests of individuals".[14]

8 A measure of how this responsibility has been found lacking may be observed in PDPC enforcement decisions relating to organisations found to have contravened the data protection provisions under the PDPA.[15] A news article on 2 November 2021[16] reported that 68% of the total number of data breach incidents recorded from April 2016 to October 2021 involved a breach of the entities' Protection Obligation. Learnings include businesses relying on servers insufficiently protected with weak passwords, resigned staff's access still being available and customers' ordering or membership data being exposed due to insecure protocols. The move to transacting online via the Internet has enabled social engineering and phishing attacks by malicious parties and introduced new cybersecurity risks like ransomware. The mass shift to working from home due to the COVID-19 pandemic created challenges in information technology infrastructure, especially in the area of access security, resulting in not insignificant stress for small and large organisations alike. While the Protection Obligation's percentage share of the total number of data breach incidents certainly contributes to an interesting headline, such details from the incidents themselves are perhaps more indicative of the downsides that the digital economy has brought.

---

12 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017) Part II.

13 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017) at paras 3.2–3.3.

14 Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (27 July 2017) at para 3.3.

15 Personal Data Protection Commission, "Enforcement Decisions" <https://www.pdpc.gov.sg/All-Commissions-Decisions> (accessed 3 July 2021).

16 Rei Kurohi, "$2.68 Million in Fines Collected for Personal Data Protection Breaches to Date" *The Straits Times* (2 November 2021).

B. Weakening of consent effectiveness

9 The manifestation of a digital economy is best illustrated through the establishment of e-commerce portals and marketplaces (for example, Amazon.com Inc). The modern Internet marketplace commonly performs an aggregation role of matching supply ("sellers") and demand ("buyers"). It is in the interests of this marketplace to accumulate maximal numbers of each party for revenue maximisation at minimal costs. In 2017, *The Economist* published an article that aptly summarises the thinking that raw data (like crude oil) is not valuable in itself, but rather, when gathered completely and accurately, connected to other relevant data, and processed in a timely manner, new value (like petroleum and jet fuel) is created or realised.[17] It also underscores that for such marketplaces to thrive, data collection and, inevitably, personal data collection of buyers (who normally outnumber sellers) is the actual profitable business, so as to generate greater revenue for sellers or intermediaries through large data sets that may be analysed computationally to reveal patterns, trends and associations, especially relating to human behaviour and interactions (otherwise known as "big data").

10 With the need for personal data collection, so follows the "Privacy Policy" or "Notice". Agreeing to the terms as stated in such documents constitutes consent as defined by most privacy or data protection laws. However, the presupposition of all consent lies in the assumption that the terms are understood and the consent decision is informed. This state can only occur if the privacy policy or notice is actually read and understood.

11 Numerous published surveys on the content, language and length of modern privacy notices of larger organisations reveal that they have become onerous to read and understand,[18] and that the precautionary legalese, vague and elastic form of language may be (if viewed cynically) a deliberate legal risk management strategy. Whether valid or not, such strategies may

---

17 "The World's Most Valuable Resource Is No Longer Oil, but Data" *The Economist* (6 May 2017).

18 See, *eg*, "How Silicon Valley Puts the 'Con' in Consent" *The New York Times* (2 February 2019): "The average person would have to spend 76 working days reading all of the digital privacy policies they agree to in the span of a year. Reading Amazon's terms and conditions alone out loud takes approximately nine hours."

be tested in the courts of law, most likely only when challenged. All of the above results in "consent fatigue"[19] and "consent erosion",[20] whereby consent evolves into a much less effective safeguard for personal data protection.

12 The oft-quoted scope of consent, that pertaining to the collection, use and disclosure of personal data, is normally presented in this three-step "bite-sized" version for conciseness. Upon further elaboration, the complete personal data "life cycle" is then presented with the addition of the storage, retention and disposal phases. Critically, however, the actual control an individual possesses over providing (or denying) meaningful consent beyond the collection phase may be doubtful, or often reduced to deciphering "word play" within the privacy notice.

13 For most Internet portals, the widely accepted convention of creating a user account before commencement of usage is the only opportunity for an individual to provide consent, without which "account verification and creation" cannot proceed and the individual is reduced to a read-only "browsing" person, defeating the objective of the consumer (to, well, consume) in the first place. While the PDPA does provide objections against this scenario of "no consent – no product/service",[21] as commonly articulated, it may not be properly enforceable when organisations use bundled consents against a broad range of operations and purposes, justified with difficulties related to interconnected product classes, operational process complexities or an inadequately defined network of intermediaries.

14 Lastly, the use of data intermediaries, a notable characteristic of a modern digital economy, commonly poses significant challenges for larger organisations to determine actual data flows, lines of control and the extent of data sharing. While the PDPA imposes only the Protection and Retention Limitation obligations directly on data intermediaries, a study of sample PDPC enforcement cases involving data intermediaries reveals that

---

19 Tara Taubman-Bassirian, "How to Avoid Consent Fatigue" *IAPP* (29 January 2019).

20 Lee Soo Chye, Teo Yi Ting Jacqueline & Sheam Zenglin, "Towards Codes and Certifications – The Protection of Personal Data in the Digital Age" [2019] PDP Digest 53.

21 Personal Data Protection Act 2021 (Act 26 of 2012) s 14.

many organisations become complacent, and neglect governance and risk management aspects, with poor oversight and policies contributing to PDPA compliance issues. While such organisations, as data controllers, may logically be expected to articulate the nature of consent given by individuals to include its data intermediaries, in practice individuals may need to invest time and effort to investigate and discover their personal data's "exposure" to each data intermediary before arriving at a consent decision. For individuals, expending such effort goes against one of the basic premises of the digital economy: that of increased speed and efficiency for all.

15 All of the above factors contribute to the weakening of consent effectiveness in the classical data protection toolbox, perhaps relegating it to an easily understandable "concept" but placed at a lower priority compared to the rigours of a modern digital economy demanding speed, lowest cost and other productivity or efficiency metrics.

III. Consent withdrawal in the digital economy: Concept meets reality

16 The digital economy heralded a new paradigm applied especially to software and services; a "free" use model on a time-limited or perpetual basis. News, literature, computer games, interesting but untested software concepts, useful software utilities, even physical deliveries and product samples, for example, could now be obtained on a no-cost basis.

17 An oft-quoted saying, "When a product is free, the user is the product",[22] attempts to explain the true business model of this new paradigm. In April 2018, a public statement by Facebook's chief executive Mark Zuckerberg, who plainly said Facebook sells advertisements[23]

22 Scott Goodson, "If You're Not Paying for It, You Become the Product" *Forbes* (5 March 2012).

23 In April 2018, a telling (and, some would say, hilarious) incident occurred when Facebook's chief executive Mark Zuckerberg was on the US Capitol Hill for the first of two days of congressional testimony on the Cambridge Analytica data leak. Zuckerberg took responsibility for the leak, as well as the company's inability to weed out Russian disinformation during the 2016 US election.

Senator Orrin Hatch, an 84-year-old Utah senator, did not seem to know how Facebook, one of the two biggest advertising companies on the Internet,

(*continued on next page*)

(for profit), concisely explained this new paradigm. Facebook's business model is based on offering its tools and services mostly for free to billions of users and then making money by allowing businesses to show advertisements to Facebook's users. Advertisers pay the price to Facebook that is determined in an auction, based on demand and supply.

18 In the Facebook-Cambridge Analytica data breach incident of March 2018,[24] the acquisition of up to 87 million Facebook users' personal data by Cambridge Analytica (with no explicit permission given to Cambridge Analytica) highlighted the scale on which Facebook had access to its users' personal data, the ease with which such data could be shared without its users' knowledge and, most importantly, the fact that the data sharing had been going on for an extended period despite Facebook's public pronouncements and assurances on data privacy.

19 In effect, the "free" model has created a subtle change in netizens' psyche. When an individual's mental cost-benefit analysis initially stands at zero cost and all benefits, the subsequent inclusion of the "cost" of possibly sharing personal data for perhaps unknown purposes and absent notifications is also discounted to zero. In fact, the utility of sharing more personal data may be increased, as in the case of Facebook usage, if more "friends" can be found.

20 This phenomenon is not limited to social media platforms like Facebook. Users of online mapping tools (for example, Google Maps) may value the utility and convenience, and even marvel at the ingenuity of the software with nary a concern that where Google is concerned, nothing is more valuable than knowing users' locations.

---

made its revenue. Hatch asked Zuckerberg: "So, how do you sustain a business model in which users don't pay for your service?"

"Senator, we run ads", replied a briefly confused Zuckerberg.

See Sean Burch, "'Senator, We Run Ads': Hatch Mocked for Basic Facebook Question to Zuckerberg" *The Wrap* (10 April 2018).

24 See Wikipedia, "Facebook–Cambridge Analytica Data Scandal" <https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal> (accessed 10 July 2021).

21 In a lawsuit brought by the state of Arizona in the US,[25] Google executives had worked to develop technological workarounds to keep tracking users even after they had opted out. Rather than abide by its users' preferences, Google allegedly tried to make location-tracking settings more difficult to find and pressured smartphone manufacturers and wireless carriers to adopt similar measures. Even after users turned off location tracking on their devices or opted out, Google found ways to continue tracking them, according to a deposition from a company executive. In summary, a cynical analysis of this organisation's true objective in creating this software application may lead to the conclusion that it is not so much for assisting the lost; rather, it is to collect even more data, which can be said to have belonged to individuals in the first instance.

22 Therein lies the dilemma: the perceived benefits of convenience, utility and, possibly, fun outweigh any personal data risk, yet to be realised in the absence of any bad news of data breaches or privacy violations. The granted consent, long forgotten or currently irrelevant, results in no requirement or motivation for consent withdrawal. Withdrawal of consent may imply a full closure of the previously created Internet portal "user account", resulting in the total loss of benefits.

23 No doubt the digital economy at large does not solely comprise Facebook, Google or other platforms engaged in nefarious behaviour. However, the same "dulling" of individuals' perception towards the value of and risk to their personal data largely exists, to the extent that any consent withdrawal, though understandable in concept, in reality ("where the rubber meets the road") becomes impractical and possibly even unthinkable. What would the current 2.7 billion[26] monthly active Facebook users say to that? Would you stop using Google maps by withdrawing consent to the sharing of your location data with Google, which the mapping application states (logically) is necessary to mark your current geo-location?

---

25 United States, Attorney General State of Arizona, "Updated Redacted Google Complaint" (21 May 2021) <https://www.azag.gov/media/interest/updated-redacted-google-complaint> (accessed 21 July 2021).

26 Statista, "Leading Countries Based on Facebook audience size as of January 2021" <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/> (accessed 25 April 2021).

IV. Enhanced Personal Data Protection Act and changes in the consent framework

24 On 2 November 2020, the Personal Data Protection (Amendment) Act[27] ("the Act") was passed in Singapore's Parliament, following its introduction in October 2020. The Act seeks to amend the PDPA by (a) strengthening the accountability of organisations in respect of the handling and processing of personal data; (b) enhancing the legal framework for the collection, use and disclosure of personal data; (c) providing individuals with greater autonomy over their personal data; and (d) enhancing the enforcement powers of the PDPC.

25 In force since 1 February 2021, the enhanced PDPA introduces an expanded consent framework, with two new forms of consent: deemed consent by contractual necessity; and deemed consent by notification. New exceptions to the consent regime can be applied, including using, collecting or disclosing data for legitimate interests, business improvement and commercial research and development; and if the legitimate interests of the organisation and the benefit to the public exceed any adverse effect on the individual.

26 With the expansion of the PDPA's consent framework and deemed consent exceptions, consent withdrawal becomes a moot point. The overall effect of organisations receiving more flexibility in legitimate personal data usage and individuals expending less attention on dealing with consent and consent withdrawal falls in neatly with the digital economy's demands for higher productivity and speed of action.

V. Conclusion

27 This article highlights the weakened effectiveness of consent in the original state of the PDPA (with its consent-centric characteristics) in the rising digital economy for which data is the enabler.

28 The traditional method for obtaining "all-or-nothing" consent, through the Privacy Notice mechanism, does not serve the interests of individuals well. The prevalent use of data intermediaries in the digital

27 Act 40 of 2020.

economy complicates the consent relationship once thought to be simply between the individual and the organisation holding his personal data.

29 Consent withdrawal in reality is far more complicated than what theory suggests. The marketplace's paradigm change to "free" models in the digital economy has influenced individuals' behaviour in valuing other benefits above personal data protection. Consent withdrawal may have become a non-starting option.

30 The Act presents a significant revision, aligning the PDPA with rising global standards and trends in data privacy laws. It represents Singapore's recognition of the rise of technology and technology-driven companies built on data utilisation for value creation in the Digital Economy. In particular, revisions to the consent framework reduce focus on the seeking of consent (and corresponding consent withdrawal), and instead provide more flexibility to organisations for business improvements.

THE PUBLIC AVAILABILITY EXCEPTION*

Benjamin WONG†
LLB (Hons) (National University of Singapore),
LLM (London School of Economics);
Advocate and Solicitor (Singapore)

I. Introduction

1 The Personal Data Protection Act 2012[1] ("PDPA") includes a "public availability exception", which exempts organisations from complying with certain data protection obligations when dealing with personal data that is publicly available. This exception represents a clear line drawn by the Legislature, between information in the public domain and information in the private domain.

2 While the public availability exception is not a universal feature of data protection frameworks around the world, Singapore is not unique in this regard. For example, under the California Consumer Privacy Act of 2018, the definition of "personal information" excludes "publicly available information".[2] In addition, both the New Zealand Privacy Act 2020[3] and the European Union General Data Protection Regulation[4] also contain public availability exceptions.

3 The purpose of this article is to discuss the application of the public availability exception in Singapore. To this end, this article will examine the decisions and advisory guidelines of the Personal Data Protection Commission ("PDPC"), among other material.

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors are the author's own.

† Sheridan Fellow, National University of Singapore.

1 Act 26 of 2012.

2 California Civil Code §1798.140(o)(2).

3 Privacy Act 2020 (2020 No 31) s 22, Information privacy principle 2(2)(d).

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC Art 9(2)(e).

II. Relevant data protection obligations

4 It should be emphasised from the outset that, under the PDPA, the public availability exception is not a general exception.[5] It does not provide a blanket exemption from all the data protection obligations. Instead, the public availability exception only affects specific data protection obligations: in particular, it primarily affects the Consent Obligation, Notification Obligation and Transfer Limitation Obligation.

5 First, the Consent Obligation generally requires organisations to obtain consent before collecting, using or disclosing personal data.[6] However, an organisation is exempted from the Consent Obligation when it is collecting, using or disclosing personal data that is publicly available.[7] In such cases, no consent need be obtained.

6 Second, the Notification Obligation generally requires organisations to inform individuals about the purposes of the collection, use or disclosure of their personal data. However, where an organisation is exempted from the Consent Obligation pursuant to the public availability exception, it is also exempted from the Notification Obligation.[8]

7 Third, the Transfer Limitation Obligation prohibits an organisation from transferring personal data outside Singapore, unless it takes "appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations … to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the [PDPA]".[9] However, this

5 This is unlike some of the exceptions found in s 4 of the Personal Data Protection Act 2012 (Act 26 of 2012). For example, the s 4(1)(*a*) exception for "any individual acting in a personal or domestic capacity" provides a general exemption from the data protection obligations: see Benjamin Wong, "The Personal and Domestic Exclusion" [2020] PDP Digest 130.

6 Personal Data Protection Act 2012 (Act 26 of 2012) s 13(*a*).

7 Section 17 of the Personal Data Protection Act 2012 (Act 26 of 2012), read with para 1 of Part 2 of the First Schedule.

8 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(3)(*b*).

9 Section 26(1) of the Personal Data Protection Act 2012 (Act 26 of 2012), read with reg 10(1) of the Personal Data Protection Regulations 2021 (S 63/2021).

requirement is taken to be satisfied by the transferring organisation if the transferred personal data is publicly available in Singapore.[10]

8 All the other data protection obligations (such as the Access, Correction and Accuracy obligations) continue to apply to personal data even if it is publicly available.[11] A pertinent example was given by the PDPC in *Re My Digital Lock Pte Ltd*:[12] even though a photograph of an individual in a public space may be taken without his or her consent, the Purpose Limitation Obligation would "still operate to limit the collection, use or disclosure of such personal data to appropriate purposes".[13]

III. Concept of public availability

9 According to the PDPA, personal data is "publicly available" when it is "generally available to the public".[14] The PDPC has clarified that personal data is generally available to the public "if any member of the public could obtain or access the data with few or no restrictions".[15] The key question, therefore, is what restrictions an ordinary member of the public would face when attempting to access the personal data in question. The burden of proof in this regard rests on the organisation pleading the public availability exception.[16]

10 Thus far, the PDPC's decisions have mainly addressed three distinct scenarios where the public availability exception could potentially apply. These scenarios are examined below.

---

10 Personal Data Protection Regulations 2021 (S 63/2021) reg 10(2)(*e*).

11 See paras 27–30 below for some minor qualifications.

12 [2018] PDP Digest 334.

13 *Re My Digital Lock Pte Ltd* [2018] PDP Digest 334 at [39]. See generally Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25.

14 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

15 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.85. See *Re Exceltec Property Management Pte Ltd* [2018] PDP Digest 184 at [32].

16 See *Re My Digital Lock Pte Ltd* [2017] PDP Digest 146 and *Re Amicus Solutions Pte Ltd* [2020] PDP Digest 404 for cases where the organisation failed to prove the public availability of the personal data concerned.

A. Free-access record

11 It is reasonably clear that, where personal data is *freely* accessible on a public record without restrictions, that personal data is publicly available, and the public availability exception applies to that personal data. This may be observed from two PDPC decisions.

12 In *Re Selby Jennings, a trading style of Phaidon International (Singapore) Pte Ltd*,[17] the complainant had uploaded his *curriculum vitae* ("CV") on an online platform ("eFinancial"), which made his CV and contact details publicly available. When he was later contacted by the organisation about an employment opportunity, the complainant instructed the organisation to remove his CV and contact details from its database as he did not wish to be contacted about further job opportunities. However, due to an oversight by the organisation's employee, the organisation continued to contact him on two further occasions. The complainant filed a complaint with the PDPC about the organisation's continued use of his personal data despite his express withdrawal of consent. The PDPC found that the organisation was not in breach of the Consent Obligation because, throughout the material time, the personal data of the complainant was available on eFinancial, and there were "no restrictions placed on any user or recruitment company from accessing the information on eFinancial".[18]

13 Similarly, in *Re Strategem Global Recruitment Pte Ltd*,[19] the complainant had registered with the organisation as a job seeker. Subsequently, the complainant had instructed the organisation that he no longer wished to receive information about job opportunities. However, due to a technical glitch, the organisation continued to e-mail the complainant. The PDPC found that the organisation did not breach the Consent Obligation because the complainant's CV was publicly available at the material time on another job search platform.[20]

---

17 [2017] PDP Digest 206.

18 *Re Selby Jennings, a trading style of Phaidon International (Singapore) Pte Ltd* [2017] PDP Digest 206 at [8].

19 [2017] PDP Digest 209.

20 *Re Strategem Global Recruitment Pte Ltd* [2017] PDP Digest 209 at [4].

B. Restricted-access record

14 The situation is more complex in cases where access to the public record in question is subject to some restrictions. Some PDPC decisions have addressed this scenario.

15 In *Re Exceltec Property Management Pte Ltd*,[21] the residents of three condominiums made complaints against their respective Management Corporation Strata Titles ("MCSTs") or managing agents. Broadly speaking, the residents' complaints were about the disclosure of their personal data (including their names, unit numbers and voting shares) on notice boards and web portals. It was alleged that the disclosures were in breach of the Consent Obligation and Notification Obligation.

16 The PDPC found that there was no breach of the Consent Obligation and Notification Obligation. Among other reasons, this was because the public availability exception applied to the residents' personal data.[22] Here, the PDPC pointed out that residents' names, unit numbers and voting shares could be found in the strata roll, which all MCSTs were obliged to maintain.[23] Under the Building Maintenance and Strata Management Act[24] ("BMSMA"), there were "few restrictions" on accessing the strata roll: all that had to be done was to make an application to the MCST and pay the prescribed fee.[25] Although the BMSMA theoretically limited access to the strata roll to a defined class of people, this class included prospective purchasers and mortgagees; thus, in practice, it was difficult to ensure that an applicant fell within the class, and "almost any member of public" could claim to be a prospective purchaser and gain access to the strata roll.[26] In addition to the strata roll, some of the personal data could also be purchased from the Singapore Land Authority.[27]

17 *Re Exceltec Property Pte Ltd* is instructive because it demonstrates that formal obstacles to accessing a record, such as fees and application procedures, do not necessarily prevent the personal data therein from being

---

21 [2018] PDP Digest 184.
22 *Re Exceltec Property Pte Ltd* [2018] PDP Digest 184 at [38]–[39].
23 *Re Exceltec Property Pte Ltd* [2018] PDP Digest 184 at [34].
24 Cap 30C, 2008 Rev Ed.
25 *Re Exceltec Property Pte Ltd* [2018] PDP Digest 184 at [35].
26 *Re Exceltec Property Pte Ltd* [2018] PDP Digest 184 at [34]–[35].
27 *Re Exceltec Property Pte Ltd* [2018] PDP Digest 184 at [36].

publicly available. Further, it demonstrates that the focus is on the *real and practical* restrictions on access (as opposed to restrictions that are merely theoretical and legal).

18 The subsequent case of *Re Xbot Pte Ltd*[28] was consistent with *Re Exceltec Property Pte Ltd*. In that case, the organisation had developed a mobile application and website that provided access to their database of residential property transactions. The PDPC found that there was no breach of the Consent Obligation because the personal data on the database was publicly available – they had in particular been obtained from the Urban Redevelopment Authority's Real Estate Information System and the Housing and Development Board's "Resale Flat Prices" portal, and the information therein was available to the public, although in some cases a fee was payable.[29]

C. *Publicly observable data*

19 Apart from recorded data, the PDPA specifies that personal data is also publicly available when it "can be observed by reasonably expected means at a location or an event" at which the individual appears and that is open to the public.[30] It appears that the legislative intent behind this subcategory of "publicly available data" was "not to unduly limit activities performed in the public under reasonable situations, such as photography in public places".[31]

20 In its advisory guidelines, the PDPC clarified two key elements of this subcategory. First, personal data "can be observed by reasonably expected means" when the individual concerned "ought to reasonably expect their personal data to be collected in that particular manner at that location or event", and the test here is an objective one.[32] Second, a location or event is considered "open to the public" if "members of the public can enter or

28 [2020] PDP Digest 292.

29 *Re Xbot Pte Ltd* [2020] PDP Digest 292 at [10].

30 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

31 *Parliamentary Debates, Official Report* (15 October 2012), vol 89 at p 831 (Assoc Prof Dr Yaacob Ibrahim, Minister for Communications and Information).

32 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.90.

access the location with few or no restrictions", and the fact that some restrictions exist does not necessarily mean that the location or event is not open to the public.[33]

21 One case where this subcategory was applicable was *Re SG Vehicles Asia*.[34] In that case, the complainant had purchased a vehicle from the organisation, and had posed for a photograph with the vehicle in a public car park. The organisation later published the photograph on its website, and did not respond to the complainant's requests to remove the photograph. The PDPC found that this was not a breach of the Consent Obligation because the photograph was taken in an "open area that was accessible to the public", such that "the personal data in question could easily have been observed by reasonable means by members of the public at the material time".[35]

IV. Extension of exception to personal data that was formerly publicly available

22 Does the public availability exception apply to personal data that, despite having been publicly available at one point in the past, has now ceased to be publicly available?

A. Applicability of extension to Consent Obligation and Notification Obligation

23 In relation to the Consent Obligation (and, by necessary extension, the Notification Obligation), the PDPC has taken the view that the public availability exception extends to personal data that was formerly publicly available at the time of collection.

24 According to the PDPC, "so long as the personal data in question was publicly available at the point of collection, organisations will be able to use and disclose personal data without consent" even if the personal data is no

33 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 12.91 and 12.92.

34 [2018] PDP Digest 361.

35 *Re SG Vehicles Pte Ltd* [2018] PDP Digest 361 at [5].

longer publicly available at the point of use or disclosure.[36] In such cases, it would also not be necessary for the organisation to provide notification for the collection, use or disclosure.

B. Applicability to Transfer Limitation Obligation?

25 Should the public availability exception be extended to cover formerly publicly available personal data in the context of the Transfer Limitation Obligation?

26 In the context of the Consent Obligation, the rationale given by the PDPC for extending the public availability exception to cover personal data that was formerly publicly available is that it would be:[37]

> … excessively burdensome for organisations intending to use or disclose publicly available personal data without consent to constantly verify that the data remains publicly available, especially in situations where the use or disclosure happens some time after the collection of the personal data.

It is suggested that the above-mentioned rationale applies in equal force, *mutatis mutandis*, in the context of the Transfer Limitation Obligation: if an organisation has collected personal data on the assumption that it was publicly available, it would likely be excessively onerous for that organisation to check that the personal data is still publicly available every time it wishes to transfer that personal data outside Singapore. Therefore, it would make sense for the extension to also apply to the Transfer Limitation Obligation.

---

36 Personal Data Protection Commission ("PDPC"), *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.88. This was affirmed by the PDPC in *Re Selby Jennings, a trading style of Phaidon International (Singapore) Pte Ltd* [2017] PDP Digest 206 at [9] and in *Re My Digital Lock Pte Ltd* [2018] PDP Digest 334 at [39].

37 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.88.

V. Limitation of exception in situations involving unlawful use of other personal data

27 In the recent case of *Bellingham, Alex v Reed, Michael*,[38] the High Court had the opportunity to interpret the public availability exception in the context of the Consent Obligation. In this case, the court recognised a limitation to the public availability exception: it does not apply to personal data obtained through the unlawful use of other personal data.

28 The plaintiff ("Reed") had brought private action against the defendant ("Bellingham") pursuant to s 32(1) of the PDPA. Reed alleged that Bellingham had, *inter alia*, breached the Consent Obligation in relation to Reed's e-mail address. On the facts, Bellingham had obtained Reed's e-mail address through Reed's LinkedIn account (which was a publicly available source) and subsequently used that e-mail address.

29 The court held that the public availability exception did not apply to Bellingham's non-consensual collection and use of Reed's e-mail address. According to the court, "where personal data that is publicly available is obtained only through the unlawful use of other personal data, s 17(1) of the PDPA cannot apply and the personal data so obtained cannot be collected, used or disclosed without consent".[39] Here, Bellingham had used Reed's name to locate Reed's e-mail address, and the court had earlier found that Bellingham was "not entitled to use or disclose [Reed's name] without Reed's consent".[40]

30 The scope of this implied limitation remains an open question. In particular, it remains to be seen whether the limitation applies only when the "unlawful use" stems from a breach of the PDPA, or whether other types of "unlawful use" (for example, use in breach of confidence) could also trigger this limitation.

---

38 [2021] SGHC 125.

39 *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [37].

40 *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [34]. Alternatively, it could be argued that it was Reed's status as an investor that was the personal data that was wrongfully used.

VI. Other situations involving public availability

31 There are at least three other situations where the public availability of personal data has legal consequences under the PDPA. The foregoing discussion in this article about the concept of public availability will also be relevant in these situations. However, as these situations are beyond the scope of this article, they will be only briefly highlighted here.

32 First, the concept of public availability features in the three new offences for the egregious mishandling of personal data.[41] Under these three new offences – namely, the offences of unauthorised disclosure of personal data, improper use of personal data and unauthorised re-identification of anonymised data – it is a defence for the accused to prove that the information in question was publicly available (but where the information was publicly available solely because of an "applicable contravention", the accused must also prove that he or she did not know and was not reckless as to whether that was the case).[42]

33 Second, the public availability of personal data also affects the new Data Breach Notification Obligation.[43] The Data Breach Notification Obligation generally requires organisations to, *inter alia*, notify the PDPC and affected individuals about "notifiable data breaches".[44] A data breach is "notifiable" if, *inter alia*, it "results in, or is likely to result in, significant harm to an affected individual".[45] "Significant harm" is deemed when the "data breach is in relation to any prescribed personal data or class of personal data" or "in other prescribed circumstances";[46] however, these

41 These offences were introduced in the year 2020 by the Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020).

42 Personal Data Protection Act 2012 (Act 26 of 2012) ss 48D(2)(*a*), 48E(2)(*a*) and 48F(2)(*a*). See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 23.3.

43 The Data Breach Notification Obligation was introduced in the year 2020 by the Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020).

44 Personal Data Protection Act 2012 (Act 26 of 2012) ss 26D(1) and 26D(2).

45 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B(1)(*a*).

46 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B(2). For the list of prescribed personal data and prescribed circumstances, see Part 1 of the Schedule to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021).

prescribed personal data and prescribed circumstances exclude personal data that is publicly available (and that is not publicly available solely because of a data breach).[47]

34 Third, the concept of public availability also features in the Access Obligation. The Access Obligation generally requires organisations to provide individuals with access to their personal data upon request.[48] Exceptionally, organisations are prohibited from providing such access where providing access could reasonably be expected to "reveal personal data about another individual".[49] However, the PDPC has clarified that this prohibition does not apply where any exception to the Consent Obligation (including the public availability exception) allows the disclosure of the other individuals' personal data without consent.[50]

VII. Conclusion

35 The public availability exception is a "significant exception" within the data protection framework of the PDPA.[51] The significance of this exception is likely to grow, as increasing amounts of personal data become available online, and as smart city initiatives result in more personal data being collected from public spaces. It is hoped that this article will be useful in clarifying the scope of application of this important exception.

---

47 Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021) Schedule, Part 2, paras 1(*a*) and 2. See also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.16.

48 Personal Data Protection Act 2012 (Act 26 of 2012) s 21(1).

49 Personal Data Protection Act 2012 (Act 26 of 2012) s 21(3)(*c*).

50 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 15.34.

51 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.84.

REVIEW OF DECISIONS RELATING TO THE REGULATION OF DATA COLLECTION, USE AND DISCLOSURE*

Benjamin WONG†
LLM (London School of Economics),
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

I. Introduction

1 This review examines the decisions issued in the year 2020 by the Personal Data Protection Commission ("PDPC"), that relate to the regulation of data collection, use and disclosure. The focus is on those data protection obligations in the Personal Data Protection Act 2012[1] ("PDPA") that constrain the processing of personal data by organisations. The relevant data protection obligations include the Consent Obligation, Purpose Limitation Obligation, Retention Limitation Obligation and Transfer Limitation Obligation.

II. Consent Obligation

2 The Consent Obligation prohibits organisations from collecting, using or disclosing personal data about an individual unless (a) the individual's consent has been given or deemed to have been given; or (b) the collection, use or disclosure of the individual's personal data, without consent, is required or authorised under the PDPA or any other written law.[2]

3 *Re Majestic Debt Recovery Pte Ltd*[3] addresses the Consent Obligation.

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors are the author's own.

† Sheridan Fellow, National University of Singapore.

1 Act 26 of 2012.

2 Personal Data Protection Act 2012 (Act 26 of 2012) s 13.

3 [2020] SGPDPC 7.

4 *Re Majestic Debt Recovery Pte Ltd* involved a company, Majestic Debt Recovery Pte Ltd ("MDR"), that was in the business of collecting debts. MDR had been engaged by a creditor to collect a debt from a debtor company. MDR sent its representatives to visit the premises of the debtor company, during which those representatives exchanged heated words with the debtor company's personnel. The representatives recorded video footage of the exchanges (which included footage of the complainant and other personnel of the debtor company) and posted it on MDR's official Facebook page. This was done even though the complainant had protested against the taking and uploading of the video recording.

5 The PDPC found that MDR had acted in breach of the Consent Obligation, because MDR's representatives had uploaded the video recording on Facebook despite the complainant's protests, thereby disclosing the complainant's personal data to the public without the complainant's consent.[4] Whilst MDR claimed to have had obtained prior consent (both express and implied), it could not provide evidence of such consent, and even if the purported consent had indeed been obtained, that consent would have been effectively withdrawn by the complainant's express protestations.[5]

6 It is notable that in *Re Majestic Debt Recovery Pte Ltd*, the PDPC also expressed doubts about the very possibility of obtaining valid consent in cases like the present. This was because it was considered "unlikely or even unconceivable that an individual who owed a debt would willingly consent to be filmed by the debt collecting agency calling on him, and for such recordings to be posted on social media".[6] Further, even if consent were superficially obtained *ex ante*, there was a "real risk" that such consent could be vitiated "as having been obtained through unfair, or deceptive or misleading practices";[7] for example, where consent was unreasonably made a condition for the obtaining of the loan.[8]

---

4 *Re Majestic Debt Recovery* [2020] SGPDPC 7 at [6].

5 *Re Majestic Debt Recovery* [2020] SGPDPC 7 at [13]. See s 16 of the Personal Data Protection Act 2012 (Act 26 of 2012).

6 *Re Majestic Debt Recovery* [2020] SGPDPC 7 at [7].

7 *Re Majestic Debt Recovery* [2020] SGPDPC 7 at [7]. See ss 14(2) and 14(3) of the Personal Data Protection Act 2012 (Act 26 of 2012).

8 *Re Majestic Debt Recovery* [2020] SGPDPC 7 at [13].

III. Purpose Limitation Obligation

7 The Purpose Limitation Obligation requires that organisations collect, use or disclose personal data only for purposes (a) "that a reasonable person would consider appropriate in the circumstances"; and (b) "that the individual has been informed of under section 20 [of the PDPA], if applicable".[9]

8 *Re Majestic Debt Recovery Pte Ltd* addresses the Purpose Limitation Obligation.

9 The facts of *Re Majestic Debt Recovery Pte Ltd* have been summarised above.[10] In this case, as an aside to its finding of a breach of the Consent Obligation, the PDPC also noted that the posting of a video recording of a debt collection visit on social media, for the purpose of shaming the debtor, could be in breach of the Purpose Limitation Obligation as there was a "real risk that this purpose may not be one which a reasonable person would consider appropriate".[11]

10 *Re Majestic Debt Recovery Pte Ltd* appears to be consistent with the PDPC's previous decision in *Re Club the Chambers*,[12] in terms of its treatment of the disclosure of personal data for the purposes of shaming. However, it is difficult to draw a general conclusion that the purpose of shaming will in all cases be inconsistent with the Purpose Limitation Obligation, and it is suggested that due account should be taken of the particularities of each case – these may include the sensitivity of the personal data involved, and the specific reasons for which the individual concerned is being shamed.[13]

IV. Retention Limitation Obligation

11 The Retention Limitation Obligation mandates that an organisation must "cease to retain its documents containing personal data, or remove the

---

9 Personal Data Protection Act 2012 (Act 26 of 2012) s 18.

10 See paras 2–6 above.

11 *Re Majestic Debt Recovery* [2020] SGPDPC 7 at [7] and [13].

12 [2019] PDP Digest 304 at [22].

13 For a broader discussion on the Purpose Limitation Obligation, see Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25.

means by which the personal data can be associated with particular individuals", once it is reasonable to assume that (a) "the purpose for which that personal data was collected is no longer being served by retention of the personal data"; and (b) "retention is no longer necessary for legal or business purposes".[14]

12 *Re Singapore Red Cross Society*[15] and *Re Times Software Pte Ltd*[16] address the Retention Limitation Obligation.

13 In *Re Singapore Red Cross Society*, the Singapore Red Cross Society ("SRCS") suffered a data breach of its blood donor appointment database, resulting in the exfiltration of the personal data of approximately 4,297 individuals.

14 In respect of the personal data of approximately 900 of the affected individuals, the PDPC found that SRCS was in breach of the Retention Limitation Obligation, as SRCS had unnecessarily retained that personal data.[17] This happened because SRCS gave incorrect instructions to its vendor when purging personal data from the blood donor appointment database, resulting in an incomplete purge; the error was not detected by SRCS as SRCS failed to verify that the purging exercise was done correctly.[18]

15 *Re Times Software Pte Ltd* involved Times Software Pte Ltd ("Times"), an information technology ("IT") services vendor. Times had been engaged by Dentons Rodyk & Davidson LLP ("Dentons") and TMF Singapore H Pte Ltd ("TMF") for certain payroll and/or human resource services. For this purpose, both Dentons and TMF provided Times with employee personal data. This personal data was stored in Times' file server system ("FSS"). Due to a technical error, the FSS was made accessible via the Internet, such that the employee personal data stored therein was exposed over the Internet.

16 Preliminarily, the PDPC found that Times was the data intermediary of both Dentons and TMF, in its processing of employee personal data on

14 Personal Data Protection Act 2012 (Act 26 of 2012) s 25.
15 [2020] SGPDPC 16.
16 [2020] SGPDPC 18.
17 *Re Singapore Red Cross Society* [2020] SGPDPC 16 at [7].
18 *Re Singapore Red Cross Society* [2020] SGPDPC 16 at [7].

behalf of, and for the purposes of, both Dentons and TMF.[19] This did not exempt Times from the Retention Limitation Obligation because, whilst data intermediaries are generally exempt from the PDPA's data protection obligations "in respect of [their] processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing", data intermediaries remain bound by the Retention Limitation Obligation (among other specified obligations).[20]

17 In respect of the employee personal data given by TMF, the PDPC found that Times was in breach of the Retention Limitation Obligation.[21] According to Times, TMF had provided Times with employee personal data for, *inter alia*, Times to develop a new software functionality.[22] However, Times had failed to delete the employee personal data after the new software functionality had been implemented and the need for retaining the employee personal data had come to an end.[23]

18 In both *Re Singapore Red Cross Society* and *Re Times Software Pte Ltd*, it may be observed that the PDPC highlighted the failure of SRCS and Times, respectively, to *check* that unnecessary personal data was actually deleted.[24] Although the presence or absence of checks is not relevant to the establishment of liability (since the Retention Limitation Obligation is framed in absolute terms), checks can reduce the likelihood of an organisation breaching the Retention Limitation Obligation, and evidence of checks may perhaps be relevant to the sanction that is imposed on an errant organisation.

V. Transfer Limitation Obligation

19 The Transfer Limitation Obligation prohibits an organisation from transferring personal data "to a country or territory outside Singapore except in accordance with requirements prescribed under [the PDPA] to

19 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [9].
20 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(2).
21 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [14].
22 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [4].
23 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [14].
24 See *Re Singapore Red Cross Society* [2020] SGPDPC 16 at [7] and *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [14].

ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under [the PDPA]".[25]

20 *Re Singapore Technologies Engineering Ltd*[26] addresses the Transfer Limitation Obligation.

21 *Re Singapore Technologies Engineering Ltd* involved Singapore Technologies Engineering Limited ("STE"), a company that was incorporated in Singapore. STE had a subsidiary (VT San Antonio Aerospace Inc or "VT SAA") that was based in the US. VT SAA suffered a ransomware attack, in which the personal data of 287 individuals in Singapore was potentially exposed to unauthorised access. As the affected personal data had previously been transferred by STE to VT SAA, from Singapore to the US, the question that arose was whether this transfer had been done in accordance with the Transfer Limitation Obligation.

22 In this case, STE was found to be in compliance with the Transfer Limitation Obligation.[27]

23 In general, an organisation that wishes to transfer personal data out of Singapore must "take appropriate steps to ascertain whether, and to ensure that" the recipient is bound by "legally enforceable obligations" to "provide to the transferred personal data a standard of protection that is at least comparable to the protection" under the PDPA.[28] "Legally enforceable obligations" include obligations imposed on the recipient by binding corporate rules ("BCRs").[29] Here, STE had put in place BCRs regulating the transfer of personal data out of Singapore.[30]

24 An organisation relying on BCRs must ensure that the BCRs meet a number of substantive requirements.[31] In the present case, the BCRs implemented by STE satisfied those substantive requirements. In particular,

---

25 Personal Data Protection Act 2012 (Act 26 of 2012) s 26(1).

26 [2020] SGPDPC 21.

27 *Re Singapore Technologies Engineering Ltd* [2020] SGPDPC 21 at [7].

28 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(1)(*b*), now Personal Data Protection Regulations 2021 (S 63/2021) reg 10(1).

29 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(1)(*c*), now Personal Data Protection Regulations 2021 (S 63/2021) reg 11(1)(*c*).

30 *Re Singapore Technologies Engineering Ltd* [2020] SGPDPC 21 at [8].

31 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(3), now Personal Data Protection Regulations 2021 (S 63/2021) reg 11(3).

the PDPC found that: (a) the BCRs were legally binding on all of STE's "direct and indirect subsidiaries worldwide"; (b) the BCRs "specified the countries and territories to which personal data may be transferred"; (c) each company receiving transferred personal data was legally bound to provide a standard of protection to the personal data that was "at least comparable to the protection under the PDPA"; and (d) the BCRs specified rights and obligations, including the "permitted purposes for transfer of personal data, data protection obligations of the receiving company, and protection and security of personal data".[32]

25 *Re Singapore Technologies Engineering Ltd* is notable for being the first PDPC decision in which the concept of BCR has been applied. It demonstrates how a Singapore-based organisation can rely on the BCR mechanism to transfer personal data outside of Singapore. In this regard, it should be borne in mind that BCRs "may only be used for recipients that are *related* to the transferring organisation" [emphasis added].[33] A recipient is "related" if (a) the recipient controls the transferring organisation; (b) the recipient is controlled by the transferring organisation; or (c) the recipient and the transferring organisation are under the control of a common person.[34] In situations where the recipient is non-related, legally enforceable obligations may instead be imposed by contract.[35]

---

32 *Re Singapore Technologies Engineering Ltd* [2020] SGPDPC 21 at [8].

33 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(3)(*c*), now Personal Data Protection Regulations 2021 (S 63/2021) reg 11(3)(*c*).

34 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(4), now Personal Data Protection Regulations 2021 (S 63/2021) reg 11(4).

35 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(1)(*b*), now Personal Data Protection Regulations 2021 (S 63/2021) reg 11(1)(*b*).

ACHIEVING ACCOUNTABILITY THROUGH DATA PROTECTION BY DESIGN*

Steve TAN†
LLB (National University of Singapore),
LLM (University College London);
CIPP/A

Justin LEE‡
LLB (Singapore Management University)

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Partner and Deputy Head, Technology, Media and Telecommunications/Data Privacy practice group, Rajah & Tann Singapore. Steve Tan has been appointed Adjunct Professor of National University of Singapore teaching "Privacy & Data Protection Law" at the law faculty. Highly regarded for his expertise in data privacy and technology law work, Steve has pioneered several data-protection-related services which organisations have found valuable. Steve has been recognised as a leading lawyer in *PLC Cross-border Media and Communications Handbook, Asia Pacific Legal 500, AsiaLaw Profiles, Practical Law Company Which Lawyer, Chambers Asia Pacific, Best Lawyers, The International Who's Who of Telecoms and Media Lawyers*, and *Who's Who Legal: Data*. Steve has been named Communications Lawyer of the Year in the Corporate Livewire 2015 Legal Awards and in Corporate Insider Business Excellence Award 2019. Steve is cited as "one of the best in the field of personal data protection" in *Legal 500* 2017 and as being "one of the gurus in the field of data protection" in *Legal 500* 2019. Steve is a Certified Information Privacy Professional (Asia) (CIPP/A).

‡ Senior Associate, Technology, Media and Telecommunications/Data Privacy practice group, Rajah & Tann Singapore. In the course of his practice, Justin Lee has advised clients on a wide range of transactional and regulatory matters with a particular focus on data privacy, intellectual property and technology law.

I. Introduction

1 The year 2020 saw the continued transformation of the economic landscape in Singapore and the rest of the world towards a highly data-driven digital economy, with the COVID-19 global pandemic serving to significantly accelerate this evolution. With a large proportion of the workforce working from home and the ability for people to meet and interact with each other in-person limited or discouraged, many businesses have been forced to place greater emphasis on the digitalisation of their commercial and operational processes and systems in order to continue to be able to effectively connect with their customers and business partners. This brought about a concomitant growth in the collection, creation and processing of data by organisations, with much of such data comprising personal data. Consequently, for many organisations, there is now a burgeoning bias towards digital data being their key asset. Unfortunately, unlike tangible physical assets, data in digital form is often overlooked, and arising from the mirage of invisibility of such digital assets, many organisations fail to put in place sufficient measures to secure such digital assets.

2 Against this backdrop of accelerated economic digitalisation, the regulatory approach adopted by the Personal Data Protection Commission ("PDPC") in recent years has proven to be prescient, robust and pragmatic. As tacit recognition of the fact that data is the fuel that drives a vibrant digital economy, the PDPC has consistently sought to adopt a regulatory approach which strikes a healthy balance between encouraging more effective and innovative use of data by organisations and the need for stronger accountability in the management of personal data by such organisations. The PDPC's key regulatory objective in this regard would be to create a strong culture of accountability in the management of personal data among organisations in Singapore, whereby organisations are able to provide the necessary degree of confidence to the individuals whose personal data they possess or control, that such organisations have proactively identified and addressed risks to their personal data. This in turn benefits accountable organisations as they would have created a solid foundation on which they can safely leverage personal data in new and innovative ways.

3 A core element of accountability in the management of personal data is the need for organisations to be able to proactively identify, assess and

mitigate risks to personal data in their possession or control, bearing in mind that vectors of risk and vulnerability reside with the use of information and communication technology ("ICT") systems and operational processes that organisations leverage on to process personal data. As such risks will only become more pronounced as organisations continue to digitalise significant aspects of their operations, it is critical that organisations take active steps to ensure that the ICT systems and processes being used/deployed in their digitalised business operations are designed, developed, implemented and used in a manner which embraces the need for accountability, and that the personal data being processed by such systems or through such processes is adequately protected.

4 In doing so, organisations would do well to take guidance from the PDPC's *Guide to Data Protection by Design for ICT Systems*,[1] as well as relevant enforcement decisions issued by the PDPC dealing with the data protection obligations in the context of organisations' ICT systems, processes or activities. Data protection by design[2] ("Data Protection by Design") is, in essence, the application of data protection principles right from the start when coming out with a new product or solution, or when an organisation undertakes activities involving the processing of personal data. In more simplistic terms, it entails a concerted effort in applying the data protection obligations under Singapore's Personal Data Protection Act[3] ("PDPA") to the new product, solution or activity at the inception during their design. By doing so, the risk of the organisation suffering a breach of any of the data protection obligations under the PDPA, with respect to the new production, solution or activity it is intending to commercialise or undertake, will be significantly reduced. Data Protection by Design could be said to be practising the maxim of "prevention is better than cure". Therefore, through the practice of Data Protection by Design, organisations will be well poised to showcase their accountability in complying with the PDPA's data protection obligations. The concept of

1 Published 31 May 2019.

2 This concept has its origins in or is influenced by the "Privacy by Design" framework that was created by Dr Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canada.

3 Personal Data Protection Act 2012 (Act 26 of 2012).

accountability[4] pervades the PDPA. Accountability, in essence, is where an organisation demonstrates responsibility for all personal data within its possession and control and has put in place measures to ensure that it complies with all the data protection obligations in the PDPA. Though the concept of Data Protection by Design is not expressly mentioned in the PDPA, one can clearly see the intimate link between Data Protection by Design and accountability, in that the application of Data Protection by Design by an organisation to its internal processes, its business operations, and its products and services, will facilitate that organisation in being accountable for personal data within its possession or control.

5 There are many use cases for practising Data Protection by Design. For example, if an organisation is developing an online platform to conduct e-commerce, right from the outset, it would need to embed principles of data protection within the software that powers the online platform as well as the underlying processes through which personal data is collected, used and processed by the organisation. This would include but is not limited to:

(a) considerations of administering notification of purposes to a customer when the customer first provides personal data to the organisation when creating an account with the organisation and obtaining appropriate consent;

(b) deciding the types of personal data to be collected, limited only to those which are absolutely necessary to achieve the reasonable purposes of processing;

(c) ascertaining the protection measures to be deployed for such personal data including encryption and/or anonymisation;

(d) entering into contracts with appropriate data protection provisions with data intermediaries which the organisation would be engaging to process such personal data;

(e) ensuring settings within the platform are set to a high privacy level; and

(f) extensive security testing of the online platform before it goes live.

4 As exemplified by ss 11 and 12 of the Personal Data Protection Act 2012 (Act 26 of 2012) and buttressed by the new data breach notification obligation.

6 This article will briefly discuss and highlight some key areas of guidance that can be extracted from some of the PDPC's recent enforcement decisions,[5] in order for organisations to better understand how the practice of Data Protection by Design, such as the application of the principle of end-to-end security across the various stages in the life cycle of development and use of their ICT systems, could have averted potential breaches of the PDPA.

II. Key areas of guidance from recent enforcement decisions issued by the Personal Data Protection Commission

7 With respect to software development or software modification which many organisations embark on in this digital economy, one of the key but commonly overlooked tenets of Data Protection by Design is that data protection must be a primary consideration right from the beginning of the software development life cycle, when the specifications and requirements of the relevant ICT system are being articulated, such that data protection principles can be hardwired into the architectural design of the ICT system. This ensures that accountability in data protection is thoughtfully integrated into the design of the ICT system from the get-go. If the ICT system is being developed by a third-party vendor, such specifications and requirements (including the data protection principles captured therein) must be clearly communicated in writing to the vendor in a sufficiently comprehensive manner. From a practical perspective, it may very well require the development project to have as a member of its core team a data protection specialist, who would be able to bring to the table data protection insights, which the technical functional team members can interweave into the design of the system.

8 The PDPC's decision in *Re The Future of Cooking Pte Ltd*[6] is instructive in this regard. This decision involved a text file containing the personal data of 178 unique individuals who had made a purchase on The Future of Cooking Pte Ltd's ("TFC's") e-commerce website. The text file was publicly accessible via a certain Uniform Resource Locator ("URL") for approximately three months as a result of a bug in a plugin installed on the TFC e-commerce website. The PDPC found that the failure by TFC to

5 They are in the main decisions issued in 2020.

6 [2020] SGPDPCS 23.

specify appropriate data protection measures to be adopted for the website by the third-party vendor that was carrying out a redesign of the e-commerce website, as well as a failure to conduct security testing of the website before it went live after the redesign, resulted in the exposure of TFC's customers' personal data.

9 This decision is one of several enforcement decisions issued by the PDPC in past years which have flagged the failure of organisations to impose adequately clear and comprehensive written data protection obligations on their vendors that are either developing a software which will be processing customers' personal data or engaged to process personal data on their behalf. It can be seen that if TFC had adequately considered the application of Data Protection by Design in carrying out its e-commerce website redesign project, the failures highlighted by the PDPC could have been averted.

10 It should be noted that the foregoing learnings need not be limited to the development of ICT systems and can apply equally to all other data processing activities which an organisation could undertake. In such cases, the organisation should consider how data protection principles can be purposefully integrated into the data processing activity being undertaken (*ie*, the practice of Data Protection by Design) and accordingly ensure that there are appropriate measures in place to deal with the data processing activity at hand. The PDPC's decision in *Re Times Software Pte Ltd*[7] is instructive in showing how breaches that occurred from either an action or omission on the part of an organisation could have been avoided through careful consideration of the consequence of that action or omission. In other words, the application of Data Protection by Design would result in the organisation paying careful thought and consideration to the consequence of certain activity that is being conducted in relation to an existing software or system and consequently leading to behaviour or measures that would avert the breach that had occurred. In this decision, Times Software Pte Ltd ("Times") was a data intermediary for three customers in carrying out data processing activities including the use of its payroll software. Times had received these customers' employee-related data ("Employee Data") which it had stored in its file server system ("FSS"). The FSS suffered a hard disk failure. Consequently, Times restored a backup of

7 [2020] SGPDPC 18.

the Employee Data in the FSS and reset the FSS operating system settings to their default settings, which resulted in the disabling of the password protection feature. This meant that the Employee Data was exposed to web crawlers and indexed by the Google search engine and stored in Google's cache as the FSS was accessible over the Internet. Times was found to be in breach of the Protection Obligation. Though it was acknowledged that Times had a standard operating procedure ("SOP"), the PDPC stated that: "Times should have ensured that their SOP included specific procedures that were designed to reasonably detect non-compliance and to discourage deliberate, reckless or careless failures to adhere to the SOP by its employees." The PDPC also found that Times should have encrypted personal data in the FSS, and should not have used live customer data for testing purposes. Looking at the facts of the case, it may be said that a stringent application of Data Protection by Design in the conduct of its operations and handling of Employee Data in the FSS could have averted the breach. Times had put in place certain remedial measures[8] post-breach and it may be said that a robust Data Protection by Design approach from the start could have brought about the application of one or more of such remedial measures before such a breach were to happen; this in turn could have averted the breach.

11 The application of a Data Protection by Design framework in dealing with the development of any ICT systems would not only entail ensuring that robust data protection measures are communicated to and imposed on the vendor prior to the commencement of any development work, but would also include organisations exercising proper supervision and monitoring over the vendor during the development phase, so as to ensure that sufficient data protection measures are baked into any development work. In *Re Singapore Red Cross Society*,[9] the PDPC found that the Singapore Red Cross Society's ("SRCS's") lack of supervision over the work of its third-party website developer had led to a failure by SRCS to detect the presence of a phpMyAdmin database administration tool (used to manage the blood donor appointment database that was accessible via the SRCS website), with the aforementioned tool being the vulnerability subsequently used by unauthorised individual(s) to exfiltrate the blood donors' personal data from the database. This vulnerability was

8 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [8(a)].

9 [2020] SGPDPC 16.

compounded by the fact that SRCS did not have in place a password management policy requiring strong passwords of sufficient length and complexity during the development phase, which resulted in a weak password (*ie*, "12345") being set for the tool. Furthermore, there were no regular security reviews of its systems which could have allowed a reviewer to have weeded out the tool. Some of the personal data was found by the PDPC to have been retained by SRCS in breach of the Retention Limitation Obligation.[10] This case showcases how all-encompassing the application of Data Protection by Design could be for an organisation's operations, including dealing with issues of eradicating weaknesses in the security of ICT systems where personal data is reposed, ensuring that there are measures in place to securely destroy personal data once the organisation has no legal or business purpose to continue retaining such personal data.

12 Following the completion of the development of the software or ICT system comes what can arguably be considered a critical phase of the software development life cycle, namely, the testing phase. Based on the PDPC's enforcement decisions in 2020, it is evident that organisations need to pay significantly more attention to the testing phase when developing and implementing any software or ICT system; a sizeable number of the PDPC's enforcement decisions in 2020 included findings by the PDPC that the organisation in question had failed to conduct adequate testing of its software or ICT systems, which could have permitted the discovery of problems with the software or ICT system which eventually led to the data breach for which the organisation was investigated by the PDPC.

13 In some decisions, the PDPC has consistently highlighted that proper user testing and security testing are critical parts of the reasonable security arrangements that organisations must make in discharging their obligations under the PDPA's Protection Obligation. In particular, such user testing and security testing should mimic real world usage and must be sufficiently comprehensive in covering all reasonably foreseeable circumstances in which the software or ICT system in question may be used. Some examples of one or more of the above points are as follows:

---

10 Personal Data Protection Act 2012 (Act 26 of 2012) s 25.

(a) In *Re COURTS (Singapore) Ptd Ltd*,[11] the PDPC found that the organisation's testing scenarios for its membership programme platform should have included the possibility of multiple sequential logins by different users or even concurrent logins by different users at peak usage.

(b) In *Re Grabcar Pte Ltd*,[12] the organisation had not conducted tests to simulate multiple users accessing its mobile app, whether concurrently or consecutively, and also had not conducted any specific test to verify how the mobile app update it was introducing would interact with the existing caching mechanism in its mobile app.

(c) In *Re The Central Depository (Pte) Limited*,[13] the PDPC found that the organisation should have included the scenario of a change of address by a user as part of its test for a certain module in its project to migrate from its previous post trade processing software to a new post trade processing software, as such testing would have had a reasonable chance of detecting the error within the software which caused account holder dividend cheques to be mailed to outdated addresses.

(d) In *Re BLS International Services Singapore Pte Ltd*,[14] the PDPC found that the organisation had not conducted sufficiently extensive testing on its booking system and therefore failed to detect a coding error within the URL encryption feature of its booking system.

(e) In *Re Novelship Pte Ltd*,[15] the PDPC highlighted that the organisation had not conducted adequate testing prior to the launch of its website. The testing conducted by the organisation had been limited to design and functionality issues. Notably, the testing carried out did not include vulnerability scanning on the website. If the organisation had conducted the necessary vulnerability scanning, it would have detected that its website was vulnerable to URL manipulation, which is one of the top ten security vulnerabilities listed by the Open Web Application Security Project.

11 [2020] SGPDPC 17.
12 [2020] SGPDPC 14.
13 [2020] SGPDPC 12.
14 [2020] SGPDPCS 24.
15 [2020] SGPDPCS 15.

14 These enforcement decisions are arguably a clear indication that the lack of adequate user testing and security testing for software and ICT systems are a common failing among organisations who have suffered data breaches and/or have breached the Protection Obligation under the PDPA. It would therefore be pertinent for organisations in Singapore, particularly those who are currently undertaking digitalisation of their business operations, to take note of the learnings from these enforcement decisions in order to ensure that they are aware of the level of user testing and security testing that is expected by the PDPC as well as the various real-world scenarios that such testing will need to encompass, and accordingly plan for the necessary testing in a thoughtful and deliberate manner with Data Protection by Design in mind.

III. Conclusion

15 Accountability dictates that an organisation adequately protects personal data within its possession or control. Accountability can be facilitated through the application of Data Protection by Design to an organisation's processes, activities, products, services and development of software and ICT systems. By carefully considering and embedding data protection principles into all aspects of an organisation's operations where personal data may be involved, the organisation can safely navigate circumstances similar to the cases considered in this article, and thereby avert a possibility of the organisation itself suffering a data breach. It is hoped that organisations take heed of the problem areas identified in the PDPC's enforcement decisions and take the necessary steps to ensure that they approach the digitalisation of their business and operations with the principles of Data Protection by Design at the forefront of their consideration, in order to achieve the level of accountability expected by their customers.

PERSONAL ACCOUNTABILITY UNDER THE PERSONAL DATA PROTECTION ACT: PAST AND PRESENT*

Lanx GOH†
LLB (University of Birmingham), DipSing (National University of Singapore), LLM (Intellectual Property and Privacy Law) (University of California, Berkeley), MSc (Criminology and Criminal Justice) (University of Oxford); CIPM, CIPP/A, CIPP/E, CIPP/US, FIP; Advocate and Solicitor (Singapore); Accredited Mediator (Singapore Mediation Centre and Singapore International Mediation Institute)

Joshua KOW
LLB (Hons) (National University of Singapore); Advocate and Solicitor (Singapore); CIPP/A, CIPP/E, CIPM, FIP, CISSP

* The authors are grateful to Lee Pei Yi, Jamey for her assistance in the preparation of this article. Any views expressed in this article are the authors' personal views only and should not be taken to represent the views or policy positions of their respective employers. All errors remain the authors' own.

† Head of International Privacy and Global Data Protection Officer, Ant Group; Adjunct Associate Professor, National University of Singapore Faculty of Law; Adjunct Law Lecturer, Singapore Management University School of Law. Lanx Goh was formerly the Head of Investigation with the Singapore Personal Data Protection Commission, Data Privacy Senior Counsel with TikTok Pte Ltd, and Senior Legal Counsel and Privacy & Cybersecurity Lead with Klook Travel Technology Limited. He is a member of the Law Society's Cybersecurity and Data Protection Committee and Fellow of Information Privacy and Board Member with the International Association of Privacy Professional, Asia Advisory Board. He is also one of the authors of *Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018) and has spoken at various conferences such as Data Protection in the Digital World Summit, Bulgaria 2019, FTI/HKACC: In-House Counsel: An Integral part of Cybersecurity, IAPP Asia Privacy Forum, and Singapore International Cybersecurity Week 2021.

I. Introduction

1 Since coming into force on 2 July 2014, the Personal Data Protection Act[1] ("PDPA" or "the Act") has ensured a baseline standard of protection for personal data across Singapore's economy by complementing sector-specific legislative and regulatory frameworks.[2] This was achieved by holding organisations accountable for the collection, use and disclosure of individuals' personal data,[3] followed by investigations and administrative enforcement through directions or penalties based on how far they have fallen short.[4]

2 In relation to the scope of enforcement, the Act provides an especially wide definition of what constitutes an "organisation".[5] Yet, while corporate and natural persons[6] both fall within that scope, the published decisions of the Personal Data Protection Commission ("the Commission") have overwhelmingly been against the former rather than the latter.

3 A review of the Commission's decisions to date reveals that only a handful of individuals have ever been found to be personally accountable for violating the Act. Furthermore, any such liability was found only in the context of highly specific factual scenarios which allowed them to be considered "organisations"; for example, where the respondents was buying and selling personal data for personal profit[7] or independently carrying out

---

1 Act 26 of 2012, as amended.

2 Personal Data Protection Commission, *Shaping the Future of Personal Data Protection: Annual Report 2013/2014* at p 15.

3 What was originally known as the "Openness Obligation" has since been aptly renamed the "Accountability Obligation", reflecting developments in data protection relating to the concept of accountability. See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 21, fn 79.

4 See, for example, Personal Data Protection Commission, *Advisory Guidelines on Enforcement of Data Protection Provisions* (revised 1 February 2021) at para 27, setting out the Commission's power to fine organisations and the factors to be considered in determining fine quantum.

5 See the definition of "organisation" in s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

6 See the definition of "individual" in s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

7 *Re Sharon Assya Qadriyah Tang* [2018] PDP Digest 319 at [10].

a "business of his own".[8] Apart from these exceptional cases, individuals have rarely ever been directly taken to task for mismanaging personal data, whereas companies have more than often shouldered liability for the actions of their staff.

4 The most recent amendment to the Act challenges this paradigm. The 2020 amendment[9] ("the 2020 Amendment") to the Act introduces, among a slew of other notable changes, three additional criminal offences ("the Individual Offences") relating to unauthorised disclosure, improper use and unauthorised re-identification of personal data respectively.[10] The Individual Offences make clear that individuals can, in particularly egregious circumstances, be made directly accountable for personal data "in the possession or under the control of an organisation or a public agency".

5 In this article, the authors analyse the wording of the Individual Offences, and offer a view on how they might operate moving forward. The authors consider how past decisions of the Commission might have been handled differently under them, and provide thoughts on how the shift towards "personal accountability" as a result could affect Singapore's data protection landscape more generally.

II. The Individual Offences – Sections 48D, 48E and 48F

6 By way of introduction, the Individual Offences for unauthorised disclosure, improper use and unauthorised re-identification of personal data can be found at ss 48D, 48E and 48F of the PDPA respectively. These offences have come into effect as of 1 February 2021 and, to the authors' respective knowledge, no publicly available case law interpreting them has been published as of the writing of this article.

---

8 *Re Chua Yong Boon Justin* [2017] PDP Digest 91 at [11].

9 Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020).

10 Personal Data Protection Act 2012 (Act 26 of 2012) ss 48D, 48E and 48F. For completeness, the Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020) also introduced broadly similar amendments to the Monetary Authority of Singapore Act (Cap 186, 1999 Rev Ed) and Public Sector (Governance) Act 2018 (Act 5 of 2018), although these are not the focus of this article.

7 At its second reading in Parliament,[11] Minister for Communications and Information S Iswaran noted that the four aims of the 2020 Amendment were to: (a) strengthen consumer trust through organisational accountability; (b) ensure effective enforcement; (c) enhance consumer autonomy; and (d) support data use for innovation. Without a doubt, the Individual Offences are intended to fulfil the second aim of ensuring effective enforcement and, in particular, to "hold individuals accountable for egregious mishandling"[12] of personal data in the possession or under the control of organisations or public agencies.

8 For ease of reference, the text of the offences is set out below:

> **Unauthorised disclosure of personal data**
> **48D**.—(1) If —
>
> (*a*) an individual *discloses*, or the individual's *conduct causes disclosure of*, personal data in the possession or under the control of an organisation or a public agency to another person;
>
> (*b*) the disclosure is *not authorised* by the organisation or public agency, as the case may be; and
>
> (*c*) the individual does so —
>
> (i) *knowing* that the disclosure is not authorised by the organisation or public agency, as the case may be; or
>
> (ii) *reckless* as to whether the disclosure is or is not authorised by the organisation or public agency, as the case may be,
>
> the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.
>
> **Improper use of personal data**
> **48E**.—(1) If —
>
> (*a*) an individual *makes use of* personal data in the possession or under the control of an organisation or a public agency;
>
> (*b*) the use is *not authorised* by the organisation or public agency, as the case may be;
>
> (*c*) the individual does so —

11 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

12 Ministry of Communications and Information and the Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection (Amendment) Bill* (14 May 2020) at para 30.

(i) *knowing* that the use is not authorised by the organisation or public agency, as the case may be; or

(ii) *reckless* as to whether the use is or is not authorised by the organisation or public agency, as the case may be; and

(*d*) the individual, as a result of that use —

(i) *obtains a gain* for the individual or another person;

(ii) *causes harm* to another individual; or

(iii) *causes a loss* to another person,

the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

Unauthorised re-identification of anonymised information

48F.—(1) If —

(*a*) an individual *takes any action to re-identify or cause re-identification* of the person to whom anonymised information in the possession or under the control of an organisation or a public agency relates (called in this section the affected person);

(*b*) the re-identification is *not authorised* by the organisation or public agency, as the case may be; and

(*c*) the individual does so —

(i) *knowing* that the re-identification is not authorised by the organisation or public agency, as the case may be; or

(ii) *reckless* as to whether the re-identification is or is not authorised by the organisation or public agency, as the case may be,

the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

[emphasis added]

9 On plain reading, the wording of the Individual Offences reveals that they apply in a largely similar manner, while carrying an identical financial penalty and/or imprisonment term for the accused. Nevertheless, four points bear emphasis:

10 First, ss 48D and 48F, which deal with unauthorised disclosure and unauthorised re-identification respectively, share a common three-limb structure – two of which concern the actions or mental state of the accused, and one which concerns authorisation by the organisation or public agency. For either offence to be made out, the following must be proved beyond reasonable doubt: (a) mishandling of personal data under an organisation's or public agency's possession or control; (b) the lack of authorisation by the

organisation or public agency; and (c) either knowledge of the lack of authorisation or recklessness as to its existence.

11 On the other hand, s 48E, which deals with improper use, differs from the two aforementioned offences in one significant way. For the offence to be made out, an additional fourth limb applies[13] where the individual, as a result of that use, must: (a) obtain a gain for himself or another person; (b) cause harm to another individual; or (c) cause a loss to another person. Therefore, while s 48E covers a potentially broader scope of misbehaviour than ss 48D and 48F, securing a conviction under s 48E would be the most difficult of the three Individual Offences.

12 Second, the additional fourth limb in s 48E makes a fine distinction between an "individual" and another "person". While the Act expressly confines the definition of an "individual" to a natural person, whether living or deceased, a similar definition does not exist for the word "person". Reading s 48E(*d*) in context with the definition of "person" in the Interpretation Act,[14] this suggests that s 48E could in theory be satisfied where the accused has obtained a gain or has caused a loss to a company or association or body of persons, corporate or unincorporate[15] even when no natural person has been harmed *per se*.

13 For completeness, the definition of "loss or damage" at s 48O of the Act (previously s 32(1) prior to the 2020 Amendment) was recently considered by the General Division of the High Court in *Bellingham, Alex v Reed, Michael*,[16] where Chua Lee Ming J held, *inter alia*, that it was limited to the heads of loss or damage under common law[17] and excluded loss of control over personal data.[18] Nevertheless, these pronouncements were made in the context of an individual's private right of action in civil proceedings and prior to the 2020 Amendment, which introduced related

13 Personal Data Protection Act 2012 (Act 26 of 2012) s 48E(1)(*d*).

14 Cap 1, 2002 Rev Ed.

15 See the definition of "person" in s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

16 [2021] SGHC 125.

17 *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [93], *per* Chua Lee Ming J.

18 *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [76]–[77], *per* Chua Lee Ming J.

definitions applicable to Part IXB of the Act[19] where the Individual Offences are found. It remains to be seen how the Court of Appeal would address the interplay of similar definitions between the civil and criminal provisions of the Act,[20] if at all. Notably, and in contrast to s 48E, the term "harm" is not used in s 48O.

14 Third, while the Individual Offences separately refer to an "individual" and an "organisation [or] public agency" respectively, nothing in their express wording requires any sort of predefined or legally recognised relationship (whether employer–employee, solicitor–client, or otherwise) between the two. Therefore, it appears that as long as an individual has access to the personal data in question, whether as an employee, service provider, or perhaps even by accident or chance, an offence can be made out if the relevant disclosure, use and/or re-identification is not authorised by the organisation or public agency.

15 Fourth, some attention should also be paid to the fact that administrative enforcement of the Act and criminal prosecution are distinctly separate processes. While the Commission's powers to administer and enforce the Act are limited and ultimately conferred by the Act itself,[21] criminal offences are brought by the Public Prosecutor in accordance with the Criminal Procedure Code.[22] While this is viewed as a highly unlikely scenario due to public policy reasons, both administrative and criminal processes could in theory be brought simultaneously; for example, in the form of concurrent investigations of the organisation by the Commission, and the individual by the police. Alternatively, where such an overlap arises, the Commission may exercise its discretion under s 50(3)(*d*) of the Act and defer to the jurisdiction of the police and Public Prosecutor instead.

16 It also bears observation that individuals accused of any of the aforementioned offences may also rely on certain defences provided within

19 See the definitions of "loss", "gain" and "harm" in s 48C(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

20 *Bellingham, Alex v Reed*, Michael at [97], where Chua Lee Ming J granted leave to appeal.

21 Personal Data Protection Act 2012 (Act 26 of 2012) s 6(*g*).

22 Cap 68, 2012 Rev Ed.

the Act.[23] These generally relate to whether or not the personal data in question was publicly available at the time the individual handled it, whether the individual handled such personal data in a manner that was permitted under law or authorised by court order, or whether the individual had a reasonable belief that he had a right to handle that personal data.

17 For s 48F specifically, an individual who: (a) reasonably believed that re-identification was for a specified purpose; and (b) notified the Commission or the organisation or public agency of re-identification as soon as practicable, would also be able to rely on a defence. This would likely apply to independent testing of anonymisation deployed in information security systems,[24] such as tests conducted by third-party data professionals or white-hat hackers.[25]

18 For completeness, the Individual Offences also share similarities with the language used in ss 170 and 171 of the UK Data Protection Act 2018.[26] Section 170(1) makes it an offence for:

> … a person knowingly or recklessly—
>
> (a) to obtain or disclose personal data without the consent of the controller,
>
> (b) to procure the disclosure of personal data to another person without the consent of the controller …

Section 171(1) provides a similar offence "for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data". The relevance of UK case law on ss 170 and 171, and the extent to which they will be persuasive on the Singapore courts, remains to be seen.

---

23 Personal Data Protection Act 2012 (Act 26 of 2012) ss 48D(2), 48E(2) and 48F(2) respectively.

24 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

25 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 23.5.

26 c 12.

III. Individual accountability in past decisions

19 Since it was first introduced, the Accountability Obligation has always been viewed as the responsibility of the organisation.[27] The second reading of the 2020 Amendment is, to the authors' knowledge, the first time that the phrase "individual accountability" has ever been used in Parliament in relation to the Act.[28] The use of this phrase represents a landmark shift in the Commission's (and, indeed, the broader government's) view on the balance between individual and corporate accountability as concerns data protection, with strong implications on liability allocation between the two.

20 At present, the obligations of the Act do not apply to employees acting in the course of their employment with an organisation.[29] Where an employment relationship exists, companies (*eg*, the individual's employer) have more often been made accountable for the actions of their staff rather than *vice versa*, whether fairly or not. The imposition of fines and penalties on the organisation could, in part, be due to the lack of other avenues for the Commission to act on a complaint prior to the Individual Offences.

21 While the authors agree that organisations should be *primarily* accountable for personal data of consumers within their possession or under their control,[30] it is submitted that there will always be situations where well-accountable organisations suffer the consequences of independent, individual actions despite their best efforts. An organisation that has been dutiful in its personal data responsibilities should not, in the authors' view, always be required to bear the brunt for all individual actions without exception.

22 A previous Commission decision which illustrates this point would be *Re Executive Coach International Pte Ltd*.[31] In that case, highly sensitive

---

27 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 21.1.

28 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information), stating that "the Bill strengthens *individual accountability* for the egregious mishandling of data".

29 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(1)(*b*).

30 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 23.1.

31 [2017] PDP Digest 188.

information of the complainant's personal history, namely her past drug problem and issue with infidelity, were disclosed in an instant messaging group chat comprising the organisation's other staff and volunteer trainees without her consent and without notification of the purposes for disclosure. The information was disclosed by a director of the organisation following allegations that she was undermining the organisation's authority by persuading the employees and volunteers to leave the organisation. The complainant was, up to that time, employed as the personal assistant to the aforementioned director, and had expressed her own disappointment with the director's conduct personally, including as an employer and professional.

23 While the Commission acknowledged that the complainant's personal data was made in the context of an ongoing dispute arising from the complainant's unamicable departure,[32] that the organisation did not know or approve of the director's actions,[33] and that the disclosure was deliberately made under circumstances to discredit the complainant,[34] it nevertheless found the organisation to be in breach of ss 13 and 20 of the Act. This was because the violating acts were done by an employee who was a senior member of the organisation,[35] and because the director's disclosure was made in the course of employment.

24 In consideration of several factors, including the fact that the disclosure was made in what essentially was the organisation's group chat for work and not the public at large, the Commission decided not to issue any direction to take remedial action or to pay a financial penalty – a warning was issued to the organisation instead.

25 While the authors agree with the Commission's decision on the facts, it is submitted that this would have been appropriate for the application of the Individual Offences had they come into force earlier. The elements of ss 48D and/or 48E are clearly made out by the egregious actions of the director in what can be viewed as an attempt to "get back" at the complainant, with little regard for his employer's possession of that personal

32 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [11].

33 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [12].

34 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [19].

35 *Re Executive Coach International Pte Ltd* [2017] PDP Digest 188 at [13]. See also s 53(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

data, or the privacy of the complainant herself. It does not appear that he would be able to rely on any defences in relation to the personal data that was disclosed and/or improperly used.

26 Similarly, in *Re Management Corporation Strata Title Plan No 4375*[36] ("*Re MCST Plan No 4375*"), which concerned the disclosure of certain closed-circuit television ("CCTV") footage showing a glass door falling on a woman at Alexandra Central Mall, the security services vendor firm ("ABSM") engaged by the Management Corporation Strata Title ("MCST") was found to be liable for the actions of its on-duty senior security supervisor and security executive. Notably, the senior security supervisor had (a) replayed the portion of the footage showing the accident; (b) recorded it with his mobile phone; and (c) sent it via instant messaging to various colleagues, including the security executive, which ultimately led to the video being posted on an Internet video-sharing platform.

27 While several disclosures made by both individuals were found to be appropriate in the circumstances, the Commission found that the further disclosure of the CCTV footage by the security executive to the MCST's cleaning supervisor was unauthorised and in direct contravention of both ABSM's personal data protection policy and crisis report flow chart,[37] which required the MCST's prior approval. In finding that ABSM was in breach of s 24 of the Act, the Commission took the view that ABSM had "failed to properly train and communicate its internal policies and procedures" and that it "should have had a written policy setting out the procedures to be followed in relation to the disclosure of CCTV footage and the personal data therein".[38]

28 The Commission's decision focused mainly on what ABSM could have done better in respect of instructing its staff; however, the authors submit that the employees in question cannot be said to be entirely blameless either. While it is suggested that the security executive forwarded the footage to the cleaning supervisor as part of a chain of communication to inform the cleaners not to enter the barricaded area where the accident

36 [2020] SGPDPC 4.

37 *Re Management Corporation Strata Title Plan No 4375* [2020] SGPDPC 4 at [15]–[16].

38 *Re Management Corporation Strata Title Plan No 4375* [2020] SGPDPC 4 at [18].

occurred,[39] this could clearly and easily have been done even without sending the footage, which was not at all required to be conveyed to the cleaners.

29 Rather, it appears that the security executive was reckless as to whether this disclosure was authorised by employer or not, especially since a personal data protection policy and crisis report flow chart was available and could be checked at any time prior. Even if they did not specifically contain "procedures to be followed in relation to the disclosure of CCTV footage", the security executive would most likely have been able to obtain contact details of someone who could advise him somewhere within the documents. Furthermore, this was not any regular video, but CCTV footage which contained highly graphic personal data of a woman getting hurt. The absence of a specific procedure to be followed in relation to CCTV footage disclosure does not change the fact that ABSM's employees had proactively disclosed more than what would objectively be reasonable in the circumstances, thereby causing harm to the woman in the footage.

30 The Individual Offences also rightfully apply to situations where an employment relationship does not exist, but where the individual has misused his or her access to an organisation's personal data. A decision that comes to mind here would be the recent decision of *Re Grabcar Pte Ltd*.[40]

31 In that decision, two drivers who were part of the popular social carpooling platform GrabHitch were found to have disclosed personal data of two passengers on a public social media group called "GrabHitch Singapore Community" in connection with some disagreements on payment. Due to the nature of how carpooling services are regulated in Singapore and the fact that the Act does not apply to individuals acting in their personal or domestic capacities,[41] the Commission found that GrabHitch drivers were not subject to the Act.[42] Grabcar was found to be in breach of s 24 of the Act, although the Commission ultimately found that a financial penalty was not warranted and rightly directed Grabcar to review and improve its policies and practices in relation to GrabHitch.

---

39 *Re Management Corporation Strata Title Plan No 4375* [2020] SGPDPC 4 at [3].

40 [2020] PDP Digest 252.

41 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(1)(*a*).

42 *Re Grabcar Pte Ltd* [2020] PDP Digest 252 at [28].

32 Nevertheless, a real question arises as to whether the drivers themselves – the parties whose actions directly led to the passengers' complaints – should have been found liable under ss 48D and/or 48E had they come into force earlier. For the purposes of this analysis, the authors submit that it does not matter that the drivers were acting in their personal capacity and therefore not "organisations" under the Act, as they were very much individuals who had disclosed and/or improperly used personal data in the control of Grabcar,[43] and had done so without the authorisation of Grabcar fully knowing that they did not have such authorisation. It is also arguable that harm or loss to the two passengers resulted due to the drivers' actions, thereby fulfilling the requirement at s 48E(1)(*d*).

33 For completeness, the authors note that the Individual Offences may not be applicable to *all* situations involving misuse of personal data by individuals. A significant requirement applicable across all the Individual Offences is that the disclosure, use or re-identification is "not authorised by the organisation or public agency". This suggests, in the authors' view, that the "individual" and the "organisation" must be separate legal entities for the offence to be made out.

34 Several past decisions involve individuals who have been found by the Commission to be the "organisations" themselves. For example, in the decisions of *Re Chua Yong Boon Justin*[44] and *Re Ang Rui Siong*[45] where the respondents were respectively found to be conducting their own businesses as a real estate agent and financial consultant respectively, this requirement will only be satisfied if it can be said that the individuals in question did not authorise their own egregious acts of disclosure, use or re-identification. This is inherently artificial if not illogical, and could present a material impediment in cases where a separate "organisation" cannot be found notwithstanding the satisfaction of all other limbs. The authors encourage the Commission to consider how the language used in the Individual Offences may be amended to bring such individuals within scope.

43 *Re Grabcar Pte Ltd* [2020] PDP Digest 252 at [31].

44 [2017] PDP Digest 91.

45 [2018] PDP Digest 236.

IV. Concluding thoughts on the changing landscape

35 Though this article has sought to provide the authors' view in respect of past decisions, the authors recognise that issues of liability and accountability are rarely ever clear-cut. Decisions like *Re MCST Plan No 4375* and *Re Grabcar Pte Ltd* demonstrate the substantial overlap between corporate policy-making and individual action, and the difficulty of apportioning liability between organisations and individuals who have both contributed in some degree to the violation of the Act.

36 A lot will now turn on what an individual has been "authorised" to do under the Individual Offences. While the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[46] clarify that "[a]uthorisation may take different forms: it may be found in an organisation's written polices, manuals and handbooks, or an organisation may provide ad-hoc authorisation for a specific action or activity (which could be verbal or in writing)",[47] this means that very much will depend on how well or cleanly drafted an organisation's policy documents are, as well as the quality of evidence put forward before the Commission or the relevant court.

37 Another potential outcome of the Individual Offences might be a negative impact on employees who regularly deal with personal data as part of their duties, or on employees whose duties involve assisting with organisational compliance, such as data protection officers ("DPOs").[48] During the second reading of the 2020 Amendment, Leon Perera astutely pointed out that "there is a possibility that 'scapegoating' may happen. Junior employees with less bargaining power may be held liable, while higher ranked employees and the organisation itself may face reduced accountability thereby".[49]

38 The authors submit that Perera's concerns apply not only to junior employees, but also to individuals whose responsibilities involve the

---

46 Revised 1 October 2021.

47 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 23.2.

48 Section 11(3) of the Personal Data Protection Act 2012 (Act 26 of 2012) refers to the designation of "one or more individuals to be responsible for ensuring that the organisation complies with this Act".

49 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (Leon Perera).

management of personal data more generally. It is not outside the realm of possibility for an organisation to position a breach away from being a case for the Commission's attention, and instead towards a criminal investigation caused by the "unauthorised" actions of a DPO or similar professional, perhaps in a bid to save the public perception of the company. An organisation is, after all, more likely to preserve its reputation by reframing the problem as one of individual criminality rather than a failure of corporate oversight, and pushing "accountability" onto an individual instead.

39 Furthermore, negligence or failure to perform duties adequately could also theoretically amount to "conduct [which] causes disclosure of personal data" under s 48D(1)(*a*) or which "cause[s] re-identification" under s 48F(1)(*a*). This is especially so in the context of a large-scale data breach, where actions leading up to and during the breach are of critical importance for containment.[50] Such an argument is not without precedent; in January 2020, a South Korean court found the privacy officer of a local travel agency to be negligent in preventing a breach that affected over 465,000 customers and employees.[51] While the Act does make clear that the appointment of a DPO does not relieve an organisation of its own obligations,[52] it remains to be seen how widely the Individual Offences will be interpreted by the courts, and the extent to which charges will be brought against DPOs and similar professionals.

40 The introduction of the Individual Offences signals a mindset shift towards personal accountability under the Act. From what was originally an organisation-centric, internally focused obligation requiring, *inter alia*, the development of policies and processes for staff to adhere to,[53] the concept of accountability following the 2020 Amendment has now become a more outward-looking and relational one, which also considers the balance of responsibility between the organisation and the individual where liability is concerned.

---

50 See, for example, the "contain" step in Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at pp 14–16.

51 "South Korean Court Finds Privacy Officer Liable for Data breach" *IAPP* (10 January 2020).

52 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(6).

53 Personal Data Protection Act 2012 (Act 26 of 2012) ss 12(*a*) and 12(*b*).

41 Organisations have good reason to welcome the Individual Offences, and the authors submit that this development is a step in the right direction notwithstanding the issues raised earlier in this article. While organisations should always remain *primarily* accountable for data protection,[54] errant individuals should not be able to rely on organisational top cover to get off scot-free for their actions, especially when such actions are unauthorised in the first place. However, great care should be taken by the Commission and Public Prosecutor to ensure that charges under the Individual Offences are brought only in clearly egregious and genuine cases, to uphold the stated aim of ensuring effective enforcement and to prevent innocent individuals from being made unduly accountable for their organisations' failings instead.

---

54 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 23.1.

CROSS THAT BREACH WHEN WE GET THERE? DESIGNING PRE-EMPTIVE MEASURES TO MANAGE POTENTIAL CROSS-BORDER DATA INCIDENTS UNDER THE PERSONAL DATA PROTECTION ACT*

Nick CHIAM Zhi Wen†
LLB (magna cum laude) (Singapore Management University); CIPP/A; Advocate and Solicitor (Singapore)

LEE Jia Juinn, Kenji‡
LLB (Hons) (National University of Singapore); CIPM, CIPP/A, CIPP/E; Advocate and Solicitor (Singapore)

I. Introduction

1 Since the conception of the Personal Data Protection Act 2012[1] ("PDPA") as far back as 2012, it has been acknowledged that the collection, use and disclosure of personal data will only become "increasingly complex" as personal data of individuals in Singapore become more frequently processed overseas.[2]

---

* All views expressed in this article are the authors' personal views only and should not be taken to represent the views and/or policy positions of their employer. All errors remain the authors' own.

† Associate, WongPartnership LLP; Adjunct Faculty, Singapore Management University Yong Pung How School of Law. Nick is a member of the Singapore Law Society's Cybersecurity and Data Protection Committee.

‡ Associate, WongPartnership LLP; Research Officer, Regional Economic Studies Programme, ISEAS – Yusof Ishak Institute; Adjunct Research Fellow, EW Barker Centre for Law & Business, National University of Singapore Faculty of Law.

1 Act 26 of 2012.

2 *Parliamentary Debates, Official Report* (15 October 2012), vol 89 at p 841 (David Ong).

2 Today in 2021, however, the "fast and easy transportation of data across national boundaries"[3] has transformed from a buzz phrase to a new normal, bringing rapidly evolving risks and opportunities against the backdrop of phenomenal developments in Internet and cloud technology.[4] The global COVID-19 pandemic has also intensified "automation, robotisation and digitalisation"[5] across all sectors and amplified the volume and frequency of cross-border personal data transfers. The result is increased connectivity overall but also a corresponding increase in the surface area for cyber-attacks[6] and regulatory complexity.[7]

3 As observed by the Minister for Communications and Information during the second reading for the 2021 amendments to the PDPA, Singapore today is strategically positioned as an "important node in the global network of data flows and digital transactions" amidst "magnitudinal shifts" in the data landscape that continue to occur.[8] Indeed, the International Data Corporation projects that the global volume of data that will be created in the next couple of years will "eclipse the total data generated over the past 30 years",[9] and it would be reasonable to expect that

---

3 *Parliamentary Debates, Official Report* (15 October 2012), vol 89 at p 841 (David Ong).

4 See, for example, Ádám Liber & Tamas Bereczki, "Managing Data Breaches in the Cloud" *IAPP* (28 January 2020).

5 Ádám Liber & Tamas Bereczki, "Developing Digitized Solutions for Customers? Here's What to Think about" *IAPP* (27 May 2020).

6 See, for example, a discussion on an increase in ransomware attacks on hospitals: Jedidiah Bracy, "Amid a Global Pandemic, Ransomware Increasingly Targets Hospitals" *IAPP* (1 December 2020).

7 These developments stress-test the coherence of local laws across jurisdictions. For an example in relation to multinational clinical trials, see John Childs-Eddy, "How to Comply with Data Localization Regulations amid COVID-19's Impact" *IAPP* (28 April 2020). See also Jennifer Bryant, "Return to Office 'a Perfect Storm' of Privacy Issues for Businesses" *IAPP* (27 April 2021).

8 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

9 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

transboundary personal data flows will only continue to intensify in volume and frequency.

4 Unsurprisingly, regulators worldwide are beginning to develop co-operative frameworks with the expectation that personal data incidents will become increasingly international in nature.[10] ASEAN, in particular, recently established the ASEAN Model Contractual Clauses ("MCCs") in the form of a "living document"[11] aligned with "global best practices"[12] intended to promote the use of a minimum standard for regional transfers of personal data, including in relation to data breach notification and other assistance between the transferor and overseas recipient of personal data. This initiative was welcomed by the Personal Data Protection Commission ("PDPC"), which announced that it "recognises and encourages the use of the ASEAN MCCs" in Singapore for the purposes of the PDPA.[13]

5 Whilst the ASEAN MCCs are wholly voluntary, data incidents occurring overseas involving personal data made available by a Singapore

---

10 See, *eg*, Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council. See also Angelique Carson, "Global Regulators Seek Answers for Stronger Collaboration" *IAPP* (26 March 2019).

11 1st ASEAN Digital Ministers' Meeting (ADGMIN) 2020, *Implementing Guidelines for ASEAN Data Management Framework and ASEAN Cross Border Data Flows Mechanism* (January 2021) at para 7.

12 2nd ASEAN Digital Senior Officials' Meeting (ADGSOM), *ASEAN Model Contractual Clauses for Cross Border Data Flows* (January 2021) at p 5. Such best practices include the Fair Information Practice Principles, the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980; revised 2013), the Asia-Pacific Economic Cooperation Privacy Framework (December 2005) and the European Union's Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").

13 Personal Data Protection Commission, *Guidance for Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore* (22 January 2021) at para 2.

organisation to that overseas location ("cross-border data incident" or "CBDI") can implicate mandatory provisions under the PDPA. As used in this article, "data incident" (in relation to personal data) includes broadly: (a) "any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data"; and/or (b) "the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur".[14]

6 There is, therefore, an urgency for Singapore organisations to proactively develop and update their data incident management plans to manage actual and potential CBDI events ("CBDI management plans") to ensure that they are robust enough to address potential CBDIs effectively under the PDPA. In the authors' view, such robust CBDI management plans should not comprise solely reactive (or "response") measures but should also include *pre-emptive* measures. In this regard, pre-emptive measures refer to proactive and preventive measures that reduce the risks of a CBDI occurring in the first place, including measures that assist with the detection of potential CBDI risks. In a practical sense, pre-emptive measures can also be understood as protective measures that reduce the risk of the organisation being found to have breached its various obligations under the PDPA in the event of an actual CBDI.

7 In that spirit, the authors seek to outline in this brief primer, from the perspective of the PDPA, key practical considerations that organisations bound by the PDPA in Singapore (hereafter simply "organisations") may wish to consider when designing pre-emptive measures in their CBDI management plans, in light of their mandatory obligations under the PDPA.

8 This article is structured broadly into two parts – Part II[15] outlines how the Transfer Limitation Obligation, the Protection Obligation and the

14 Borrowing from the working definition of "data breach" used in the Personal Data Protection Commission's *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 8. This working definition appears to be a corollary of s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012) which sets out the Protection Obligation.

15 See paras 9–31 below.

Data Breach Notification Obligation may be implicated in the event of CBDIs, and Part III[16] outlines a basic framework of practical considerations for designing pre-emptive measures for CBDI management plans. It is hoped that data protection practitioners will find this primer useful from both a doctrinal as well as practical perspective in crafting effective CBDI management plans.

II. Mandatory obligations under the Personal Data Protection Act typically implicated in the event of cross-border data incidents

9 Practically, before designing pre-emptive measures for CBDI management plans, it may be useful for an organisation to trace the parameters of its obligations under the PDPA that are at risk of being found to be breached in the event of a CBDI and then work backwards to discern the protective measures required in order to pre-emptively address such risks.

10 In that regard, the authors outline below how the Transfer Limitation Obligation, the Protection Obligation, and the Data Breach Notification Obligation may be implicated in the event of CBDIs where personal data is situated overseas.[17]

A. Transfer Limitation Obligation

11 As a starting point, the Transfer Limitation Obligation is an obvious candidate for inquiry during investigations of CBDIs for potential breaches of obligations under the PDPA since the transferring party in Singapore was responsible under the PDPA for the outbound transfer at the outset.

12 Section 26 of the PDPA restricts an organisation from transferring personal data to a jurisdiction outside Singapore unless it takes appropriate steps to "ascertain whether", and to "ensure that", the recipient is bound by legally enforceable obligations to provide to the transferred personal data

16 See paras 32–51 below.

17 To be clear, these obligations are not intended to be exhaustive of all the obligations that may be breached in the event of a cross-border data incident, but are selected as illustrative of the mandatory obligations that are typically implicated under the Personal Data Protection Act 2012 (Act 26 of 2012).

"a standard of protection that is at least comparable to the protection" under the PDPA (Transfer Limitation Obligation).[18]

13 Hence, if a CBDI occurs after personal data has been transferred to an overseas recipient, the spotlight can be cast back in time on whether, at the time of data transfer, the transferring party had, in meeting the Transfer Limitation Obligation, conducted prior due diligence to verify (*ie*, "ascertain") the recipient's preparedness to provide the requisite standard of protection overseas,[19] *in addition to* whether the legally enforceable obligations imposed by the transferor (if any) were adequate to "ensure" the required level of protection.[20]

14 Furthermore, the adequacy of such legally enforceable obligations imposed on such overseas recipient would be crucial in ensuring the organisation's own compliance with the Protection Obligation and/or Data Breach Notification Obligation,[21] particularly where the overseas recipient is outside of PDPA's jurisdiction and is not legally obliged under local laws to protect the data according to the same standard and manner as prescribed under the PDPA, and/or co-operate with the organisation to manage any CBDIs.

---

18 Regulation 10 of the Personal Data Protection Regulations 2021 (S 63/2021) read with s 26 of the Personal Data Protection Act 2012 (Act 26 of 2012).

19 In undertaking due diligence, "transferring organisations may rely on data intermediaries' extant protection policies and practices, including their assurances of compliance with relevant industry standards or certification": Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 6.23.

20 The adequacy of the obligations imposed depends on whether the overseas recipient had received the data as principal in its own right or as a data intermediary for the transferor in Singapore, as well as the context of the transfer arrangement. See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 19.1–19.11.

21 Each further discussed at paras 15–31 below.

B. Protection Obligation and Data Breach Notification Obligation

15 The Protection Obligation and the Data Breach Notification Obligation may also be implicated during investigations of CBDI for potential breaches of obligations under the PDPA.

16 The statutory wording of the Protection Obligation and the Data Breach Notification Obligation (in referring to personal data in an organisation's "possession or under its control")[22] suggests that a breach thereto by an organisation may be made out even in respect of personal data that is situated overseas, so long as extant "possession" or "control" of the personal data can be attributed to the organisation at the material time of the data incident giving rise to the CBDI:[23]

(a) Protection Obligation: Section 24 of the PDPA requires an organisation to:

> … protect personal data *in its possession or under its control* by making reasonable security arrangements to prevent —
>
> (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
>
> (ii) the loss of any storage medium or device on which personal data is stored.
>
> [emphasis added]

(b) Data Breach Notification Obligation: Section 26C of the PDPA provides that where an organisation has reason to believe that a "data breach"[24] affecting personal data *in its possession or under its control* has

---

22 Section 11(2) of the Personal Data Protection Act 2012 (Act 26 of 2012) also stipulates that an organisation is responsible for personal data in its possession or under its control.

23 Of course, such possession or control by the organisation in Singapore are only thresholds for inquiry – whether the Protection Obligation is actually breached would depend on whether the organisation in Singapore had failed to make "reasonable security arrangements" to prevent the relevant data incident giving rise to the cross-border data incident.

24 Personal Data Protection Act 2012 (Act 26 of 2012) s 26A:

> '[D]ata breach', in relation to personal data, means —
>
> (*a*) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or
>
> (*b*) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access,

(*continued on next page*)

occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. Section 26D of the PDPA further stipulates that where the organisation assesses that a data breach is a "notifiable data breach",[25] the organisation must notify the PDPC as soon as practicable, but in any case, no later than three calendar days after the day the organisation makes that assessment.

17 However, the PDPA is silent on both the meaning and ambit of the words "control" and "possession".

18 In the case of personal data situated overseas, whilst (on plain reading) it may reasonably be argued that the organisation does not have "possession" of such personal data,[26] the PDPC has suggested that "control" in the context of data protection may extend more broadly to "cover the *ability, right or authority* to determine: (i) the purposes for; and/or (ii) the manner in which, personal data is processed, collected, used or disclosed" [emphasis added].[27]

---

collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

25 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B(1):

> A data breach is a notifiable data breach if the data breach —
>
> (*a*) results in, or is likely to result in, significant harm to an affected individual; or
>
> (*b*) is, or is likely to be, of a significant scale.

26 There is some support that "possession" may be understood in its plain meaning (which is conceptually distinct from "control") – the Personal Data Protection Commission has held that:

> … in a situation where the organisation transfers personal data to its data intermediary, the organisation could remain in control of the personal data set while, simultaneously, the data intermediary may have possession of the same personal data set … even though the organisation was not in direct possession of the personal data that was held in the data intermediary's servers, it was still obliged to implement reasonable security arrangements to protect the personal data as it had control over such data.

See *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [17] and *Re WTS Automotive Services Pte Ltd* [2019] PDP Digest 317 at [10]–[13].

27 *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [18].

19 Accordingly, organisations may be interested to understand the *extent* to which its "control" of personal data situated overseas would be sufficient to render the organisation responsible for meeting the Protection Obligation and the Data Breach Notification Obligation in respect of such personal data, if at all.[28] This understanding would be helpful, in the authors' view, to inform the development of appropriate pre-emptive measures for CBDI management plans.

20 On that basis, the authors propose two archetypal possibilities (with a range of intermediate positions possible) as a working schema for analysing the ambit of an organisation's "control" of data, at two ends of a spectrum, for the purposes of attributing responsibility for the Protection Obligation and Data Breach Notification Obligation in respect of overseas personal data:[29]

---

28 The Personal Data Protection Commission has taken the position that:

> … it is possible for the same dataset of personal data to be in the possession of one organisation, and under the control of another. For example, in a situation where the organisation transfers personal data to its data intermediary, the organisation could remain in control of the personal data while, simultaneously, the data intermediary may have possession of the same personal data set.

See *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [17]–[20].

29 This schema is also consistent with similar expressions of "control" used in the context of computer misuse legislation in Singapore. The Computer Misuse Act (Cap 50A, 2007 Rev Ed) ("CMA") provides for offences relating to unauthorised access of data held in a computer under s 3(1) of the CMA, and s 2(5) of the CMA stipulates that access by a person to data held in a computer is unauthorised if:

> (*a*) he is not himself entitled to control access of the kind in question to the … data; and
>
> (*b*) he does not have consent to access by him of the kind of question to the … data from any person … so entitled.

In the UK House of Lords case of *R v Bow Street Metropolitan Stipendiary Magistrate* [1999] 3 WLR 620 ("*Bow Street*"), Lord Hobhouse in delivering the leading judgment considered the meaning of "control" in relation to ss 1 and 17(5) of the UK Computer Misuse Act 1990 (c 18) ("UKCMA1990"), and held that "it is plain that [s 17(5) of the UKCMA1990] is not using the word control in a physical sense of the ability to operate or manipulate the

(*continued on next page*)

(a) a narrow construction at one end, as referring to the Singapore organisation's operational, technical, or physical control of the processing of overseas personal data ("Technical Control"). This interpretation would also be consistent with one aspect of control described by the Hong Kong Administrative Appeals Board ("HKAAB") (cited by the PDPC in explaining the ambit of control under the PDPA) as including "the physical act of collecting, holding, processing or using the personal data";[30] or

(b) a broad construction on the other end, as referring to the Singapore organisation's legal right to authorise or forbid the scope of processing in relation to the overseas personal data, including in respect of any overseas personal data which is processed on behalf of the Singapore organisation by another data intermediary ("Authorising Control"). As the HKAAB puts it, control includes "the ability of [an organisation in] determining the purpose for which …

---

computer", but rather control in the sense of entitlement to "authorise and forbid" the relevant access to data.

Sections 3(1) and 2(5) of the CMA are *in pari materia* with ss 1 and 17(5) of the UKCMA1990, and Lord Hobhouse's holding in *Bow Street* was later referred to by the Singapore court in *Public Prosecutor v Loh Chai Huat* [2001] SGDC 174 ("*Loh Chai Huat*") to interpret s 2(5) of the CMA as meaning "[a] person either has the authority to control access by authorising or forbidding access, or if he has no such authority, he must be given consent to access by a person so entitled to control access".

To be clear, the analogy between the CMA and Personal Data Protection Act 2012 (Act 26 of 2012) is limited because s 2(5) of the CMA concerns control of access to data, rather than control of data *per se*. Indeed, in *Loh Chai Huat*, the key consideration for the court was focused on the question of whether "authority to access" under the CMA may be defined by the "purpose of access", such that if A gives B authority to access certain data to carry out project X, should B gain access to the data to carry out project Y, B's access is without authority.

Nevertheless, the authors are of the view that the *Bow Street* distinction between control in the "physical sense" and control in the sense of entitlement to "authorise and forbid" provides a useful launchpad for deliberation as to the possibly construction of an organisation's "control" of personal data for the purposes of attributing responsibility in respect of an organisation's responsibility under the PDPA.

30 *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [19].

> and the manner in which personal data is processed [whether] on its own or jointly or in common with other organisations".[31]

21 Under this schema of understanding "control", the precise nature of *reasonable security arrangements expected of an organisation* (under the Protection Obligation) and the *mandatory breach notification requirements* (under the Data Breach Notification Obligation) imposed on the Singapore organisation under the PDPA during the PDPC's inquiry in the event of a CBDI depends on whether the extent to which the organisation has Technical Control or Authorising Control over the personal data situated overseas.

(1) Technical Control

22 First, to the extent an organisation maintains Technical Control over personal data situated overseas, in the event of a CBDI in respect of such data, the organisation may be responsible for any failure to implement reasonable *technical and operational security arrangements* in preventing the relevant data incident (under the Protection Obligation) and/or any failure to *assess data incidents and make the relevant notifications to the PDPC and/or affected individuals* (under the Data Breach Notification Obligation). The PDPC has held in enforcement decisions, for example, that where an organisation was able to promptly implement technical restrictions to public access to personal data accessible on a website, such personal data was under the control of the organisation.[32]

23 This is consistent with the PDPC's recent illustrations highlighting an organisation's responsibility for data under its Technical Control: where an employee "travels overseas with customer lists on his notebook"; where an organisation "owns or leases and operates a warehouse overseas for archival of customer records"; or where the organisation "stores personal data in an overseas data centre on servers that it owns and directly maintains", that same organisation in Singapore "has direct primary obligations under the [PDPA] to, *inter alia*, protect the personal data … transferred or situated

---

31 *Re AIG Asia Pacific Insurance Pte Ltd* [2019] PDP Digest 189 at [19].

32 See, *eg*, *Re ABR Holdings Limited* [2017] PDP Digest 117 at [14] and *Re JP Pepperdine Group Pte Ltd* [2017] PDP Digest 180 at [13].

overseas" because such data "remains in the possession or control of an organisation".[33]

24 However, the extent of Technical Control required to attribute responsibility to organisations for breach of the Protection Obligation and/or the Data Breach Notification Obligation in respect of personal data situated overseas would appear to be a developing area. For example:

(a) Where an organisation has transient Technical Control over inbound and/or outbound personal data in circumstances where the organisation acts merely as a conduit, could an organisation escape liability for breach of the *Protection Obligation* in the event of a CBDI, on the basis that it was merely a conduit for personal data at the material time?

(b) Could organisations who are merely acting as conduits for the transmission of personal data avail themselves of the safe harbour afforded to network service providers under s 26(1A) of the Electronic Transactions Act?[34] Section 26(1A) provides that "a network service provider shall not be subject to any liability under the PDPA in respect of third-party material in the form of electronic records to which he merely provides access". Should such safe harbour extend specifically to shield an organisation from liability under the Protection Obligation and/or the Data Breach Notification Obligation under the PDPA? Would any form of "control" over personal data cause it to fall outside the meaning of "third-party" material?

(c) An organisation would generally be deemed under the PDPA to have complied with the Transfer Limitation Obligation in respect of data in transit.[35] Should there be a different treatment for data in transit in relation to the Data Breach Notification?

---

33 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 19.1.

34 Cap 88, 2011 Rev Ed.

35 See reg 10(2)(*d*) of the Personal Data Protection Regulations 2021 (S 63/2021); see also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 19.11.

(2) Authorising Control

25 Second, to the extent an organisation has Authorising Control over the processing of the data, the organisation may also be responsible for failure to implement reasonable *legal and administrative security arrangements* in preventing the relevant data incident (under the Protection Obligation) and/or any failure to *assess data incidents and make the relevant notifications to the PDPC and/or affected individuals* (under the Data Breach Notification Obligation).

26 A clear case of responsibility attributed under the PDPA by virtue of an organisation's Authorising Control is when such control is exercised over personal data through its authorised data intermediary. Despite the data intermediary having independent obligations to protect personal data it has received from the organisation, the organisation remains liable for any breach of the data protection obligations under the PDPA for any processing by a data intermediary on the organisation's behalf and purposes.[36]

27 The significance of an organisation's Technical Control and/or Authorising Control over personal data situated overseas, in attributing liability under the Protection Obligation, is illustrated by the PDPC's decision in *Re Cigna Europe Insurance Company SA-NV*[37] ("*Cigna*"), a case of a CBDI involving a data intermediary:

> (a) In *Cigna*, an organisation (a Singapore branch office of a Belgium company offering health insurance) ("the Organisation") suffered a data incident involving the disclosure of personal data of individuals who had taken health insurance coverage with the Organisation ("Members").
>
> (b) To provide health insurance coverage, the Organisation had entered into a services agreement with a related company in the UK ("Service Provider") which supported the processing of insurance

36 Under s 4(3) of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA"), every organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by any data intermediary as if the personal data were processed by the organisation itself. See also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 6.21.

37 [2020] PDP Digest 286.

claims through an information technology system operated by the Service Provider ("System").

(c) Due to technical issues in the System, on two separate occasions, claims settlement letters intended for certain Members were erroneously sent by Service Provider to other Members.

(d) As the System was operated in the UK at the time of the data incident, this case concerned a CBDI.

28 Regarding Technical Control, the PDPC held that the Organisation "does not bear any direct responsibility under the PDPA for the occurrence of the two incidents" because "the technical issues in the System … were not within the Organisation's operational control or even its knowledge" at the material time.[38]

29 Nevertheless, despite the lack of Technical Control by the Organisation, the PDPC proceeded to consider the Protection Obligation as relevant to the investigation, on the basis that when the CBDI had occurred, the Organisation had Authorising Control over the processing of the data overseas:[39]

> Nevertheless, *as the processing of the Members' personal data by [the Service Provider] was pursuant to the Services Agreement between the Organisation and [the Service Provider], the question arises as to whether the Organisation had in place the appropriate measures to ensure protection* of the Members' personal data while the data was stored with and processed by [the Service Provider]. In this regard, s 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, disclosure and similar risks.
>
> I find that the Organisation had in place the appropriate measures … to ensure protection of personal data by [the Service Provider] and to monitor [the Service Provider's] compliance. These measures include [various clauses in the contracts between the Organisation and the Service Provider to protect personal data transferred to it by the Organisation] …
>
> …
>
> … the Protection Obligation (s 24) is relevant to the transfer of personal data from the Organisation to CES. As discussed in the preceding section of this Decision, the Organisation had in place the appropriate security arrangements, including contractual provisions, which met the

38 *Re Cigna Europe Insurance Company SA-NV* [2020] PDP Digest 286 at [5].

39 *Re Cigna Europe Insurance Company SA-NV* [2020] PDP Digest 286 at [6]–[7] and [13].

> requirements of s 24 of the PDPA. Those contractual provisions would also meet the requirements of s 26(1) of the PDPA …
> [emphasis added]

30 Apart from cases involving *direct* data intermediaries, the extent of Authorising Control required to attribute responsibility to organisations for breach of the Protection Obligation in respect of personal data situated overseas would appear to be a developing area. The treatment of Authorising Control for the purposes of the Data Breach Notification Obligation also remains an open question. There are, however, current indications that the PDPC may be prepared to take a practical approach in enforcement, for example, where the organisation does not reasonably have knowledge of specific arrangements across a transboundary supply chain. This is illustrated by the recent case of *Re Times Software Pte Ltd*[40] ("*Times Software*"):[41]

> (a) In *Times Software*, a data intermediary ("primary data intermediary") had outsourced certain payroll services to another subcontractor ("downstream data intermediary") to carry out data-processing activities that were directly related and necessary to what the data intermediary was undertaking to an organisation ("upstream organisation").
> (b) Observing (*inter alia*) that the upstream organisation "may not even be aware that its primary data intermediary had engaged a subcontractor",[42] the PDPC held that the upstream organisation, being in no position to "influence" the downstream data intermediary, should not be responsible for the downstream data intermediary.
> (c) The PDPC held, more generally, that:[43]
>
> > … where there are multiple layers of sub-contracting and sub-processing of personal data, there is a separate data controller and data intermediary relationship in each layer[, and] the scope of data processing outsourced in each layer of sub-contracting [will be]

40 [2020] SGPDPC 18.

41 For a detailed summary of facts, see WongPartnership, "Data Protection Quarterly Updates (October–December 2020): Special Update" (February 2021) at pp 2–4.

42 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [31].

43 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [31].

> determined by the relevant contract [setting out] the data controller's and data intermediary's respective obligations to protect the personal data. [emphasis in original omitted]

31 Of course, some open questions remain: What if the upstream organisation was in fact in a position to "influence" the downstream data intermediary – would any extent of demonstrable Authorising Control by the upstream organisation in respect of processing by a downstream data intermediary change any of the conclusions reached in *Times Software*? These issues await future clarification.

III. Basic framework for designing pre-emptive measures

32 Once the organisation discerns the parameters of its responsibilities under the PDPA for personal data situated overseas, the practical challenge would then be to design appropriate measures for its CBDI management plans in respect of such personal data.

33 The CARE protocol provided in the PDPC's *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act*[44] already presents a useful baseline for organisations to craft *response* measures to actual CBDIs, which of course may be further customised to address the organisation's needs and/or other foreign law requirements, as applicable.[45]

34 To complement the CARE protocol, the authors propose below a basic framework to guide an organisation's design of measures for CBDI management plans that are *pre-emptive* in nature, intended to address root causes, and with a preventive aim.[46] The authors' proposed framework is

---

44 Revised 15 March 2021.

45 "CARE" is an acronym for "Contain", "Assess", "Report", and "Evaluate", representing four key steps suggested by the Personal Data Protection Commission to be taken in the event of a data incident. See Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021). See also Lim Sui Yin, Jeffrey, "Implementing Data Breach Programmes: Understanding Nuances in Practice and the Personal Data Protection Act" [2020] PDP Digest 103.

46 Personal Data Protection Commission ("PDPC"), *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) ("the Guide") at p 6. The PDPC has indicated that the

(*continued on next page*)

loosely based on an adaption of the various principles of data protection by design[47] (which are, by their nature, pre-emptive principles), using such principles as launchpads for analysis.

A. Pre-emptive measures should be preventive in nature, with risk minimisation as the objective

35 Pre-emptive measures under a CBDI management plan should be designed to be preventive in nature, with risk minimisation as the objective. Such pre-emptive measures should include processes that enable the assessment, identification, management, and prevention of data protection risks in its cross-border data flows *before* they culminate as CBDIs, in order to "systematically identify and mitigate data protection risk".[48]

36 To identify the relevant risks that may lead to CBDIs, organisations should survey the international lifecycle of personal data in their Technical and/or Authorising Control. This may necessitate a process of global inventorisation and data flow audits, that is, documentation of personal data flows to understand how personal data is being collected, stored, used, disclosed, archived and/or disposed of worldwide through data inventory maps and/or data flow diagrams.

37 For example, basic cross-border inventorisation and data flow audit, from the perspective of the organisation in Singapore, may include a review of the following:

(a) the various types of personal data handled (or envisaged to be handled) by the organisation across all business units globally, as well

---

Guide is not intended to "specify the processes or systems that organisations should put in place to prevent future occurrence", or "additional measures … required to address the root cause(s)" of data incidents.

47 These refer to the seven foundational principles of Privacy by Design developed by the former Information and Privacy Commissioner of Ontario, as referenced in Personal Data Protection Commission, *Guide to Data Protection by Design for ICT Systems* (revised 14 September 2021) at pp 6–7. These include the following principles – "proactive and preventive", "data protection as the default", "end-to-end security", "data minimisation", "user-centric", "transparency" and "risk minimisation".

48 Personal Data Protection Commission, *Guide to Data Protection by Design for ICT Systems* (revised 14 September 2021) at p 7.

as the organisation's purposes for collecting, using, disclosing or processing it;

(b) the various outbound flows of personal data (including whether such personal data includes particularly sensitive species of personal data such as an individual's financial or health information), and the extent to which the organisation retains Technical Control and/or Authorising Control over such transferred data; and

(c) the various overseas receiving parties, and such recipients' purposes for collecting, using, disclosing or processing these sets of personal data, as well as the extent to which each such overseas recipient is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA (including a review of the adequacy of such legally enforceable obligations).

38 Organisations interested to align their inventorisation and data flow audits with international standards may find the "Record of Processing Activities" ("ROPA") required under Art 30 of the EU General Data Protection Regulation[49] ("GDPR") useful. Article 30 of the GDPR enumerates the comprehensive recording requirements for organisations within the scope of the GDPR in relation to a company's personal data processing activities, which must be produced to the relevant supervising authority upon request. As commentators have pointed out, the Art 30 ROPA requirements can be helpful as a template for the relevant data points to consider and may be adapted for the purposes of compliance with local laws even if one's purpose is not to comply with the GDPR.[50]

39 Once the cross-border personal data flows have been surveyed, relevant risks can then be identified (and prioritised) pursuant to data protection impact assessments conducted according to the PDPC's *Guide to Data Protection Impact Assessments*,[51] and pre-emptive measures implemented accordingly, for example, by ensuring that the organisation's

49 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

50 See, *eg*, Tanusha Verma & Grant Barrett, "The Value of Investing in Well-constructed Records of Processing Activities" *IAPP* (23 February 2021).

51 Published 1 November 2017.

privacy and security policies extend to all overseas personal data assessed to be under the organisation's Technical and/or Authorising Control. This exercise would also provide the organisation with the opportunity to evaluate potential vulnerabilities in any of its overseas transfers and evaluate how it may strengthen the security of the same.

40 To be clear, inventorisation and data flow audits are unlikely to be sufficient as once-off affairs and should be refreshed periodically in tandem with the evolution of business operations over time. In addition, it would also be important for the organisation to monitor risks on an ongoing basis. As the PDPC recommends, monitoring should be done "by both regular management oversight and using of monitoring tools", and in this regard, organisations should also consider subscribing to alerts and advisories on the latest cross-border data security trends, including alerts on emerging vulnerabilities and exploits.[52] Such awareness would enable organisations to "take action to mitigate the risks and vulnerabilities as soon as possible".[53]

B. Pre-emptive measures should integrate data protection on an "end-to-end" basis

41 Pre-emptive measures under a CBDI management plan should also integrate data protection on an "end-to-end" basis, in the sense of having

---

52 See Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 8. Where feasible, for example, the organisation may wish to consider monitoring of inbound and outbound traffic, deployment of real-time intrusion software, and/or use of security cameras for monitoring internal/external perimeters of its overseas data centres and sever rooms: see, *eg*, Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 9.

53 Personal Data Protection Commission ("PDPC"), *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 8. The PDPC provides some illustrations, *eg*:

> Logs from operating systems, applications and network devices should be regularly reviewed for anomalies and can help to identify malicious attacks on systems. Organisations may also subscribe to information sources such as SingCERT alerts and advisories on security issues, vulnerabilities and exploits which provide information on the latest security trends.

regard to (a) how the organisation and overseas recipients of data work together; and (b) how all the components of relevant technical systems interconnect across jurisdictions.[54]

42 First, "end-to-end" thinking requires that organisations take proactive steps to ensure that data protection measures are integrated into both the processes and features of the systems they have Technical Control over, as well as in their agreements with service providers governing the processing of personal data which they have Authorising Control over. Such efforts could provide a basis for the organisation to argue in the event of the CBDI that the organisation had taken steps to ensure reasonable security arrangements (under the Protection Obligation) and that the recipient is bound by legally enforceable obligations to provide to the transferred personal data "a standard of protection that is at least comparable" to the protection under the PDPA (under the Transfer Limitation Obligation).

43 The organisation should periodically consider whether there is a business need for any overseas transfer of personal data and whether its overseas establishments will require access to any of the personal data. For example, an organisation's overseas branches may not require access to the organisation's entire human resource database, and the organisation may exercise appropriate Technical Control with end-to-end security protocols put in place to restrict access by such overseas branches or only restrict access to key personnel on a need-to-know basis through encrypted communication channels by default.

44 Likewise, it would be in the interests of organisations to issue proper instructions to their overseas vendors and exercise reasonable oversight over their cross-border supply chains to ensure that outsourced providers are delivering the services as authorised. Otherwise, there is a risk that a failure of protection in respect of the personal data being processed overseas leading to a CBDI will fall on the organisation as a potential breach of the Transfer Limitation and/or Protection Obligation.[55]

45 Second, "end-to-end" thinking requires that organisations have regard to different jurisdictional requirements. As the PDPC emphasises,

---

54 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 8.

55 For a recent example of enforcement relating to the Protection Obligation, see *Re Tripartite Alliance Limited* [2021] SGPDPCS 3 at [11]–[12].

organisations "will separately have to determine the applicable laws in respect of the data activities involving personal data overseas".[56] Hence, being alive to the interconnection of processes across different jurisdictions on an "end-to-end" basis also means that the organisation should have regard to local data protection and other sectoral laws when developing CBDI management plans so that its plans can be coherent across multi-jurisdictional requirements.

46 In particular, there may be foreign law obligations that may apply in the event of a CBDI, such as data breach notification obligations to overseas regulators.[57] It would therefore be useful for organisations to be able to determine, pre-emptively, the applicable legislation in respect of their overseas data assets in the event of a CBDI, and their relevant obligations thereunder.

47 Likewise, when considering cross-jurisdictional requirements, organisations may also wish to take the opportunity to evaluate whether the overseas location has a "comparable data protection regime"[58] or whether regional certifications (such as the Asia-Pacific Economic Cooperation

---

56 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 11.1, fn 6.

57 For example, where the Singapore-based organisation also has an establishment in the European Union within the jurisdiction of the GDPR, the organisation would also be obliged to subject to the mandatory data breach notification requirements under the GDPR in addition to the Data Breach Notification Obligation under the Personal Data Protection Act 2012 (Act 26 of 2012). Accordingly, any of the organisation's cross-border data incident management plan will also need to be able to adequately address its parallel legal obligations under each of the respective applicable legislation. Local sector-specific obligations may also apply; for example, foreign requirements that may be analogous to the Monetary Authority of Singapore's *Notice 644 on Technology Risk Management* (21 June 2013) whereunder financial institutions shall notify the Monetary Authority of Singapore as soon as possible, but not later than one hour, upon the discovery of "relevant incident", which is defined to mean a system malfunction or information technology security incident, which has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers.

58 See, *eg*, Personal Data Protection Commission, *Guide to Managing Data Intermediaries* (21 September 2020) at p 33.

Cross Border Privacy Rules ("CBPR") System and Privacy Recognition for Processors ("PRP") System certifications) are applicable.[59] An overseas recipient that is CBPR or PRP certified will be considered legally bound to provide comparable protection for the transferred personal data to the PDPA, and such certifications can be helpful for an organisation's compliance with the Transfer Limitation Obligation.

48 As a practical matter, the organisation may also wish to impose contractual obligations on overseas persons processing personal data within the organisation's Authorising Control (for example, data intermediaries) to require compliance with established international technical standards such as the ISO/IEC 27001, ISO/IEC 27018:2019, ISO/IEC 29100:2011 and/or the Multi-Tier Cloud Security Standard for Singapore,[60] so as to demonstrate the organisation's efforts to ensure a consistent level of data protection across both local and overseas processing operations. As a matter of prudence, it would also be best practice for the organisation to conduct due diligence to ensure that outsourced providers have in place adequate data protection risk management programmes, which also extend to such providers' own subcontractors.[61] In this regard, the PDPC's *Guide to Managing Data Intermediaries*[62] provides further guidance to organisations concerning the management of data intermediaries, including in situations where such data intermediaries are offshore.[63]

C. Data minimisation

49 Organisations may wish to seriously consider taking the posture of data minimisation when reviewing its cross-border processes (where feasible, having regard to business needs), in the sense of strictly collecting,

---

59 See Personal Data Protection Commission, "Singapore Now Recognises APEC CBPR and PRP Certifications Under PDPA", media release (2 June 2020).

60 SS 584 (2013).

61 After all, "[t]he requirements need to be uniform throughout the chain because a data violation will end up affecting everyone involved": See Ryan Chiavetta, "How Do You Manage Your Vendor's Vendors?" *IAPP* (1 May 2019).

62 Published 21 September 2020.

63 Personal Data Protection Commission, *Guide to Managing Data Intermediaries* (21 September 2020).

storing and using personal data only to the extent "that is relevant necessary for the intended purpose for which data is processed".[64] Although data minimisation is not an express requirement under the PDPA, it may nevertheless be helpful to reduce risks in relation to a CBDI in terms of both "time" and "space".

50 As to time (in the sense of duration), if the organisation is relying on data intermediaries (such as offshore cloud services providers) to store personal data overseas, it should periodically review whether to cease such storage pursuant to its obligations under s 25 of the PDPA ("Retention Limitation Obligation").[65] From a risk minimisation perspective, as the PDPC has cautioned, "[h]olding personal data for an indeterminate duration of time increases the risk"[66] of the organisation contravening its other obligations under the PDPA over time.

51 As to space (in the sense of volume), the greater the amount of personal data that comes within the scope of the organisation's Technical and/or Authorisation Control, in respect of personal data situated overseas, the higher the data protection risk exposure for the organisation in the case of a CBDI. Organisations should therefore consider transferring and/or storing personal data overseas strictly to the extent relevant and necessary for the intended purpose for which data is processed so as to minimise the surface area liable to the risks of CBDIs occurring due to lapses that may occur overseas.

---

64 See Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 8.

65 The Retention Limitation Obligation requires the organisation to:

> … cease to retain 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 that personal data was collected is no longer being served by retention of the personal data; and
>
> (*b*) retention is no longer necessary for legal or business purposes.

66 See Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 February 2021) at para 18.1.

IV. Conclusion

52 When it comes to practical measures to be implemented under the PDPA, it is trite that "there is no 'one size fits all' solution" – each organisation would need to consider what is reasonable and appropriate in the circumstances, taking into account amongst other things the nature of the personal data, the form in which the personal data has been collected and the possible impact to the individual concerned.[67]

53 Specific commercial factors are also likely to feature strongly in the design of actual pre-emptive measures, including, for example, whether cyber insurance needs to be considered as a method of risk transfer to cushion the financial impact in the event of actual CBDIs,[68] as well as the bargaining position between the organisation and its offshore providers when crafting contractual obligations.

54 The authors' recommendations in this article are therefore not intended to be exhaustive because there can be no standard playbook for pre-emptive measures appropriate to every organisation and every potential CBDI. Nevertheless, the authors hope that the above framework provides useful building blocks with which each organisation can find helpful for the designing of bespoke pre-emptive measures for CBDI management plans.

55 Ultimately, in an increasingly interconnected world where cross-border personal data flows are becoming the new normal, pre-emptive measures for data protection are fast becoming essential investments. As the PDPC cautions, planning for data incident management is "best done early", and organisations who fail to do so "will find it chaotic and challenging" in the face of actual data incidents.[69] It may well be too little too late for organisations to wait to cross that breach when they get there.

---

67 See, for example, Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 17.2 and 12.41.

68 See, for example, Rafae Bhatti, "What SolarWinds Teaches Us about Managing Risk of Cyber Loss" *IAPP* (6 January 2021).

69 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 9.

WELCOMING THE MANDATORY DATA BREACH NOTIFICATION REGIME: A COMPARATIVE ANALYSIS AND OBSERVATIONS FROM PRACTICE*

LIM Chong Kin†
LLB (Hons), LLM (National University of Singapore);
Advocate and Solicitor (Singapore); Solicitor (England and Wales)

Charis SEOW‡
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore);
CIPP/E; CIPM

I. Introduction

1 One unfortunate statistic that rose in tandem with the dramatic increase of remote working arrangements in 2020 was the scale and frequency of cyberattacks and data breaches.[1] In this light, the introduction of the mandatory data breach notification regime in the Personal Data Protection Act 2012[2] ("PDPA") was both timely and significant.

2 With effect from 1 February 2021, organisations must comply with the Data Breach Notification Obligation ("DBN Obligation") in Part VIA

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer or any other party. All errors remain the authors' own. The authors also wish to acknowledge assistance rendered by Low Jia Rong (Associate, Drew & Napier LLC) for this article.

† Managing Director (Corporate & Finance), Head (Telecommunications, Media & Technology) and Co-Head (Data Protection, Privacy & Cybersecurity), Drew & Napier LLC; Co-Head, Drew Data Protection & Cybersecurity Academy.

‡ Assistant Vice President and Deputy Data Protection Officer, OCBC Bank.

1 See IdentityForce, "2020 Data Breaches" <https://www.identityforce.com/blog/2020-data-breaches> (accessed 30 June 2021). See also Ellen Sheng, "Cybercrime Ramps up Amid Coronavirus Chaos, Costing Companies Billions" *CNBC* (29 July 2020).

2 Act 26 of 2012.

of the PDPA. The DBN Obligation consists of two key components: (a) the duty to assess data breaches to determine if they are notifiable; and (b) the duty to notify the Personal Data Protection Commission ("PDPC") and affected individuals. The DBN Obligation has widespread practical implications for organisations and necessitates a review of existing data protection policies and procedures.

3 In this article, the authors will examine the mandatory data breach notification regime in Singapore and compare it to similar regimes in selected jurisdictions. The authors will then discuss the practical impact that the DBN Obligation has on organisations before sharing some observations from practice.

A. Background context

4 Data breach notification is not a new concept. Even before the amendments to the PDPA, the PDPC had already outlined a *voluntary* data breach notification regime in its *Guide to Managing Data Breaches*, which was published 8 May 2015 and subsequently revised on 22 May 2019 as the *Guide to Managing Data Breaches 2.0*.

5 Although the notification of data breaches was not mandatory at the time, the PDPC nevertheless considered voluntary notifications of data breaches to be a mitigating factor in its grounds of decisions[3] and a relevant consideration in its summary decisions.[4] The PDPC's stance towards notification of data breaches was taken by many to be a signal of what was to come.

B. Examination of the Data Breach Notification Obligation

6 As a preliminary point, the PDPA provides for separate definitions for a "data breach" and a "notifiable data breach". In other words, there is a

---

3 See *Re SPH Magazines Pte Ltd* [2020] SGPDPC 3; *Re Management Corporation Strata Title Plan No 3593* [2020] SGPDPC 6; and *Re Times Software Pte Ltd* [2020] SGPDPC 18.

4 See the Personal Data Protection Commission summary decisions *Re Chan Brothers Travel Pte Ltd* [2020] SGPDPCS 11; *Re RISEAerospace Pte Ltd* [2020] SGPDPCS 21; and *Re FWD Singapore Pte Ltd* [2020] SGPDPCS 5.

distinction between the two concepts and not all data breaches are automatically notifiable to the PDPC or the affected individuals.

7 A "data breach" is defined in s 26A of the PDPA as:

> (*a*) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or
> (*b*) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

8 In comparison, a "notifiable data breach", as defined in s 26B(1) of the PDPA, is where a data breach:

> (*a*) results in, or is likely to result in, significant harm to an affected individual; or
> (*b*) is, or is likely to be, of a significant scale.

9 The terms "significant harm" and "significant scale" are not defined in the PDPA. However, the PDPA provides that:[5]

> (a) a data breach is *deemed* to result in significant harm to an individual if it relates to any prescribed personal data or class of personal data; and
> (b) a data breach is *deemed* to be of a significant scale if it affects at least the prescribed number of individuals.

10 The circumstances in which significant harm or significant scale are deemed are found in regs 3 and 4 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021[6] ("DBN Regulations").

11 First, the criterion of "significant harm" will be examined. Regulation 3(1) of the DBN Regulations provides that a data breach is deemed to result in significant harm if it relates to:

> (*a*) the individual's full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual

5 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B(3).
6 S 64/2021.

set out in Part 1 of the Schedule, subject to Part 2 of the Schedule;[7] or

(*b*) all of the following personal data relating to an individual's account with an organisation:

(i) the individual's account identifier,[8] such as an account name or number;

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

12 The PDPC, in its *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act*[9] ("Data Breach Guide"), explains that "significant harm" could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation and other forms of harms that a reasonable person would identify as a possible outcome of a data breach.[10]

13 Based on how reg 3(1)(*a*) of the DBN Regulations is presented, it suggests that in order for a data breach to be deemed to result in significant harm, the breach in question must relate to an individual's full name, alias, or identification number, *and* a particular class of personal data set out in the Schedule to the DBN Regulations.

14 The use of the word "and" gives rise to the impression that the two criteria under reg 3(1)(*a*) of the DBN Regulations are cumulative. As such, the disclosure of full names and identification numbers alone in a data breach scenario may not trigger a notification, unless it can be shown that

---

7 Examples of prescribed information includes financial information; life, accident and health insurance information; identification of vulnerable individuals; physical and mental health information; and information on abuse (domestic, child, and sexual); information on adoption matters, *etc*.

8 An "account identifier" includes a number assigned to any account the individual has with an organisation that is a bank or finance company: reg 3(2) of the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021).

9 Revised 15 March 2021.

10 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 23, fn 5.

other types of prescribed personal data (*eg*, credit card or bank account numbers) were also part of the compromised dataset.

15 However, the authors also note the use of the qualifying phrase "without limiting subsection (1)(*a*)" in s 26B(2) of the PDPA. This suggests that the scope of ss 26B(1)(*a*) and 26B(2) of the PDPA do not completely overlap. In this regard, there could be scenarios where reg 3(1) of the DBN Regulations is not triggered but where the disclosure of a particular dataset (*eg*, full names, identification numbers and mobile phone numbers) could nevertheless trigger a notification pursuant to s 26B(1)(*a*) of the PDPA. One such scenario may be where the full name and other identification exposed in a data breach could result in identity theft by a malicious party.

16 The authors now turn to the criterion of "significant scale". The prescribed number of affected individuals under reg 4 of the DBN Regulations is 500. Notably, a data breach affecting 500 or more individuals must be notified to the PDPC *even if* the data breach does not involve prescribed personal data under the Schedule to the DBN Regulations.[11]

17 Section 26B(3) of the PDPA similarly includes the qualifying phrase "without limiting subsection (1)(*b*)". While the number of affected individuals is fixed in the DBN Regulations at 500, another factor which may affect the scale of a data breach could be the amount of personal data exposed in the data breach. Hence, where there are fewer than 500 affected individuals in a data breach, but a very large quantity of personal data is exposed or, in fact, has been exfiltrated by a malicious party, the organisation may wish to assess the risk to the individuals concerned in considering whether the data breach should be regarded as being of a significant scale.

---

11 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.20. See also Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 24.

C. Duty to assess the data breach

18 Once organisations have a "reason to believe" a personal data breach has occurred, they must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is notifiable.[12]

19 In terms of timing, the PDPC's *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[13] ("Key Concepts Guidelines") provide that organisations should aim to conduct their assessment (*ie*, establish the facts surrounding the data breach and determine whether it is notifiable) within 30 calendar days. If an organisation is unable to do so within that time frame, it should be prepared to provide the PDPC with an explanation. Unreasonable delays may be a breach of the DBN Obligation, which may result in the PDPC taking enforcement action.[14]

20 For data intermediaries, once they have a reason to believe that a data breach has occurred, they must notify the primary organisation or the public agency for which it is processing personal data "without undue delay".[15] Where an organisation has been so notified, it has a duty to assess the breach.[16]

D. Duty to notify the Personal Data Protection Commission and affected individuals

21 Once an organisation assesses that a data breach is a notifiable data breach, it must notify the PDPC "as soon as is practicable" but, in any case, no later than three calendar days after the day it makes the assessment.[17]

---

12 Personal Data Protection Act 2012 (Act 26 of 2012) s 26C(2).

13 Revised 1 October 2021.

14 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.4. See also Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 22.

15 Personal Data Protection Act 2012 (Act 26 of 2012) ss 26C(3) and 26E. See also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.7.

16 Personal Data Protection Act 2012 (Act 26 of 2012) s 26C(3)(*b*).

17 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(1).

22 In comparison, there is no fixed timeline for notifying the affected individuals. Unless an exception applies, the organisation must notify affected individuals "in any manner that is reasonable in the circumstances".[18] Organisations are not required to notify individuals if significant harm is rendered unlikely because of previously implemented technology measures or responsive actions.[19]

23 Aside from the duty to the notify the PDPC and affected individuals, organisations may report the incident to the police if they suspect that criminal acts have been perpetrated as part of the data breach, and to the Singapore Computer Emergency Response Team where a data breach is also a cyber incident.

II. Comparative overview of other data breach notification regimes

24 In this next part, the authors will compare elements of the DBN Obligation with the data breach notification regimes in other selected jurisdictions.

A. Duty to assess data breaches

25 The authors highlight that the duty to assess "in a reasonable and expeditious manner" whether a data breach is notifiable under s 26C of the PDPA bears strong resemblance to the wording in s 26WH of Australia's Privacy Act 1988. Under that provision, once there are reasonable grounds to suspect an eligible data breach, the entity must carry out "a reasonable and expeditious assessment" of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach and take all reasonable steps to ensure that the assessment is completed within 30 days.[20]

18 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(2).

19 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(5). There are other exceptions in ss 26D(6) and 26D(7).

20 Privacy Act 1988 (Cth) s 26WH.

B. Notification to the authorities

26 Most jurisdictions are aligned on the position that only data breaches which pose sufficient risk or serious harm to the affected individuals, or satisfy some criteria relating to risk or harm, need to be notified to the authorities. The following examples were considered:

(a) The European Union's ("EU's") General Data Protection Regulation[21] ("GDPR"): It is mandatory for data controllers to notify the supervisory authority of a data breach "unless the personal data breach is unlikely to result in a *risk to the rights and freedoms of natural persons*" [emphasis added].[22] Specifically, the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing.[23]

(b) Australia's Privacy Act 1988: An "eligible data breach" is one where "a reasonable person would conclude that the access or disclosure would be likely to result in *serious harm*" [emphasis added].[24]

(c) Canada's Personal Information Protection and Electronic Documents Act:[25] Organisations must report data breaches to the Privacy Commissioner "if it is reasonable in the circumstances to believe that the breach creates a *real risk of significant harm* to an individual" [emphasis added].[26]

(d) New Zealand's Privacy Act 2020:[27] A "notifiable privacy breach" is one where "it is reasonable to believe has caused *serious harm* to an

21 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").

22 GDPR Art 33(1).

23 GDPR Recitals 75 and 76.

24 Privacy Act 1998 (Cth) ss 26WE(2)(a)(ii) and 26WE(2)(b)(ii).

25 SC 2000, c 5.

26 Personal Information Protection and Electronic Documents Act (SC 2000, c 5) s 10.1.

27 2020 No 31.

affected individual or individuals or is likely to do so" [emphasis added].[28]

(f) Philippines' Data Privacy Act of 2012:[29] Notification is required when sensitive personal information or any other information that may be used to enable identity fraud is reasonably believed to be acquired by an unauthorised person, and if such acquisition is likely to give rise to a *real risk of serious harm* to any affected data subject.[30]

27 In many jurisdictions, the data protection laws specify a list of factors to consider when assessing risk in a data breach scenario. In the EU, the European Data Protection Board recommends that organisations consider seven different factors when assessing the risks to individuals as a result of a data breach, including the type of breach; the nature, sensitivity and volume of personal data; the severity of consequences for the affected individuals; and the number of affected individuals.[31]

28 Similarly, Australia's Privacy Act 1998 lists eight "relevant matters"[32] in determining whether the data incident would likely result in serious harm, while New Zealand's Privacy Act 2020 sets out six considerations when assessing whether a privacy breach is likely to cause serious harm.[33] It is observed that there are some overlapping factors including the sensitivity of the data; whether the data is protected by a security measure; or the nature of the harm.

29 In the Philippines, the relevant considerations include whether the personal data would likely affect national security or public safety; whether

28 Privacy Act 2020 (2020 No 31) (New Zealand) s 112(1)(a).

29 Republic Act 10173.

30 See s 20(f) of the Data Privacy Act of 2012 (Republic Act 10173). See also s 38(c) of the Implementing Rules and Regulations of the Data Privacy Act of 2012; and National Privacy Commission, *Personal Data Breach Management* (NPC Circular 16-03) (15 December 2016) section 11.

31 European Data Protection Board, *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (revised and adopted on 6 February 2018) at pp 24–26.

32 Privacy Act 1988 (Cth) ss 26WG(c)–26WG(j).

33 Privacy Act 2020 (2020 No 31) (New Zealand) ss 113(a)–113(f).

at least 100 individuals will be affected; and whether the breach involves vulnerable groups.[34]

30 In contrast, the deeming provisions in ss 26B(2) and 26B(3) of the PDPA, when read with the DBN Regulations, offer organisations greater clarity by stipulating the exact types of personal data that would satisfy the "significant harm" limb of the DBN Obligation, as well as an exact numerical threshold for the "significant scale" limb.

31 It should be highlighted that regs 3 and 4 of the DBN Regulations bear remarkable resemblance to the notification requirements in the California Civil Code. Under California law, businesses must notify individuals once there is a breach of personal information.[35] The term "personal information" is defined as either (a) a first name (or first initial) and last name in combination with the listed data elements such as social security numbers, credit card numbers, medical and health insurance information, and biometric data; or (b) a username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.[36] Further, if a business is required to notify more than 500 California residents, the business must also notify the state attorney-general.[37]

C. Time frames for notification to the authorities

32 Section 26D(1) of the PDPA requires organisations to notify data breaches to the PDPC as soon as is practicable, but in any case no later than three calendar days after the day the organisation makes that assessment. Notably, the notification requirement is only triggered *after* the organisation has made its assessment of the data breach (of which it has 30 days to complete).

33 In comparison, the formulation is slightly stricter under the GDPR which requires a notification to be made "without undue delay and, *where feasible*, not later than 72 hours after having become aware of it" [emphasis

34 See National Privacy Commission, *Personal Data Breach Management* (NPC Circular 16-03) (15 December 2016) section 13.

35 California Civil Code §1798.82(a).

36 California Civil Code §1798.82(h).

37 California Civil Code §1798.82(f).

added].[38] Another jurisdiction that adopts a similar time frame is the Philippines where notification to the authorities is required within 72 hours of knowledge or reasonable belief that a personal data breach has occurred.[39]

34 In contrast, instead of fixed timelines to notify the authorities, the privacy laws in Australia and New Zealand require organisations to notify the respective authorities "as soon as practicable"[40] while Canada requires notification "as soon as feasible after the organisation determines that the breach has occurred".[41]

D. Notification to affected individuals

35 Turning to the criteria for notifying the affected individuals, it was observed that jurisdictions generally set a higher threshold for such notification. In some cases, there are statutory exceptions to this notification requirement.

36 Under the GDPR, a data controller will need to notify the affected individuals of a data breach where the data breach is likely to result in a *high risk* to the rights and freedoms of natural persons without undue delay.[42] Because the risk has to be "high", the threshold for notification to the affected individuals rests higher than the notification to the supervisory authorities.[43] Moreover, there is no need to notify the individuals if any of three specified conditions under the GDPR are met.[44]

37 Under Australia's Privacy Act 1988, depending on each option's practicability, organisations can notify all affected individuals, just the

38 GDPR Art 33(1).

39 National Privacy Commission, *Personal Data Breach Management* (NPC Circular 16-03) (15 December 2016) section 17(A).

40 Privacy Act 1988 (Cth) s 26WK(2)(b); Privacy Act 2020 (2020 No 31) (New Zealand) s 114.

41 Personal Information Protection and Electronic Documents Act (SC 2000, c 5) s 10.1(2).

42 GDPR Art 34.

43 European Data Protection Board, *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (revised and adopted on 6 February 2018) at p 20.

44 GDPR Art 34(3).

individuals at risk, or publish the statement given to the Privacy Commissioner on their websites, taking reasonable steps to publicise the statement's contents.[45]

38 Under New Zealand's Privacy Act 2020, exceptions have been spelt out in considerable detail. These include exceptions for the maintenance of the law, individual safety, protecting trade secrets and special health considerations.[46]

39 Singapore's position is broadly in alignment with the above jurisdictions. Where an exception applies, an organisation does not need to notify affected individuals of a data breach (though it must still notify the PDPC).[47] The two main exceptions are where:[48]

> (a) the organisation has taken remedial actions that render it unlikely that the notifiable data breach will result in significant harm to the affected individual; or
>
> (b) the personal data that was compromised by the data breach is subject to technological protection (*eg*, encryption) that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

E. Time frames for notification to affected individuals

40 The PDPA is largely in line with other jurisdictions which do not prescribe a fixed time frame for notification to affected individuals. During the second reading of the Personal Data Protection (Amendment) Bill, the

45 Privacy Act 1988 (Cth) s 26WL(2).

46 Privacy Act 2020 (2020 No 31) (New Zealand) s 116.

47 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(2). See also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.27.

48 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(5). In addition, under s 26D(6), organisations may be obliged to withhold notification to the affected individuals if instructed by a law enforcement agency or directed by the Personal Data Protection Commission ("PDPC"). Under s 26D(7) an organisation may apply to the PDPC to waive the requirement.

Minister for Communications and Information, S Iswaran, explained the rationale for this approach:[49]

> We have not set a fixed timeframe for an organisation's notification to affected individuals of a data breach because data breach circumstances can be very varied. Our positions have been developed in consultation with the public and benchmarked against jurisdictions like Australia, Canada, the EU and California. I will not rule out anything, but I think in the first instance we want to move forward and see how this works in practice.

41 Under the GDPR, the data controller must communicate the personal data breach to the data subject "without undue delay",[50] while the time frames for notifying the affected individuals under the laws of Australia, New Zealand and Canada largely mirror their time frames for notifying the authorities. In contrast, organisations in the Philippines are required to notify affected individuals within 72 hours.[51]

III. Practical impact of the DBN Obligation

A. Develop and implement a robust data breach management plan

42 One immediate practical step to ensure compliance with the DBN Obligation is to have a robust data breach management plan. In designing and implementing such a plan, the organisation may take guidance from the PDPC's Data Breach Guide.[52]

43 As a first step, organisations should assemble a data breach response team which should include the data protection officer. As this team will take the lead in a data breach scenario, it is recommended that some team

---

49 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

50 GDPR Art 34.

51 National Privacy Commission, *Personal Data Breach Management* (NPC Circular 16-03) (15 December 2016) section 18(A).

52 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at pp 9–11.

members are management-level personnel to ensure that time-critical decisions can be made without delay.

44 Second, a robust data breach management plan should provide a clear explanation of what constitutes a personal data breach. Ideally, this should include illustrations of the common types of data breaches within similar organisations. This may be accompanied by a risk assessment matrix which will assist the team in assessing whether a data breach is notifiable.

45 Third, there should be a clear reporting structure on when to escalate the data breach to the management team or board. In a large organisation, it may not always be feasible to educate all employees on what needs to be done in a data breach scenario. However, at the minimum, employees should be able to identify a data breach and know when and how to escalate it.

46 Finally, in respect of the steps to respond to a data breach, a robust data breach management plan should thoroughly address each step of the "CARE" framework:[53]

(a) Contain the data breach and implement mitigating actions.

(b) Assess the data breach and the effectiveness of containment actions taken.

(c) Report, if required, the data breach to the PDPC and the affected individuals.

(d) Evaluate the response and consider future preventative measures.

B. Contracts with vendors and third parties

47 In addition, organisations should consider reviewing their existing contracts with vendors and other third-party service providers.

48 Organisations should negotiate to include clauses that require counterparties to co-operate in the event of a data breach. Such clauses should be broad enough to address the containment, assessment and

53 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 13.

notification of a data breach.[54] Where appropriate, organisations may also include indemnities for losses suffered by late or deficient notifications that can be attributable to the counterparty's fault or negligence.

49 In a situation where its vendor is a data intermediary, the organisation should also ensure that the contract requires the vendor to notify the organisation of a data breach without undue delay. To reduce ambiguity, the organisation may wish to specify an exact time frame (*eg*, 24 hours).

50 To address the above points, existing vendor contracts may be modified through supplemental agreements or by way of an addendum to the original contract.

51 As good practice, organisations may also wish to update their contract templates to include data breach notification clauses and include compliance with the DBN Obligation as an additional item in its third-party due diligence checklists.

C. Risk monitoring and continuing compliance

52 Through early detection, effective data monitoring systems can limit the fallout from a data breach. The PDPC recommends that organisations monitor their network traffic for abnormal activities, use real-time intrusion detection software, and deploy security cameras to monitor data centres and server rooms.[55]

53 To ensure continued compliance with the DBN Obligation, organisations should keep their data breach management plans up to date and refresh them at periodic intervals. To ensure that plans run smoothly, organisations should consider conducting "fire drills", walkthroughs or tabletop exercises that simulate data breach incidents.

54 Moreover, to ensure employees across departments know when to escalate actual or suspected data breaches, familiarity with reporting procedures should be addressed in staff data protection training sessions.

---

54 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(2). See also Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at p 131, fn 56.

55 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 9.

IV. Some observations from practice

55 In this next part, the authors will share some observations from assisting clients in managing data breaches, and the common challenges that arise in practice.

56 For organisations that are unprepared, managing a data breach is fraught with challenges. Without a contingency plan, containing the data breach, co-ordinating the internal investigation with multiple parties and reporting to an anxious board can be a stressful experience.

57 Often, this stress is compounded where the data breach is a result of a cyber-attack and the organisation has to co-ordinate with information technology ("IT") vendors who may be based remotely, located in other time zones or unfamiliar with the organisation's internal set-up. In the more sophisticated cyber-attacks, the internal IT may not be equipped to handle the initial containment and external cyber experts may need to be engaged.

58 Another source of stress is where a data breach spans multiple jurisdictions, necessitating a global investigation. A well-coordinated response is difficult to achieve when the data breach response team is under pressure to quickly ascertain the extent of the breach (oftentimes amid evolving facts) and juggle the different data breach notification requirements and time frames across jurisdictions.

59 In practice, not many organisations are fully equipped to tackle complex data breaches alone. The authors recommend that organisations prepare a list of third parties to activate during a crisis as it is challenging to onboard third parties under urgent deadlines. These third parties may include external law firms to provide legal advice and prepare the notifications to the PDPC and/or affected individuals, and cyber forensic investigators to assist with risk assessment and work with the organisation's IT team.

60 Conversely, it has also been observed that where organisations already have robust IT incident response plans, they may choose to incorporate the DBN Obligation into their existing incident response framework. However, organisations should be aware that while there are overlaps (*eg*, a ransomware attack where electronic files containing personal data are compromised), there remains a distinction between an IT incident and a data breach incident. Some IT incidents (*eg*, power outages or network

disruptions) are not data breaches, whereas some data breaches (*eg*, accidental disclosures of personal data) are not IT incidents.

61 Depending on the circumstances, the financial and reputational fallout from a data breach can be severe. Organisations may wish to weigh the costs and benefits of obtaining insurance especially for cybersecurity incidents.

62 Another challenge is the pressure for a swift public relations ("PR") response. Organisations may choose to engage crisis management and PR firms to minimise negative publicity from the data breach. Organisations are reminded that their press release, notification to the PDPC (and other regulators) and notification to affected individuals should be factually consistent across the board. Some organisations prepare internal memorandums and frequently asked questions to ensure the data breach response team and external PR teams are on the same page.

63 Finally, the authors highlight some legal considerations. If a risk of litigation or regulatory action is identified, organisations should preserve documents as evidence. Some organisations choose to circulate a litigation hold notice to suspend document destruction policies. In communications, organisations should consider the importance of preserving legal privilege and confidentiality, and reserving their rights against potential adverse parties.

V. Concluding thoughts

64 Ultimately, organisations should treat data breaches like any other unforeseen business risk and put in place a robust data breach management plan to prevent panic, protect resources, minimise losses and interruptions, and ensure daily operations can return to normal after the initial crisis.

THE DATA BREACH NOTIFICATION OBLIGATION AND CASE STUDIES FOR FINANCIAL INSTITUTIONS AND EMPLOYERS*

Alexander YAP Wei-Ming†
MA (Oxon), Advocate and Solicitor (Singapore)

Eugene HO Yizhe‡
LLB (NUS), Advocate and Solicitor (Singapore)

TAN Zhi Feng§
LLB (NUS), Advocate and Solicitor (Singapore)

Christine TEE Hui Min¶
LLB (NUS), Advocate and Solicitor (Singapore)

Jean CHAN#
LLB (NUS), Advocate and Solicitor (Singapore)

I. Introduction

1 The growing trend of data breaches across the world, compounded with the potentially enormous costs associated with such breaches, is worrying for both individuals and organisations in Singapore. The *Singapore Cyber Landscape 2020*[1] reported that the ongoing COVID-19 pandemic sparked a global surge in cybercrime in 2020, and that with the rise in ransomware attacks the frequency of data breaches is expected to

---

* Any views expressed in this article are the authors' personal views only, and should not be taken to represent the views of Allen & Gledhill LLP. All errors remain the authors' own.

† Partner, Allen & Gledhill LLP.

‡ Partner, Allen & Gledhill LLP.

§ Partner, Allen & Gledhill LLP.

¶ Partner, Allen & Gledhill LLP.

\# Associate, Allen & Gledhill LLP.

1 8 July 2021. See Cyber Security Agency of Singapore, *Singapore Cyber Landscape 2020* (8 July 2021) at pp 12–13.

remain high. A Singapore threat report, which sought to examine the effect of COVID-19, reported that pursuant to March–April 2020 surveys, 93% of Singapore respondents had seen an increase in overall cyber-attacks as a result of employees working from home.[2]

2 To strengthen organisations' accountability and to empower individuals to take timely measures to protect themselves[3] (and, in the authors' view, perhaps in a wary acknowledgement that data breaches may be increasingly ubiquitous), Singapore's data protection laws were recently amended to establish a mandatory data breach notification regime. Pursuant to the Personal Data Protection (Amendment) Act 2020[4] ("the Amendment Act"), a new Part VIA on the notification of data breaches was introduced to the Personal Data Protection Act 2012[5] ("PDPA") together with a set of subsidiary legislation regulating the notification of data breaches – the Personal Data Protection (Notification of Data Breaches) Regulations 2021[6] ("the Notification Regulations"). Part VIA of the PDPA has been in effect since 1 February 2021.

3 The article first provides a general overview of the data breach notification obligation regime under the PDPA.[7] Thereafter, the article discusses how such regime interacts with certain reporting requirements applicable to financial institutions regulated by the Monetary Authority of Singapore ("MAS"),[8] and issues employers face where employees whose acts or omissions had directly or indirectly caused a data breach.[9]

---

2 See VMWare Carbon Black, *Singapore Threat Report: Extended Enterprise Under Threat* (June 2020) at p 8.

3 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

4 Act 40 of 2020. The Amendment Act partially came into operation on 1 February 2021.

5 Act 26 of 2012.

6 S 64/2021.

7 See paras 4–14 below.

8 See paras 15–25 below.

9 See paras 26–40 below.

II. Data breach notification

A Overview of data breach notification obligation

(1) "Data breach"

4 The term "data breach" is defined in the PDPA to mean:[10]

(*a*) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or

(*b*) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

5 The definition of "data breach" is broad and there is no restriction as to how a breach may arise, whether through acts of malicious third parties, acts of rogue or negligent employees, human errors, technical or system errors, or otherwise. The unauthorised acts of access, collection, use, disclosure, copying, modification or disposal are also far-reaching and ransomware or involuntary encryption would generally be considered to fall within such unauthorised use.[11] No exfiltration of data is needed.[12] Advanced persistent threats, where the undetected infiltrators establish a foothold in the network and gain access to personal data, would likely constitute a data breach even if no personal data is extracted.

(2) "Notifiable data breach"

6 A data breach is a "notifiable data breach" under the PDPA if it:[13]

(*a*) results in, or is likely to result in, significant harm to an affected individual; or

(*b*) is, or is likely to be, of a significant scale.

---

10 Personal Data Protection Act 2012 (Act 26 of 2012) s 26A.

11 See, for example, *Re HMI Institute of Health Sciences Pte Ltd* [2021] SGPDPC 4.

12 In the authors' view, taking into account the Personal Data Protection Commission's views in decisions such as *Re PeopleSearch Pte Ltd* [2020] PDP Digest 525.

13 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B.

7 On the assessment of "significant harm", guidance from the Personal Data Protection Commission ("PDPC") indicates that such harm could include physical, psychological, economic and financial harm, and other forms of severe harms that a reasonable person would identify as a possible outcome of a data breach.[14] In any event, a data breach is deemed to result in significant harm to an individual if it relates to:[15]

> (a) the individual's full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual set out in Part 1[16] (subject to Part 2)[17] of the Schedule to the Notification Regulations; or
>
> (b) all of the following personal data relating to an individual's account with an organisation:
>
> > (i) the individual's account identifier,[18] such as an account name or number;

14 Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.13, fn 57.

15 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B(2); Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021) reg 3(1).

16 This would include, for example, the individual's remuneration, income, credit/debit card number, bank account number, certain information of minors and vulnerable adults, information leading to identification of alleged victims of specified sexual offences, private key, net worth, certain financial information, credit worthiness, certain insurance, health or reproductive information, and certain adoption information.

17 The prescribed personal data or classes of personal data set out in Part 1 of the Schedule to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021) ("Notification Regulations") excludes (a) personal data that is publicly available (not solely because of any data breach); and (b) personal data that is disclosed to the extent that is required or permitted under any written law. See paras 1 and 2 of Part 2 of the Schedule to the Notification Regulations.

18 The term "account identifier" includes a number assigned to any account the individual has with an organisation that is a bank or finance company, pursuant to reg 3(2) of the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021).

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

8 For the assessment of "significant scale", a data breach is deemed to be of a significant scale if the data breach affects not fewer than 500 individuals.[19] If an organisation is unable to determine the actual number of affected individuals, the organisation should notify the PDPC when it has reason to believe[20] that the number of affected individuals is not fewer than 500 individuals.[21]

(3) "Assessment of whether the data breach is a notifiable data breach"

9 There are three main factors that would trigger an organisation's obligation to conduct an assessment of whether the data breach is a notifiable data breach:

(a) a *data breach* affecting personal data;[22]

(b) the organisation must have *reason to believe* that a data breach affecting personal data has occurred. Note that the threshold of "reason to believe" is also explained in the PDPC's published guidance as having "credible grounds to believe", for example through self-discovery, alert from the public, or notification from a data intermediary;[23] and

---

19 Personal Data Protection Act 2012 (Act 26 of 2012) s 26B(3); Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021) reg 4.

20 See para 9 below regarding "reason to believe".

21 This may be based on the estimated number from an initial appraisal of the data breach. The organisation may subsequently update the Personal Data Protection Commission of the actual number of affected individuals when it is established. See Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 24; Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.21.

22 See para 4 above on the definition of "data breach".

23 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021)

(*continued on next page*)

(c) the personal data affected is *in the possession or under the control of* the organisation.[24]

10 If all of the above factors are satisfied, the organisation must conduct an assessment of whether the data breach is a notifiable data breach in a reasonable and expeditious manner. This assessment should generally be completed within 30 calendar days.[25] The steps taken as part of the assessment should be documented, as these documents may be required to be produced to the PDPC if there is a notification to the PDPC, or any investigation of the suspected data breach by the PDPC.[26]

11 It should be noted that the obligation to conduct an assessment of whether the data breach is a notifiable data breach does not apply to data intermediaries.[27] The data intermediary's obligation, where it has reason to believe that a data breach has occurred in relation to personal data that such data intermediary is processing on behalf of and for the purposes of another organisation (*ie*, the "data controller"), is to without undue delay notify that data controller of the occurrence of the data breach.[28] It would then be incumbent on the data controller to, upon notification by the data intermediary, conduct an assessment of whether the data breach is a

---

at p 22; Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.2.

24 Personal Data Protection Act 2012 (Act 26 of 2012) s 26C(2).

25 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 22; Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.4.

26 Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 22; Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 20.5.

27 Section 2 of the Personal Data Protection Act 2012 (Act 26 of 2012) defines "data intermediary" to mean "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation".

28 Personal Data Protection Act 2012 (Act 26 of 2012) s 26C(3)(*a*).

notifiable data breach.[29] Put another way, the obligation is on the data intermediary to notify the data controller; and the obligation is on the data controller to conduct the requisite assessment and thereafter perhaps to notify the PDPC and affected individuals.

(4) "Notify the Commission"

12 Where an organisation has assessed that the data breach is a notifiable data breach, the organisation must notify the PDPC as soon as practicable, in any case no later than three calendar days after the day the assessment was made.[30] To illustrate, if the organisation determines on 1 December 2021 that a data breach is notifiable, the organisation must notify the PDPC by 4 December 2021.

13 The notification to the PDPC should be in the PDPC's prescribed form[31] and contain all prescribed information[32] to the best the knowledge and belief of the organisation at the time of notification.[33]

(5) "Notify each affected individual"

14 Where an organisation has determined that the data breach is a notifiable data breach and so notifies the PDPC, the organisation must also notify each affected individual (*ie*, each affected individual to which

---

29 Personal Data Protection Act 2012 (Act 26 of 2012) s 26C(3)(*b*).

30 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(1).

31 The notification must be in the form and manner specified by the Personal Data Protection Commission and can be submitted at <https://eservice.pdpc.gov.sg/case/db> (accessed 1 December 2021). See Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at p 26.

32 See reg 5 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021); see Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at pp 26–27 and Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 20.38–20.41.

33 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(3)(*a*).

significant harm results or is likely to result)[34] with the prescribed information[35] at the same time or after notifying the PDPC, unless any exceptions[36] in the PDPA apply.

III. Case study 1: Financial institutions

A. Monetary Authority of Singapore regulations and the Personal Data Protection Act regime

15 The PDPA was first enacted in 2012 in response to a need for a general data protection framework to ensure a baseline standard of protection for individuals' personal data, as the then-sectoral frameworks for data protection (*eg*, for the protection of financial and health data) were disparate.[37] The enactment of the PDPA, however, has not brought about a harmonisation or rationalisation of the general personal data protection

34 See s 26D(2) of the Personal Data Protection Act 2012 (Act 26 of 2012) which states that "[s]ubject to subsections (5), (6) and (7), on or after notifying the Commission under subsection (1), the organisation must also notify each affected individual affected by *a notifiable data breach mentioned in section 26B(1)(*a) in any manner that is reasonable in the circumstances" [emphasis added]. This makes it clear that the obligation to notify the individual only arises where significant harm results or is likely to result to the individual. Put another way, if the data breach is of a "significant scale" but does not result in "significant harm" to the affected individuals, such affected individuals need not be notified.

35 See reg 6 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021); Personal Data Protection Commission, *Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act* (revised 15 March 2021) at pp 28–29; and Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 20.42–20.45.

36 See s 26D of the Personal Data Protection Act 2012 (Act 26 of 2012); Personal Data Protection Commission Singapore, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at paras 20.26–20.34.

37 *Parliamentary Debates, Official Report* (15 October 2012), vol 89 at p 827 (Assoc Prof Dr Yaacob Ibrahim, Minister for Information, Communications and the Arts).

regime under the PDPA with the existing sectoral regulations for financial institutions in Singapore. Instead, the PDPA applies in parallel with financial regulations under the purview of the MAS. Regulated financial institutions in Singapore therefore have to contend with two separate, overlapping regimes.

16 The introduction of the data breach notification obligations under the PDPA gives rise to the same issue of overlapping regimes for regulated financial institutions in Singapore. The data breach notification obligations under the PDPA are expressed to "apply concurrently with any obligation of the organisation under any other written law to notify any other person (including any public agency) of the occurrence of a data breach, or to provide any information relating to a data breach".[38] Regulated financial institutions therefore have to consider, when a data breach occurs, (a) what type of information is involved; and (b) whether they are separately required to notify the MAS under financial regulatory laws and regulations.

(1) Overlapping types of information

17 Financial institutions should be aware of the separate types and classes of data and information that are regulated under the PDPA and financial regulatory laws and regulations, respectively.

18 For example, banks licensed in Singapore under the Banking Act[39] continue to be subject to laws governing the privacy of customer information under the Banking Act, and, separately, the obligations under the PDPA. Under the Banking Act, banks are required to ensure that customer information is not disclosed to any other person except as expressly permitted under the provisions of the Banking Act.[40] "Customer information" is defined for this purpose to mean any information relating to, or any particulars of, an account (whether in respect of a loan, investment or any other type of transaction) of a customer, or any deposit information.[41]

38 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(9).

39 Cap 19, 2008 Rev Ed.

40 Banking Act (Cap 19, 2008 Rev Ed) s 47; Third Schedule.

41 Banking Act (Cap 19, 2008 Rev Ed) s 40A.

19 In the case of individuals, such customer information could separately constitute personal data subject to the PDPA. Conversely, the types and classes of personal data prescribed in the Notification Regulations (*eg*, account number, credit card, charge card or debit card number, deposit or withdrawal of moneys, granting of advances, loans and other facilities, and investment in any capital market products),[42] in relation to the assessment of whether a data breach is deemed to result in significant harm, may include customer information.

20 In the case of corporate or other entities, such customer information may or may not include personal data, depending on the nature of the specific information. A further consideration would also be whether data relating to individuals of such corporate or other entities may in any event constitute "business contact information"[43] and thus fall outside of the ambit of the PDPA's data breach notification regime.

21 On the other end of the spectrum, information of employees of the bank would likely constitute personal data subject to the PDPA, but would not be customer information subject to the privacy of customer information obligations under the Banking Act.

(2) Overlapping reporting requirements

22 A data breach may involve circumstances that separately give rise to reporting requirements for financial institutions regulated by the MAS. The following are examples of financial regulatory reporting requirements that may arise in a data breach.

(a) Financial institutions are required to notify the MAS of any material adverse developments.[44] Material adverse developments

42 Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021) reg 3; Schedule, Part 1.

43 Pursuant to s 2 of the Personal Data Protection Act 2012 (Act 26 of 2012):

> 'Business contact information' means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.

44 Monetary Authority of Singapore, *Guidelines on Individual Accountability and Conduct* (10 September 2020; effective 10 September 2021) at para 5.3.

include misconduct, lapses in risk management and controls, or breaches in legal or regulatory requirements that have the potential to cause widespread disruption to the financial institution's day-to-day operations, services or activities, and/or significantly impact the financial institution's customers and other stakeholders, or the safety and soundness of the financial institution in Singapore. Financial institutions therefore will have to consider whether any data breach amounts to a material adverse development that needs to be notified to the MAS. Factors that would be relevant in making such assessment include whether customer data is involved, the number of individuals affected, the nature and sensitivity of the data that has been compromised, and reputational risk.

(b) Where a financial institution has entered into any outsourcing arrangement, the financial institution is required to notify the MAS as soon as possible of any adverse development arising from its outsourcing arrangements that could impact the institution, including any event that could potentially lead to prolonged service failure or disruption in the outsourcing arrangement, or any breach of security and confidentiality of the institution's customer information.[45] As such, where any data breach is due to the acts or omissions of an outsourced service provider or otherwise involves an outsourced service provider, the data breach may have to be notified to the MAS.

(c) Financial institutions are required[46] to notify the MAS within an hour of a system malfunction[47] or information technology ("IT")

45 Monetary Authority of Singapore, *Guidelines on Outsourcing* (revised 5 October 2018) at para 4.2.1.

46 See the Monetary Authority of Singapore notices on technology risk management.

47 "System malfunction" is defined in the Monetary Authority of Singapore ("MAS") notices on technology risk management to mean a failure of any of the financial institution's critical systems. Financial institutions are separately required under the MAS notices on technology risk management to put in place a framework and process to identify "critical systems", *ie*, a system, the failure of which will cause significant disruption to the operations of the financial institution or materially impact the financial institution's service to its customers, such as a system which processes transactions that are time critical or provides essential services to customers.

security incident,[48] which has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers. A root cause and impact analysis report[49] must also be submitted to the MAS within 14 days from the discovery of the incident. Where a data breach involves a system malfunction or IT security incident, and such breach has a severe and widespread or material impact, the MAS will have to be notified within an hour, and a root cause and impact analysis will have to be completed within 14 days.

(d) Financial institutions are required[50] to notify the MAS within five working days of the discovery of any suspicious activity or incident of fraud where such activities or incidents are material to the safety, soundness or reputation of the institution. Where the incident involves fraud, a police report should also be lodged, and a copy of the police report needs to be submitted to the MAS. If the financial institution does not lodge a police report, it will need to explain to the MAS the reasons for not lodging the police report. In light of this, where a data breach is due to a fraudulent act of an employee, fraud by third parties against the financial institution or otherwise involves an element of fraud, the financial institution will have to make the

48 "IT security incident" is defined in the Monetary Authority of Singapore notices on technology risk management to mean an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on, a critical system, or a system which compromises the security, integrity or confidentiality of customer information.

49 The report is required to contain:

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the financial institution's:

(i) compliance with laws and regulations applicable to the financial institution;

(ii) operations; and

(iii) service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

50 See the Monetary Authority of Singapore notices on reporting of suspicious activities and incidents of fraud.

prescribed incident report within five working days and consider whether there is a need to at the same time file a police report.

23 Whilst the two regimes operate in parallel, it can be observed that there are some broad similarities in financial regulatory reporting requirements to the data breach notification obligations under the PDPA, for example: (a) the requirement to perform assessments for notification, in particular, the assessment of whether a data breach amounts to a "material adverse development" notifiable to MAS and the assessment of whether the data breach is a "notifiable data breach"; and (b) the imposition of prescribed timelines for notification by the regulatory authority.

B. Practical steps for financial institutions

24 Financial institutions should ensure that their data breach management plans take into consideration regulatory reporting obligations to the MAS. Where the MAS regulatory reporting requirements are the subject of policies and processes that are independent of the data breach management plan (*eg*, a separate cyber incident response and management plan),[51] the financial institution will have to ensure that the various processes are integrated and function smoothly, and that reporting and notifications made to the different regulators are consistent, and in accordance with the relevant timelines.

25 Financial institutions should also actively assess existing systems, processes or controls, and consider whether to make enhancements and upgrades to reduce the risk of data breaches; this exercise should be conducted in conjunction with the financial institution's Protection Obligation under the PDPA.[52] Note that the MAS has been increasing its focus on the technology risks faced by financial institutions in light of the increasing digitalisation of the financial sector and in 2019, the MAS

---

51 Monetary Authority of Singapore, *Technology Risk Management Guidelines* (January 2021) at para 12.3.

52 Pursuant to s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012), an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored.

introduced notices on cyber hygiene, to prescribe a minimum set of essential cyber-hygiene practices that financial institutions must put in place. The MAS also updated its *Technology Risk Management Guidelines* in January 2021, and one of the critical reasons for the update was to give greater focus to cyber resilience. The MAS has also proposed to increase the maximum quantum of the fine that can be imposed on financial institutions for breaches of technology risk-related requirements, to signal the importance of technology risk management.[53]

IV. Case study 2: Employees

A. Common scenarios where data breach is caused by employee

26 Data breaches may arise due to the actions (or inaction) of employees. Common scenarios include:

(a) *employee error*, *eg*, where an employee erroneously inserts individual customers' e-mail addresses into the "To" field in a promotional e-mail, thereby making all e-mail addresses visible to all recipients of the e-mail;

(b) *employee negligence*, *eg*, where an employee unsuspectingly clicks on a phishing e-mail, thereby allowing a cyber-attacker to harvest the employee's user credentials and gain access to the employer's database, which may or may not subsequently result in the extraction of personal data;

(c) *omission*, *eg*, where an employee fails to install or belatedly installs software security patches, leaving gaps in the employer's system where hackers may exploit; where a departing employee fails to return or properly dispose of proprietary information (including documents containing personal data) belonging to the employer; or where an employee fails to change the default auto-fill settings of a web browser;[54] and

(d) *malicious acts*, *eg*, where an employee deliberately leaks personal details stolen from the employer's database.

---

53 See Monetary Authority of Singapore, *Consultation Paper on a New Omnibus Act for the Financial Sector* (P002-2020, 21 July 2020) at para 4.4.

54 *Re Full House Communications Pte Ltd* [2017] PDP Digest 62.

B. Practical steps for employers

27 Section 53(1) of the PDPA provides that any act done or conduct engaged in by an employee in the course of his employment shall be treated as done or engaged in by the employer, *whether or not it was done with the employer's knowledge or approval*. However, where the breach is the result of an errant employee, an employer has a defence in s 53(2) of the PDPA if the employer can prove that steps as were practicable were taken to prevent the act done or conduct engaged in.

28 As employers may be liable for data breaches caused by their employees' acts, it is pertinent for employers to take steps to eliminate or minimise such acts.

(1) Imposing suitable contractual obligations on employees

29 As a data breach could occur at any time, employers should ensure that a comprehensive contractual framework is in place, from the inception of the employer–employee relationship.

30 This would include having express terms in the employee's contract of employment in relation to data use and protection that require the employee to:

> (a) comply with policies and guidelines issued by the employer (*eg*, in relation to data use and protection) as well as any relevant regulatory body (*eg*, the PDPC), and undertake not to make improper use of information acquired in the course of employment;
> (b) immediately return and not retain all property (including documents containing personal data) to the employer upon termination of the employee's employment; and
> (c) acknowledge that the employer is permitted to collect, process, use and/or disclose data (including personal data) relating to the employee for specified purposes, including monitoring the employee's Internet access and use of the employer's computer network, and to facilitate internal or external investigations.

(2) Employee training and awareness

31 Employers ought to develop and implement written policies and good cyber-hygiene practices which are PDPA-compliant and, as part of their

obligations under s 12 of the PDPA, communicate such policies and practices to their employees. Written policies should be readily accessible by employees; for instance, uploaded on the organisation's intranet, or incorporated as part of the employee handbook.

32 To maximise employee awareness, training on personal data collection, use, disclosure and protection should be conducted:

(a) for new employees, as part of the on-boarding process; and

(b) for all employees, when there are new data protection policies or processes (*eg*, following legislative amendments to the PDPA or the issuance of new guidance from the PDPC). Refresher courses should also be conducted regularly.

(3) Data breach management plan

33 As part of the organisation's data breach management plan, employees should be mandated to report *all* suspected or confirmed data breaches *immediately* to the organisation's data management team which has expertise in handling personal data and data breaches.

C. Specific employment-law issues arising from a data breach

34 Employers should review their internal investigation and disciplinary policies to assess that:

(a) there is a framework for investigations to be completed within a prescribed time frame, to ensure compliance with the fairly short statutorily prescribed time frames for assessment and notification of a data breach; and

(b) there is adequate guidance on the disciplinary action to be meted out to employees involved in the data breach.

35 An employee who is aware of and fails to report a suspected or confirmed data breach in a timely manner may be in contravention of the employer's policy on managing data breaches and may be liable to disciplinary action by the employer.

(1) Disciplinary action

36 The types and range of disciplinary action against employees who caused and/or were involved in the data breach would be determined by the employer's internal disciplinary policy. These may include one or a combination of the following: corrective/remedial training, written warnings, re-deployment or modification of duties and responsibilities, demotion, financial penalties, suspension and/or termination.

(2) Summary dismissal

37 In instances where the harm (whether actual or potential) arising from the data breach is severe and/or the culpability of the employee is high (*eg*, wilful or deliberate breach), it would be open to the employer to summarily dismiss the employee (*ie*, to terminate the employment contract immediately, without notice or payment in lieu of notice). Whether an employee's acts justify summary dismissal would depend on the facts of each case viewed in light of the circumstances.

(3) Loss to employer

38 If the data breach results in actual financial loss, an employer may commence a civil claim against the employee for breaches of the employee's obligations, *eg*, breaches of the data protection policy or failure to perform duties with reasonable skill, care and diligence. The employer would have to demonstrate that the employee's breaches of obligations caused the loss and quantify the extent of loss suffered as a result of the employee's breaches.

(4) Person who caused breach no longer in employ when breach is discovered

39 When a data breach is discovered and the person(s) who caused the breach is no longer employed in the organisation, it is likely to be more challenging to investigate the data breach, especially in the absence of other objective evidence (*eg*, computer access logs).

40 Unlike existing employees who are obliged to comply with the employer's lawful directions, an employer cannot compel an ex-employee to assist in its internal investigations. Nevertheless, it remains open to the

employer to invite the ex-employee to voluntarily co-operate in its internal investigations.

V. Concluding thoughts

41 Data breaches may arise in unexpected ways and at unexpected times. Responding to a data breach is a time-sensitive endeavour and requires organisations to mobilise resources swiftly and effectively to investigate the incident(s), contain the breach, assess the potential impact of the breach, and notify relevant regulatory authorities and affected individuals (where necessary). It would therefore be prudent for organisations to put in place clear policies, procedures and plans on managing data breaches and to provide adequate training to employees *before* any data breach occurs, so that organisations can respond to data breaches or suspected breaches in an organised and timely manner to minimise legal and regulatory risks.

EFFECTING VOLUNTARY STATUTORY UNDERTAKINGS IN SINGAPORE – REMEDIATION RATHER THAN REPRIMAND*

Bryan TAN†
LLB (National University of Singapore),
Advocate and Solicitor (Singapore); Solicitor (England & Wales)

I. Introduction and background

1 The voluntary statutory undertaking ("VSU") regime in Singapore is relatively young, with the Personal Data Protection Commission ("PDPC") publishing the first accepted undertaking on 10 September 2020 by Grabcar Pte Ltd,[1] pursuant to s 29 of the Personal Data Protection Act 2012[2] ("PDPA") before it was repealed on 1 February 2021. Section 29 is a general provision that empowers the PDPC to give organisations directions to comply with the PDPA, such as to stop collection, use or disclosure of personal data in contravention of the PDPC:

> **Power to give directions (repealed)**
> **29.**—(1) The Commission may, if it is satisfied that an organisation is not complying with any provision in Parts III to VI, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision.
> (2) Without prejudice to the generality of subsection (1), the Commission may, if it thinks fit in the circumstances to ensure compliance with Parts III to VI, give the organisation all or any of the following directions:
> (*a*) to stop collecting, using or disclosing personal data in contravention of this Act;
> (*b*) to destroy personal data collected in contravention of this Act;

* The author acknowledges the assistance of Mr Goh Eng Han in writing this article. Any views expressed in this article are the author's personal views only and should not be taken to represent the views of his employer. All errors remain the author's own.

† Partner, Pinsent Masons MPillay LLP.

1 Personal Data Protection Commission, "Undertaking by Grabcar Pte Ltd" <https://www.pdpc.gov.sg/Undertakings/Undertaking-by-Grabcar-Pte-Ltd> (accessed December 2021).

2 Act 26 of 2012.

(*c*) to comply with any direction of the Commission under section 28(2);

(*d*) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

Directions the PDPC can give under s 29 include requesting an undertaking from organisations to cease contravention of the PDPC. Although s 29 did not explicitly provide for a VSU regime, the PDPC had already described the regime as early as 2019, when it published the *Guide on Active Enforcement*[3] ("the Guide") with a section dedicated to VSUs.

2 Since the PDPC published the first three undertakings in 2020, it has already published 11 undertakings in 2021 to date. The increasing detection and reporting of potential breaches, as well as the risks arising from the large amount of personal data firms collect from consumers in their operations, exposes a gap that a more robust VSU regime can fill. Section 48L of the PDPA, introduced in 2021,[4] goes some way to address the gap between practice (as reflected in the Guide) and legislation. It explicitly sets out the VSU regime as an avenue where the PDPC and an organisation or person can work together to achieve PDPA compliance:

> **Voluntary undertakings (Date of Commencement 1 February 2021)**
> **48L.**—(1) Without affecting sections 48I, 48J(1) and 50(1), where the Commission has reasonable grounds to believe that —
>
> (*a*) an organisation has not complied, is not complying or is likely not to comply with any provision of Part III, IV, V, VI, VIA or VIB; or
>
> (*b*) a person has not complied, is not complying or is likely not to comply with any provision of Part IX or section 48B(1),
>
> the organisation or person concerned may give, and the Commission may accept, a written voluntary undertaking.
>
> (2) Without limiting the matters to which the voluntary undertaking may relate, the voluntary undertaking may include any of the following undertakings by the organisation or person concerned:

---

3 Revised 15 March 2021. See Baker McKenzie Wong & Leow, "Client Alert: PDPC Guide on Active Enforcement Released" (June 2019) <https://www.bakermckenzie.com/en/insight/publications/2019/06/-/media/files/insight/publications/2019/06/clientalertpdpcguideonactiveenforcementju.pdf> (accessed December 2021).

4 Section 48L of the Personal Data Protection Act 2012 (Act 26 of 2012) commenced on 1 Feb 2021.

(*a*) an undertaking to take specified action within a specified time;
(*b*) an undertaking to refrain from taking specified action;
(*c*) an undertaking to publicise the voluntary undertaking.

Section 48L lists in detail the undertakings an organisation or person may take under the VSU regime. They include taking specified action within a specified time, refraining from taking specified action and agreeing to the publishing of the VSU.

II. Voluntary statutory undertaking regimes in the UK and Australia

3 The UK and Australia also have comparable VSU regimes in their personal data protection legislation.

4 In the UK, the Data Protection Act 2018[5] ("DPA") is the UK's implementation of the General Data Protection Regulation[6] ("GDPR"). Previously, under the Data Protection Act 1998,[7] the UK Information Commissioner's Office ("ICO") could issue undertakings to commit organisations to particular courses of actions to improve compliance in lieu of the ICO exercising its enforcement powers under s 40 of the Data Protection Act 1998. Now, the ICO's power to issue undertakings arises from s 115 of the DPA, which confers powers detailed in Art 58 of the GDPR including ordering an organisation to bring processing operations into compliance and advising organisations through consultations like those for codes of conduct. In practice, the undertakings are similar to those issued by the PDPC. They detail the areas of potential breach and specific actions to be taken by organisations to remedy the shortcomings. Depending on the nature of the breach, the background section of the undertaking can be substantially detailed, such as that of Google Inc in 2014.[8]

---

5 c 12.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

7 c 29.

8 Information Commissioner's Office, *Data Protection Act 1998: Undertaking (Google Inc)* (ICO Ref: ENF0492064) (30 January 2015).

5 Under the DPA, organisations can also voluntarily enter other instruments like codes of conduct, with ICO's advice and guidance. If the code of conduct is approved, the organisation's compliance with the code will be monitored by an approved monitoring body and the code will be added to a public register of approved codes of conduct.[9] The use of VSUs appears to be less common in the UK relative to the number of other enforcement actions like fines. This could be because of the larger number of precedents and alternatives available, such as entering into a code of conduct before breaches occur, so organisations are more often expected to be compliant or face immediate enforcement otherwise.

6 In Australia, the Privacy Act 1988 ("Privacy Act") is the statutory basis for personal data protection. The VSU regime in Australia arises from s 114 of the Regulatory Powers (Standard Provisions) Act 2014 and s 80V of the Privacy Act, which allow the Australian Information Commissioner ("the Commissioner") to accept written undertakings from organisations to take or refrain from specified actions so that they comply with the Privacy Act. If the personal data breach involves certain health records, the VSU regime falls under the My Health Records Act 2012 or Personally Controlled Electronic Health Records Act 2012, which adopts a more detailed framework for accepting and enforcing undertakings. In practice, the undertakings are similar to those issued by the PDPC. They detail the areas of potential breach and specific actions to be taken by organisations to remedy the shortcomings.[10] For example, Wilson Asset Management did not take reasonable steps to notify individuals of the collection and use of their personal data. In its undertaking, Wilson Asset Management committed to cease further access, collection and disclosure of the data, and to destroy the data.

7 The Australian VSU regime for data protection differs from the PDPA in the monitoring of undertakings. The Australian VSU regime uses a more stringent monitoring process, requiring an independent expert that

9 Information Commissioner's Office, "Codes of Conduct" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/> (accessed December 2021).

10 Office of the Australian Information Commissioner, "Enforceable Undertakings" <https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/> (accessed December 2021).

will report to the Commissioner on organisations' compliance with their undertakings. The organisation involved must also prepare a detailed work plan for the independent expert's confirmation. This work plan serves to further detail the remedial steps mentioned in the undertaking, and in practice gives organisations a bit more time to prepare a full plan. In contrast, Singapore organisations and persons must submit a remedial plan (albeit less detailed) already during the VSU application.[11] After the VSU is accepted, an implementation plan must be submitted to the PDPC. Monitoring is less stringent with only a status update required, compared to independent reporting required by the Australian regime.

8 Perhaps because the Australian VSU regime is more meticulous in monitoring, it is used less often than in Singapore. While the PDPC has published three undertakings in 2020 and 11 in 2021 so far, the Commissioner has published about two undertakings a year since 2015. It remains to be seen if the PDPC will move towards a more selective process of accepting only a few VSUs a year, after it has accumulated experience in publishing a variety of undertakings setting precedents for various industries and types of personal data breaches.

9 In addition to data protection, Australia also implements a VSU regime in the finance industry and for consumer protection. Finance industry firms can submit undertakings to the Australian Securities and Investments Commission, which are then enforceable by the courts. Similar to the PDPC, the objective is to achieve swift and better outcomes compared to other enforcement options. The framework in assessing enforcement outcomes before accepting VSUs is arguably more rigorous.[12] VSUs to cease anti-competitive behaviour are like those in Singapore in that both are not pre-emptive. However, the Australian regime imposes a

11 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 17.

12 Australian Securities & Investments Commission, *Regulatory Guide 100: Enforceable Undertakings* (February 2015) at p 4.

more stringent audit for compliance,[13] while the Singapore regime does not detail any compliance audits.[14]

III. Voluntary statutory undertaking mechanics in section 48L of the Personal Data Protection Act

10 Although the PDPA has been amended substantially in terms of specifying the scope of VSUs, broadening the VSU regime's time range, applicability and flexibility, the regime is relatively unchanged in practical terms from when the first undertaking was published in 2020. This is because the Guide's outline of the VSU as well as its recommendations to organisations and persons have largely remained the same from 2019 to date. For example, the Grabcar Pte Ltd undertaking in 2020 is largely similar to the latest 2021 undertaking by Fujioh International Trading Pte Ltd.[15] The undertaking is structured in a similar fashion, specifying the actions the organisation has to take in remedying the breach, confirming that the undertaking will be published pursuant to the PDPA and agreeing to update the PDPC with information to confirm that the remediation is complete. The most observable difference is that the 2021 undertaking by Fujioh International Trading details the incidents and remedial steps in a separate table for greater detail and clarity. This has been the case since the undertaking of Manulife (Singapore) Pte Ltd was executed on 15 January 2021, by which time the amendments introducing s 48L had been passed by Parliament and would enter into force on 1 February 2021. Now, with the introduction of s 48L, the VSU framework has developed with more

13 Australian Competition & Consumer Commission, *Section 87B of the Competition and Consumer Act: Guidelines on the Use of Enforceable Undertakings* (April 2014).

14 Competition and Consumer Commission, "Operator of the Expedia Singapore Website Ceases False Claims on Validity Period of 'Daily Deals' Promotions", media release (12 November 2020); Competition and Consumer Commission, "ABC Bargain Centre, Valu$ and ABC Express Outlets to Cease 'Closing Down Sale' and 'Fire Sale' Advertisements", media release (16 October 2020).

15 Personal Data Protection Commission, "Undertaking by Fujioh International Trading Pte Ltd" <https://www.pdpc.gov.sg/Undertakings/Undertaking-by-Fujioh-International-Trading-Pte-Ltd> (accessed December 2021).

granularity, which organisations and persons can quickly grasp through the complementary guidelines and statutes and implement.

11 The PDPA also broadens the time range the PDPC can administer the VSU regime. Instead of first having to establish a PDPA breach, the PDPC can now initiate the VSU regime once it has reasonable grounds to believe that an organisation or person is likely not to comply with the PDPA, or once an organisation or person notifies the PDPC of a potential breach. That allows the PDPC to undertake more proactive monitoring of PDPA compliance, intervening before a personal data breach even occurs. This avoids the complexity of formal enforcement action, while protecting personal data pre-emptively. Such an outcome is arguably more desirable than activating PDPC and organisational resources on a full investigation, then imposing drastic penalties which do not undo the damage that has already been done. A full investigation would also take almost quadruple the time.[16] While prevention is better than cure, a cure is better than extracting a pound of flesh.

12 The PDPA also broadens the applicability of the VSU regime. Previously, the VSU regime only applied to organisations. Now, the VSU regime is also applicable to individuals that do not comply with the provisions regarding the Do Not Call Registry in Part IX of the PDPA. This addresses a common source of PDPA non-compliance that was not caught in s 29 previously, unifying the enforcement measures that the PDPA can utilise for breaches of different parts of the PDPA.

13 Most importantly, the PDPA gives the PDPC increased enforcement flexibility. As stated in the *Advisory Guidelines on Enforcement of the Data Protection Provisions*[17] ("the Guidelines"), the VSU regime provides a "window of opportunity" for organisations and persons to implement their remediation plans.[18] It also gives the PDPC discretion to determine (from the submitted remediation plans or otherwise) which organisations and persons have established, accountable processes and will be more likely to make good use of this "window" to rectify current personal data breaches.

---

16 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 31.

17 Revised 1 February 2021.

18 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (revised 1 February 2021) at para 25.3.

The enforcement flexibility could also encourage organisations and persons to be more forthcoming with the PDPC about their processes and discuss potential data protection risks faced, since they do not have to worry about the PDPC imposing sanctions without further discussion. A closer relationship between the PDPC and organisations and persons will promote transparency as well as encourage timely responses to any incidents, which is particularly relevant for personal data since the industry is fast-paced and a delay could severely increase the potential damage. A transparent, consultative regulatory environment will instil public confidence in the PDPC, which happens to also be one goal of PDPC enforcement actions.[19]

IV. Effect of voluntary statutory undertakings in Singapore

14 The PDPC decides whether to accept VSU applications from organisations and publish them accordingly on the PDPC website. Usually, the organisation's point of contact will be the PDPC's case officer who is assigned to investigate the data breach incident. The PDPC decides whether to approve the VSU application based on the details above submitted in the written declaration. In the process of reaching its decision, the PDPC may also work with the organisation to improve the remediation plan further before accepting it. The PDPC considers accepting an undertaking "if it assesses that a voluntary undertaking achieves a similar or better enforcement outcome more effectively and efficiently than a full investigation".[20]

15 The Guide also goes further to illustrate some scenarios where a VSU is unlikely to be accepted, such as when the organisation or person refutes responsibility for incidents, experiences a repeat of past breaches, does not explain how compliance will be achieved, requests for extended time to produce a remediation plan, and when the breach is wilful or egregious.[21] These scenarios will help organisations avoid common pitfalls when engaging the PDPC in VSU applications.

---

19 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 8.

20 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 17.

21 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 19.

A. When should voluntary statutory undertaking applications be submitted?

16 The organisation's request in writing for the VSU must be made early, either upon commencement of investigations or in the early stages. Often, the written request is submitted when an organisation reports to the PDPC a potential data breach that it discovered. Using the example of Platinum Yoga Pte Ltd, it first communicated with PDPC when submitting its data breach notification, before investigations commenced. Since time is of the essence, this allows for the PDPC and the organisation to work together to a mutually acceptable remediation plan. In this case, the PDPC was notified on 29 October 2020 and the undertaking executed within a few months on 20 January 2021. It also suggests that an organisation may prepare a VSU as part of its breach notification plan and then tweak it as appropriate when submitting the data breach notification.

17 If the organisation decides to withdraw its request for any reason before acceptance, the PDPC may proceed with a full investigation and any appropriate enforcement.[22]

B. How does the voluntary statutory undertaking apply after acceptance?

18 An accepted VSU does not amount to finding of a data breach.[23] Nevertheless, the PDPC will still publish the undertaking on its website, together with past undertakings. If the organisation has committed to publish its undertaking or any specific actions, it must still do so separately. As seen in the Platinum Yoga Pte Ltd undertaking, an organisation must follow up immediately on its remediation plan and complete it "in accordance to the stipulated timelines". It must also "provide information and documentation" to the PDPC to update on its progress and to allow the PDPC to verify that the organisation has complied with its undertaking.

---

22 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 19.

23 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at p 18.

19 If the PDPC determines that there is non-compliance, it reserves the right to resume investigations thereafter. The PDPC can pursue further enforcement action under s 50(3A) of the PDPA if the organisation does not comply with the terms of its undertaking. Section 48L(4) states that the PDPC may direct the organisation to ensure compliance with the undertaking, but at this stage, the PDPC will move quickly, as facilitated by s 48L(4)(*b*) which indicates that the 14-day timeline in s 48K(2) does not apply to directions given for VSU non-compliance.[24]

20 For now, the Guidelines and Guide do not offer much specific information for persons interested in the VSU regime. In fact, the Guide only refers to organisations even though persons have since been included in s 48L of the PDPA. Since there have yet to be any undertakings issued for persons, it remains to be seen if remediation plans have to be as detailed as organisations, and whether persons have to address any specific details for compliance with Do Not Call provisions compared to the other personal data provisions in the PDPA. Nevertheless, persons should proactively engage the PDPC in cases of potential personal data breaches, since the Guide explains that the PDPC will work together with organisations and persons to pinpoint areas of improvement for their submitted remediation plans. The consultation process will be mutually beneficial for both sides to quickly remedy potential personal data breaches rather than rely on punitive sanctions.

V. Conclusion

21 From the analysis above, the VSU regime has stayed relatively consistent in practice since its introduction and subsequent refinement. The undertakings are largely comparable and form a good pool of resources for organisations and persons to consult. The consistency and continuity are beneficial for organisations and persons because the expectations for personal data protection are clear, allowing them to develop the appropriate measures for risk mitigation. It will allow organisations and persons to also prepare VSU applications to the PDPC more quickly in the event of a personal data breach.

24 Personal Data Protection Act 2012 (Act 26 of 2012) ss 48K and 48L.

22 In conclusion, organisations and persons should be forthcoming in approaching the PDPC under the VSU regime. They should take reference from past undertakings and guidance issued by the PDPC in crafting their VSUs. They should also take care to abide by all parts of their VSUs so that personal data breaches are remedied, and no further enforcement action will be taken. Increasing accountability also helps organisations prepare and fulfil other obligations under the PDPA, such as the Data Breach Notification Obligation. While it is understandable that organisations encountering a data breach may wish to minimise regulatory action, the VSUs point to a trend that it is better to control the damaging effects of a data breach than to contest regulatory action. Ultimately, good practices are the best approach to protecting personal data because the consequences of a data breach can quickly escalate beyond what an organisation can remedy.

NAVIGATING CROSS-BORDER DATA TRANSFER LAWS IN 2021*

Charmian AW
LLB (National University of Singapore), FIP, CIPP/A, CIPP/E, CIPP/US, CIPM

Cynthia O'DONOGHUE
JD (University of California, Davis), LLM (University of Edinburgh)

Aselle IBRAIMOVA
Doctor iur (University of Bern), LLM (University of Nottingham), CIPP/E

Amy YIN
LLM (University of California, Berkeley)

Catherine JING
LLM (Erasmus University, Rotterdam)

1 It is the year 2021, and, as with many other things, COVID-19 has accelerated and amplified shifts in the landscape of international data transfers. A significant part of this has been driven by the market simply being forced to adapt to governments' and policymakers' responses worldwide to tackle the pandemic. Companies and organisations have had to digitalise across all manner of business and operations, in order to stay afloat – or, in some cases, thrive – amidst unprecedented changes impacting our physical world.

2 In this article, the authors discuss about Singapore's enhanced cross-border data transfer framework and highlight some key legal and regulatory developments in Europe and China that have had or are expected to have an impact on data exports and imports globally.

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

I. Singapore

A. *Singapore's policy position on cross-border data transfers*

3 The position in Singapore with regard to cross-border data transfers is consistent with its policy objectives to encourage growth of the country's digital economy.[1] This is borne out by the various mechanisms that organisations can avail themselves of to ensure that data is adequately and appropriately protected when transferring personal data from Singapore overseas. These mechanisms acknowledge that businesses have a legitimate need to allow data to flow across borders. They do not purport to hinder or block such data flows, but rather seek to allocate clear responsibility and accountability to protect individuals' data on organisations wanting to make the transfer.

B. *Complying with Singapore's personal data transfer laws*

4 The obligation to ensure data remains protected even as it is transferred outside of Singapore's borders is encapsulated in s 26 of the Personal Data Protection Act 2012[2] ("PDPA"). Subsection (1) requires a transferring organisation (or data exporter, a term which is commonly used in this context) to provide a standard of protection to personal data that is transferred from Singapore overseas which is "comparable" to the protection under the PDPA.

5 Under sub-s (2), the Personal Data Protection Commission ("the Commission") is empowered to exempt the data exporter from this requirement to any extent that it considers appropriate. The data exporter

1 See, for instance, Personal Data Protection Commission, *Public Consultation for Approaches to Managing Personal Data in the Digital Economy* (February 2018); Ministry of Communications and Information and Personal Data Protection Commission, *Public Consultation on Personal Data Protection (Amendment) Bill* (14 May 2020); Ministry of Communications and Information, Ministry of Trade and Industry and Info-comm Media Development Authority, "Singapore and Australia Sign Digital Economy Agreement", press release (6 August 2020); and Personal Data Protection Commission, "Memorandum of Understanding between OAIC and PDPC", press release (25 March 2020).

2 Act 26 of 2012.

needs to ensure that the data recipient/importer is bound by "legally enforceable obligations" to protect the data at a comparable standard to the PDPA. This will be taken to be satisfied in any of the following instances:

(a) First, the recipient is subject to any law, or other legally binding instrument, that offers a comparable standard of protection to the PDPA. Neither "law" nor "legally binding instrument" is specifically defined in the PDPA.[3] Accordingly, each term should be read in its plain literal meaning, such that "law" refers to any law, whether passed in Singapore or elsewhere, and "legally binding instrument" a binding contract, deed or other document that is recognised to be legally enforceable either in Singapore or elsewhere.

(b) Second, the transfer of personal data to the recipient is necessary for the personal data to be used or disclosed pursuant to one of the exceptions to consent specified in the PDPA. This is provided the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose.

(c) Third, the data importer: (i) as a data intermediary, is certified under the Asia-Pacific Economic Cooperation ("APEC") Privacy Recognition for Processors System ("PRP") or the APEC Cross Border Privacy Rules System ("CBPR"); or (ii) in any other case, is certified under the APEC CBPR, and such applicable certification is granted or recognised in its home country.

(d) Fourth, the individual is given a written summary of how his or her data will be protected to a standard comparable to the PDPA in the recipient country, and he or she consents to his or her data being transferred to the data importer in that country. Such consent must not have been unreasonably obtained,[4] or through deceptive or

3 Neither of these terms is defined in the Interpretation Act (Cap 1, 2002 Rev Ed) as well.

4 Specifically, the transferring organisation must not have required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual: Personal Data Protection Regulations 2021 (S 63/2021) reg 10(3)(*b*).

misleading practices.[5] In practice, very few organisations rely on this mechanism of consent, because individuals retain the right to withdraw their consent at any time. It may also be incommensurately time-consuming to have to provide written summaries of each recipient country's laws and how these are comparable with the PDPA.

(e) Fifth, the individual is deemed to have consented to the disclosure of his or her data to the recipient, pursuant to contractual necessity[6] under the PDPA. As the PDPA merely regards these as situations where there is consent by operation of law, the individual still has the right to withdraw consent subsequently.

(f) Sixth, the data is in transit, which means it merely passes through Singapore in the course of onward transmission without the data being disclosed, accessed or used in Singapore (save for the purpose of such transmission).

(g) Seventh, the data is publicly available in Singapore.

6 If none of the above applies, or if the data exporter does not want to rely solely on any of the above bases or derogations, then it must enter into an agreement to transfer personal data to an overseas recipient, as follows:

(a) In order to transfer personal data to a non-related third-party data importer, the data exporter must execute a legally binding contract that requires the importer to accord comparable protection to the transferred data as in the PDPA, and specify the countries to which the data will be transferred.

---

5 The transferring organisation must not have obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices: Personal Data Protection Regulations 2021 (S 63/2021) reg 10(3)(*c*).

6 Firstly, where the individual provides personal data to an organisation to enter into a contract with it; and secondly, where the disclosure of the individual's data by an organisation to another is reasonably necessary to: (a) perform a contract between the first organisation and the individual; or (b) conclude or perform a contract between the disclosing and recipient organisations entered into at the individual's request or which is reasonably in his or her interest. See ss 15(3)–15(8) of the Personal Data Protection Act 2012 (Act 26 of 2012).

(b) In order to transfer personal data to a data importer that is related to it, the data exporter must execute a set of binding corporate rules which require every data importer to accord comparable protection to the transferred data as in the PDPA, specify the countries to which the data will be transferred, and the rights and obligations of the parties.

C. Data intermediaries

7 In Singapore, any private sector organisation looking to transfer personal data from Singapore overseas needs to comply with the cross-border data transfer obligation under s 26 of the PDPA. However, where an organisation is a data intermediary, *ie*, merely processes personal data on behalf and for the purposes of another organisation pursuant to a written contract, that intermediary is *not* subject to the Transfer Limitation Obligation.[7]

8 The *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*[8] clarify that for overseas transfers of personal data, an organisation which engages a data intermediary retains responsibility for complying with the Cross-border Data Transfer Obligation in the PDPA. This is the case regardless of whether the data is transferred by: (a) that organisation *itself* to an overseas intermediary; or (b) a Singapore-based intermediary that is processing personal data on behalf and for the purposes of the organisation.

9 Ultimately, the onus is on the transferring organisation to undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure the latter is capable of protecting personal data transferred overseas to a standard that is comparable to that required under the PDPA. One way to do this would be to rely on the intermediaries' data protection policies and practices, including compliance with relevant industry standards and certification such as ISO 27001 and Tier 3 of the multi-tiered cloud security certification scheme.

---

7 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(2).

8 Revised 4 October 2021.

D. Cloud services

10 In relation to cloud services specifically, when an organisation engages a cloud provider to process personal data on its behalf and for its purposes under a written contract, that organisation must ensure that the cloud provider: (a) only transfers data to locations with comparable data protection regimes; or (b) has legally enforceable obligations to ensure a comparable standard of protection for the transferred data. This can be encapsulated by way of contractual provisions between the organisation and the cloud provider.

11 Where such contract is silent as to the locations to which a cloud provider may transfer data that is processed on behalf of an organisation, the organisation is deemed to have complied with the Transfer Limitation Obligation by ensuring that the cloud provider (a) is based in Singapore and is certified or meets relevant industry standards; and (b) provides assurances that all the data centres or sub-processors located overseas to which the data is transferred comply with these standards. To this end, an organisation may request the cloud provider to produce technical audit reports such as the Service Organization Control 2.

E. ASEAN model contractual clauses

12 On 22 January 2021, the ASEAN, of which Singapore is a member, adopted the *ASEAN Model Contractual Clauses for Cross Border Data Flows*.[9] These model contractual clauses were designed as a template cross-border transfer agreement that businesses transferring personal data to each other within ASEAN can use, with a view to reducing the compliance cost and time involved in negotiating such contracts, particularly for small and medium enterprises, whilst ensuring such data is sufficiently protected.

F. Takeaways

13 Companies that share data with any overseas entities, whether affiliates within a group or some external third party, should pay careful attention to complying with s 26 of the PDPA. In the PDPC's enforcement decision involving Singapore Technologies Engineering Limited ("ST

9 Final copy endorsed January 2021.

Engineering"),[10] the PDPC considered whether ST Engineering had satisfied the requirements of a data exporter under the PDPA. On the facts of the case, ST Engineering was found to not be in breach of s 26 because it had in place binding corporate rules ("BCRs") to govern international transfers of personal data within the group, and which were applicable to and legally binding on all of the company's direct and indirect subsidiaries worldwide. These BCRs also specified the countries to which personal data could be transferred, and laid out the rights and obligations of the relevant group entities who were parties to them, in accordance with the PDPA's requirements.

14 Where a company engages a data intermediary or cloud provider, it should review its contracts with such intermediary or provider. Among other things, such agreements should include appropriate provisions on the permissible use and transfer or personal data and the identification of overseas locations to which the data may conceivably be transferred, as well as provide assurances with regard to how the data will be protected, such as a right to audit, an industry standard or certification.

II. Key highlights on international data transfer developments in Europe and China

A. European Economic Area and the UK

(1) Standard contractual clauses

15 The European Commission approved three sets of model clauses for transfers of personal data from the European Union ("EU") to third countries under the previous Data Protection Directive.[11] Third countries are countries or territories that do not provide the equivalent protection as in the EU. The model clauses are also known as standard contractual clauses ("SCCs") and are to be used by controllers based in the EU. The

10 *Re Singapore Technologies Engineering Limited* [2020] SGPDPC 21.

11 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in 2001, 2004 and 2010.

SCCs contractually bind the recipients of the personal data originating from the EU to comply with EU-standard data protection obligations, thereby proving the appropriate safeguards enabling such transfers.

16 Recently, the adequacy of the SCCs was called into question. The Court of Justice of the European Union's ruling in *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*[12] ("*Schrems II*") confirmed that the SCCs remain to be an adequate safeguard when transferring personal data outside the EU to third countries and upheld its use, despite the same ruling invalidating the EU–US Privacy Shield Framework. Following this, the European Commission released the updated version of the SCCs on 4 June 2021. The final version incorporated public comments and feedback from its public consultation period in December 2020 on the draft SCCs released on 12 November 2020, as well as the joint European Data Protection Board[13] ("EDPB") and European Data Protection Supervisor[14] opinion[15] and opinions from representatives of the member states. These new SCCs became effective on 27 June 2021 and extended the coverage to transfers of personal data originating from the European Economic Area[16] ("EEA").

17 The new SCCs contain updates for the General Data Protection Regulation[17] ("GDPR") and will comprise four modules covering a wide range of possible data flows: controller-to-controller transfers (Module 1);

12 C-311/18, EU:C:2020:559.

13 The European Data Protection Board is composed of representatives of the European Union national data protection authorities and the European Data Protection Supervisor.

14 The European Data Protection Supervisor is an independent supervisory authority whose primary objective is to monitor and ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.

15 European Data Protection Board and European Data Protection Supervisor, *EDPB-EDPS Joint Opinion 1/2021 on Standard Contractual Clauses between Controllers and Processors* (14 January 2021)

16 The European Economic Area includes the European Union countries and Iceland, Liechtenstein and Norway.

17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

controller-to-processor transfers (Module 2); processor-to-processor transfers (Module 3); and processor-to-controller transfers (Module 4).

The European Commission released another version of the SCCs on 4 June 2021 for use between controllers and processors under Art 28 of the GDPR.[18] The discussion below will not focus on the Art 28 SCCs but on the SCCs covering international transfers only.

(2) Overview of the standard contractual clauses

(a) Modular approach

18 A modular approach has been adopted as one single entry-point to accommodate various transfer scenarios and to deal with the complexity of modern processing. The SCCs will hold itself as one agreement but will cover four data-sharing scenarios as separate "modules". These include controller-to-controller, controller-to-processor, processor-to-controller and processor-to-processor modules. This contains some general clauses applying to all the scenarios, and some tailored to each scenario.

19 Additionally, the European Commission has allowed for flexibility in its approach, as companies can add additional clauses or safeguards to the SCCs so long as they do not conflict with the SCCs or prejudice individuals' fundamental rights granted under the Charter of Fundamental Rights of the European Union[19] ("EU Charter of Fundamental Rights").

(b) Multiple parties

20 The updated SCCs make it possible for more than two parties to adhere to contract terms with SCCs. An optional "docking clause" allows additional controllers and processors to accede to the clauses throughout their term.

---

18 Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

19 2000/C 364/01 (2 October 2000).

(c) *Schrems II* influence

21 The SCCs include warranties that directly address the *Schrems II* decision, including a duty to conduct (and document) a data transfer assessment. This requires an assessment of the local laws and practices in the country of the data importer to ensure they do not affect compliance with the SCCs. Parties must warrant at the time of agreeing to the SCCs that "they have no reason to believe that the laws and practices applicable to the data importer" prevent compliance with the provisions of the SCCs.[20]

22 Further, the new SCCs add provisions on data protection safeguards and rights of redress resulting in the SCCs ensuring that any personal data transferred retains essentially equivalent protection to the GDPR. Individuals will have the right to be informed of the categories of data transfer, obtain a copy of the SCCs and receive information about any onward transfers of their personal data.

23 Moreover, the new SCCs extend the scope of notification obligations to cover requests by all public authorities whereas the previous SCCs were limited to requests by law enforcement authorities. The Notification Obligation also applies if the data importer becomes aware of any direct access to personal information by a public authority. On receipt of a government access request, the data importer must notify the data exporter promptly where it has received a data access request (and, where possible, the data subject) and challenge such requests if it "concludes that there are reasonable grounds to consider that the request is unlawful".[21] Data importers need to ensure the SCCs allow for effective legal remedies for data subjects. If such governmental request to access personal data is unlawful, data importers must seek interim measures not to disclose the personal data and prevent unlawful access to the data, and pursue legal remedies against such requests, including appeals.

---

20 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, cl 14(a).

21 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, cl 15.2(a).

(d) Timelines

24 From 27 September 2021 organisations can no longer continue to use the old SCCs for transfers outside the EU. All organisations that have used the old SCCs for their existing arrangements will have to substitute and repaper the old SCCs for the new SCCs by 27 December 2022. The newly issued SCCs will apply equally to private and public organisations that transfer data outside the EEA and can be used by controllers and processors located not only within the EEA but also outside of the EEA that are directly subject to the GDPR pursuant to the GDPR's extraterritorial jurisdiction under Arts 3(2)(a) and 3(2)(b) – namely, sales of goods or services to individuals located in the EEA or monitoring of behaviour of individuals located in the EEA.

(3) UK standard contractual clauses

25 A key development is that the new SCCs may not be valid for use by organisations located in the UK seeking to transfer personal data. When the UK exited the EU, it incorporated the GDPR into its own domestic law framework ("UK GDPR") together with the old SCCs.

26 As the new SCCs came into effect after the UK exited the EU, they cannot be used in the UK. The UK is still using the old SCCs, which need to be aligned with the GDPR and address *Schrems II* concerns, highlighting a gap in the domestic legislation. The Information Commissioner's Office ("ICO"), the data protection authority in the UK, issued a draft international data transfer agreement ("IDTA") to replace the old SCCs in summer 2021, together with a proposed guidance on international transfers and transfer risk assessments for a public consultation. The ICO has also issued an alternative to the IDTA in the form of an addendum to the new European Commission SCCs, which would be suitable for organisations that transfer data both from the EEA and the UK. The consultation closed in October 2021, and it is not yet clear as to when the draft documents will be finalised and enter into force.

(4) European Data Protection Board guidance: Final recommendations on supplementary measures

27 The *Schrems II* ruling placed an obligation on data exporters to assess the laws of a third country (*ie*, countries outside the EEA whose laws the

European Commission has not deemed as providing adequate protection) in which the data importer is located and whether such laws provide a level of protection that is essentially equivalent to that guaranteed under the GDPR. If such protections are not equivalent, data exporters must consider whether supplementary measures should be implemented to address any gaps in protecting personal data. These measures are mainly focused on technical measures to prevent unlawful access to personal data, such as encryption, pseudonymisation of data where the key is kept exclusively with the controller, splitting the processing between two or more independent processors to prevent reconstruction of data, and others. Supplementary measures also include contractual obligations (for example, for the data importer not to provide back doors or other processes to facilitate access to personal data on its systems) and organisational measures (for the data importer to adopt rules and policies on the handling of personal data originating from the EEA).

28 The EDPB adopted final recommendations on supplementary measures ("Recommendations") for data transfers to third countries.[22] The Recommendations contain a six-step methodology to assess transfers of personal data from the EEA to third countries.[23]

29 The six steps data exporters should take when determining whether supplementary measures must be put in place for a certain data transfer are set out below. Data exporters should:

> (a) know their transfers. This step helps determine whether the relevant data flows are subject to the rules of the GDPR on international transfers;
> (b) verify the transfer tool their transfer relies on, *eg*, the new EU SCCs, binding corporate rules, or other mechanisms;
> (c) assess if there is anything in the law or practice of the third country that may impinge the effectiveness of the transfer tool used;

22 European Data Protection Board, *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (Version 2.0, adopted 18 June 2021).

23 At the time of writing, countries deemed to provide adequate protection are: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, Uruguay and the UK.

(d) identify and adopt the necessary supplementary measures to the transfer tool to address the identified gaps to ensure the equivalent protection can be provided;

(e) take any formal procedural steps for the adoption of the necessary supplementary measures identified; and

(f) re-evaluate, at appropriate intervals, the level of protection of the data transfer.

30 The EDPB considers that legislation that "may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection" by not meeting EU standards on fundamental rights, necessity and proportionality and that does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society"[24] should be considered problematic in relation to cross-border transfers. Where there is problematic legislation, a data exporter may (a) suspend the transfer; (b) implement supplementary measures; or (c) proceed with the transfer without implementing supplementary measures as long as the problematic legislation does not apply in practice to the data transfer in question or the types of personal data concerned. To demonstrate accountability, data transfer assessments must be clearly documented in a detailed report.

31 If the problematic legislation applies to the personal data in question and, despite the supplementary measures considered, the transfer tool does not afford essentially equivalent protection to personal data, the EDPB advises that such transfers to the third country must be suspended or ended.

32 Additional aspects of the Recommendations which are worth noting are as follows:

(a) **Laws and practices**. In Step 3 of the supplementary measures, data exporters are advised to assess the surveillance laws in third countries, data exporters are permitted to take into account the practical experience of the data importer, such as previous requests for access to data from public authorities, governmental surveillance

24 European Data Protection Board, *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (Version 2.0, adopted 18 June 2021) at para 43.3, fn 50.

measures, the industry sector and whether problematic legislation applies to the specific personal data types due to be transferred.

(b) **Sources of information**. Organisations are able to use various sources when conducting an assessment as long as the sources are "relevant, objective, reliable, verifiable and publicly available or otherwise accessible".[25] This includes the ability to consider reports from private providers of business intelligence, transparency reports by international organisations and internal reports of the data importer on access requests from public authorities.

(c) **Duties**. The Recommendations emphasise that it is the obligation of both data exporters and data importers to ensure the level of protection set by the EU laws when data is transferred to third countries. To comply with the accountability principle under the GDPR, controllers or processors acting as data exporters must ensure that data importers collaborate with them in ensuring protection travels with the data and jointly monitor the measures taken are effective in achieving that aim.

33 Additionally, the EDPB confirmed that a data transfer is a processing operation in and of itself. Therefore, a data transfer will require a legal basis for processing under the GDPR. The Recommendations also emphasise that the GDPR derogations are meant to be used sparingly and remain an exception to the rule barring transfers of personal data from the EEA to third countries not otherwise deemed adequate.

34 While the Recommendations are not legally binding, they are likely to carry weight and reflect the common interpretation of the data protection supervisory authorities in the EEA. Of equal note is that there is a threshold level of risk contained in the Recommendations, which means that it is for data exporters and data importers of personal data to assess whether a transfer protects data in a manner equivalent to the GDPR.

---

25 As set out in European Data Protection Board, *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data* (Version 2.0, adopted 18 June 2021) Annex 3.

(5) Adequacy decisions

35 Article 44 of the GDPR prohibits the transfer of personal data to third countries unless appropriate transfer tools are used or the country or territory in question obtained an adequacy decision from the European Commission. If the European Commission deems a third country adequate, the personal data can be transferred to that country without any additional safeguards as a requirement. Presently, the European Commission have recognised all 30 EU/EEA countries and the 13 countries that have received EU adequacy decisions as adequate.

36 One of the newest members to join this list of adequate countries is the UK, following the European Commission's assessment of the UK's GDPR framework under the UK Data Protection Act 2018,[26] including data protection rules applicable to UK law enforcement and national security and surveillance. It concluded that the UK ensures an "essentially equivalent" level of protection to that within the EU, under the GDPR and Law Enforcement Directive,[27] meaning data transfers can flow from the EU to the UK without further safeguards. The European Commission adopted two adequacy decisions on 28 June 2021 for the UK, and these are effective immediately.

37 The UK adequacy decision includes a "sunset clause" following a four-year period, which could result in UK adequacy expiring on 28 June 2025, if not before. During this period, the European Commission will monitor the legal situation in the UK and may revisit the adequacy decision in relation to the UK should the UK deviate from its current level of data protection. If there is no deviation, in that UK legal protections remain essentially equivalent to the GDPR, then the adequacy decision should be renewed.

---

26 c 12.

27 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

B. China

(1) Overview of general personal data transfer rules in China

38 In China, legal rules on cross-border data transfer are widely scattered across many different laws, regulations and governmental standards, both at the central and local government levels. The key legal rules relevant to international data transfers so far include:

(a) Cybersecurity Law of the People's Republic of China[28] ("CSL"). The CSL is the first Chinese legislation governing all aspects of cybersecurity and protection of personal data and is currently regarded as the dominant legislation in the field of data protection.

(b) Data Security Law of the People's Republic of China[29] ("DSL"). The DSL is the first comprehensive data security legislation in China and aims to regulate a wide range of issues in relation to the collection, storage, processing, use, provision, transaction and publication of any kind of data; it has become a key supplement to the CSL.

(c) Personal Information Protection Law[30] ("PIPL"). The PIPL is China's "basic law" in the form of comprehensive legislation pertaining to personal data protection.

(d) Draft Measures on Security Assessment for Cross-border Transfer of Data[31] ("Draft Measures"). The Draft Measures are intended to provide detailed requirements and guidance to organisations in relation to data export activities.

(e) Draft Network Data Security Management Regulations[32] ("Draft Regulations"). Once finalised and adopted, the Draft Regulations will provide more detailed practical guidance on how to

28 Promulgated by the Standing Committee of the National People's Congress on 7 November 2016; effective as from 1 June 2017.

29 Promulgated by the Standing Committee of the National People's Congress on 10 June 2021; effective as from 1 September 2021.

30 Promulgated by the Standing Committee of the National People's Congress on 20 August 2021, effective as from 1 November 2021

31 Published by the Cyberspace Administration of China on 29 October 2021; the deadline for comments was 28 November 2021.

32 Published by the Cyberspace Administration of China on 14 November 2021; the deadline for comments was 13 December 2021.

implement the general legal requirements under national laws with a higher legal authority that have been adopted by the National People's Congress and its Standing Committee, such as the CSL, the DSL and the PIPL.

(f) Draft Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment[33] ("Draft Data Export Guidelines"). The Draft Data Export Guidelines contain very detailed procedures, key assessment points and identification guidance for data export activities.

39 The relevant Chinese government authorities are continuing to develop more detailed implementation rules and guidelines in this area, as well as to make supplementary provisions in respect of the above-mentioned legislation and regulations.

(2) Requirements under the Cybersecurity Law

40 The CSL provides that, in principle, critical information infrastructure ("CII") operators must store locally all personal data that is collected and generated in China, unless it can be proven that such data export is due to genuine business needs and a security assessment has been conducted and passed before carrying out the intended data export.

41 "CII" is defined under Art 31 of the CSL as "critical information infrastructure in important industries and sectors such as public communications and information services, energy, transportation, water resources, financial, public services and e-government, and other critical information infrastructure that, once damaged, disabled or subject to a data leak, may severely threaten national security, the national economy, people's livelihoods or the public interest" such as to warrant the State giving them extra protection in the form of a classified system.

33 Published by the National Information Security Standardization Technical Committee on 25 August 2017; the deadline for comments was 13 October 2017.

(3) Requirements under the Data Security Law

42 The DSL stipulates that any provision of data, stored in the People's Republic of China by a Chinese entity or individual, which is made in response to a request made by any foreign judicial body or law enforcement authority, will be subject to the prior approval of the competent authority. Violations could attract hefty fines of up to RMB5m for each company and RMB500,000 for the person in charge.

43 In addition, it is also provided under the DSL that certain data relating to China's national security, national interest, or its performance of international obligations may be deemed as controlled items and thus subject to export control.

(4) Requirements under the Personal Information Protection Law

44 In addition to CII operators, the PIPL will also subject "personal data processors" (a term that is similar to data controllers), whose processed personal data exceeds a prescribed amount to be decided by the competent authority, to the above-mentioned localisation and security assessment requirements In the meantime, the authors also noticed that the Draft Measures and the Draft Regulations both mention that the cross-border transfer of personal data by a personal data processor that has processed personal data of more than one million people will be subject to a security assessment organised by the Chinese authority. It remains to be seen how the "prescribed amount" will be specified in the final detailed implementation rules in this regard.

45 The PIPL also provides that general data processors may provide personal data to parties outside of the territory of China if they have legitimate needs to do so, and at least one of the following conditions is satisfied:

> (a) A security assessment organised by the Cyberspace Administration of China has been passed in accordance with China's laws and regulations.
>
> (b) A personal data protection certification has been conducted by a professional institute according to provisions issued by the Cyberspace Administration of China.

(c) A contract in the standard form formulated by the authority has been concluded with the overseas recipient, agreeing on both parties' rights and obligations.

(d) Any other conditions provided in China's laws or regulations are satisfied.

46 At the time of writing this article, the "contract in the standard form formulated by the authority" as mentioned above has not been published yet. It is expected that more details will be formulated in the near future.

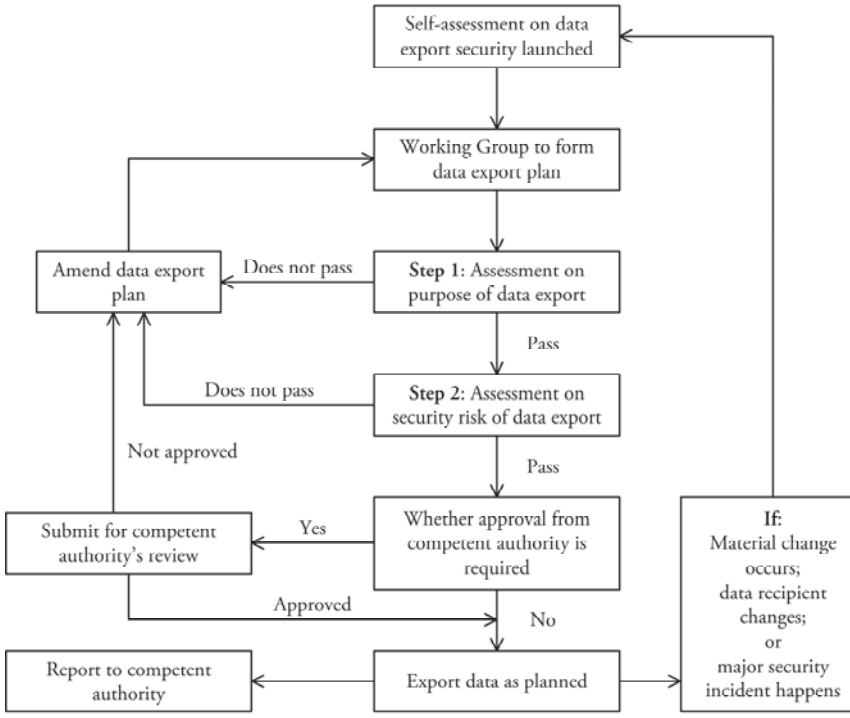
(5) Requirements under the Draft Data Export Guidelines

47 The Draft Data Export Guidelines specifically set out detailed factors to be considered and procedures to be followed from a good market practice perspective when conducting a security assessment in respect of personal data to be exported:

(a) **Designated working group**. According to the Draft Data Export Guidelines, each network operator in China may set up a working group for the self-assessment of data export security ("Working Group"). Such Working Group should consist of professionals in the fields of legal affairs, policy, security, technology and management. Self-assessment by the Working Group may be activated each time before a network operator intends to transfer personal data overseas.

(b) **Security assessments**. The Draft Data Export Guidelines also suggest that security assessments be conducted at least once a year in light of business development and network operations. In addition, another security assessment can be conducted promptly in case of any changes to the data recipient, any major changes to the purpose, scope, amount and categories of the data exported, or any major security incidents involving the data recipient or the data to be transferred.

The following chart depicts how the self-assessment procedure will apply:



48 In relation to Step 1 (assessment on purpose of data export) in the above chart, the Working Group must evaluate and ensure that the intended cross-border transfer of personal data and critical data meets the following three requirements:

(a) **Legality**. The intended data export is not prohibited by China's laws, regulations, and requirements imposed by relevant governmental authorities (such as authorities in charge of cybersecurity, public security and state security).

(b) **Justification**. Except for emergency circumstances that could endanger the life, property or safety of the person from whom the data is collected, such person's consent for the intended data export must be obtained beforehand.

(c) **Necessity**. The intended data export may be deemed to meet this requirement if it is essential for the network operator to (i) perform contracts; (ii) carry out internal business operations between entities within the same corporate group; (iii) realise treaties

or agreements entered into by China and other countries or regions, or international organisations; or (iv) conduct other activities that are essential to protect cyberspace sovereignty, state security, economic development, and public interest and rights.

49 In relation to Step 2 (assessment on security risk of data export) in the above chart, the Working Group must take into consideration the following key points:

(a) **Nature of exported data**. The categories and sensitivity, amount, scope of, and technical measures taken against the personal data and/or critical data intended to be exported may affect the result of assessment on security risk.

(b) **Sender's security capability**. The Working Group must assess the security capability of the sender of such exported data with whether or not (i) the security management system for data export has been in place; (ii) designated personnel has been appointed to deal with security management issues; (iii) contracts regarding data processing issues have been duly entered into by and between the sender and recipient; (iv) the audit mechanism for the effectiveness of its internal rules and procedures for data export has been established; (v) the emergency plan for security incidents has been formulated; (vi) complaint and tracking procedures have been set up; and (vii) the sender has been equipped with technical capabilities for security measures such as encryption transmission.

(c) **Recipient's security capability**. The factors to be assessed for the data sender are also applicable for the overseas data recipient. In addition, the Working Group must also assess the background of the recipient, such as its qualification and history of security incidents, if any.

(d) **Policy and legal environment**. The factors to be assessed include: (i) the applicable personal data protection laws, regulations and standards in the country or region where the recipient of the exported personal data is located; (ii) regional or international personal data protection organisations joined by such country or region, and binding commitments made by such country or region; and (iii) the implementation status of its personal data protection rules.

III. Concluding remarks

50 In summary, there have been significant developments to various key legal frameworks governing international data transfers. Amongst other things, these updates seek to address and regulate cross-border data flows in light of recent rapid technological advancements both within the country as well as in the global arena.

UTILITY OF A STRUCTURED FRAMEWORK IN ASSESSING FINANCIAL PENALTIES UNDER THE PERSONAL DATA PROTECTION ACT*

Kabir SINGH†
LLB (Hons) (National University of Singapore)

LOW Xide‡
MA (Oxon), BA (Jurisprudence) (University of Oxford)

John WU Bangguo§
LLB (Hons) (National University of Singapore)

I. Introduction

1 The Personal Data Protection (Amendment) Bill 2020[1] was passed on 2 November 2020 to fortify Singapore's data protection regime. Pursuant to the amendment, the maximum financial penalty imposable upon breaching organisations is to be raised to 10% of an organisation's annual turnover in Singapore or $1m, whichever is higher.[2] In addition, a list of factors distilled from the Personal Data Protection Commission's ("PDPC's") past advisory guidelines and enforcement decisions[3] was introduced into the Personal Data Protection Act 2012[4] ("PDPA") to guide

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer. All errors remain the authors' own.

† Partner, Clifford Chance, Singapore.

‡ Senior Associate, Clifford Chance Asia, Singapore.

§ Trainee Associate, Clifford Chance, Singapore.

1 Bill 37 of 2020, now the Personal Data Protection (Amendment) Act 2021 (Act 40 of 2021).

2 Personal Data Protection (Amendment) Bill 2020 (Bill 37 of 2020) cl 24(a).

3 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (21 April 2016) at paras 25.1–25.3; Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (revised 1 February 2021) at pp 38–42.

4 Act 26 of 2012.

the PDPC in assessing financial penalties.[5] While the increase in maximum financial penalty is scheduled to take effect at a later date, the existing advisory guidelines have been updated with reference to recently issued decisions to explain how enforcement decisions would take into account these factors.[6]

2 The penalty regime under the PDPA serves an important function in deterring data violations in Singapore, particularly given that the right of private action is rarely asserted in practice.[7] Accordingly, a clear, robust and fair penalty framework is essential to striking a balance between ensuring Singapore's competitiveness in the digital economy and to safeguard the personal data of individuals against misuse.

3 This article seeks to explore whether there is benefit in looking at other jurisdictions where more structured processes for calculating the quantum of penalties have been adopted. Accordingly, the article first undertakes a comparison between Singapore's approach in quantifying penalties and the approaches taken by the respective regulators in the UK, Germany and the Netherlands. Next, it sets out the potential advantages and disadvantages of adopting a prescriptive staged framework for quantifying penalties. Finally, it suggests the potential considerations in designing such a framework.

---

5 Personal Data Protection Act 2012 (Act 26 of 2012) s 48J(6); *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information): "the new section 48J details a list of factors that the PDPC will consider before imposing financial penalties". Such factors include the nature, gravity and duration of the violation, the type and nature of the personal data affected, and whether any mitigation actions were taken, *etc*.

6 See Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (revised 1 February 2021) at p 37 and Personal Data Protection Commission, *Guide on Active Enforcement* (revised 15 March 2021) at pp 28–30. These guidelines helpfully examine the application of each factor in the context of past enforcement decisions.

7 Personal Data Protection Act 2012 (Act 26 of 2012) s 48O; see *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 and *Bellingham, Alex v Reed, Michael* [2021] SGHC 125.

II. Assessing financial penalties for data breaches in Singapore

4 The PDPC adopts a fact-sensitive approach in calculating financial penalties.[8] In doing so, the PDPC will consider the list of aggravating and mitigating factors set out under s 48J(6) of the PDPA to ensure that the eventual penalty meted will be proportionate to the severity of the breach and serve as a sufficient deterrent against future non-compliance.[9] These factors range from, amongst others, the nature, gravity and duration of non-compliance, the type and nature of personal data affected, to the impact of the imposition of the financial penalty on the organisation.

5 Despite being decided before the recent amendments to the PDPA, the PDPC's decision in *Re Singapore Health Services Pte Ltd*[10] ("*Singapore Health Services*") is instructive. In *Singapore Health Services*, the PDPC explained that:[11]

> … in calculating the quantum of the financial penalty to be imposed, [it] takes an objective approach in assessing the facts and circumstances of the contravention and how a reasonable organisation or data intermediary should have behaved in the circumstances.

Accordingly, the PDPC proceeded to consider the aggravating and mitigating factors of the case. For example, the fact that sensitive personal data (*ie*, medical records) was compromised was an aggravating factor, and the organisation's co-operation during the investigation was a mitigating factor.[12] Notably, the factors taken into account are similar to those as set out under the current s 48J(6) of the PDPA.

---

8 Personal Data Protection Commission, *Guide on Active Enforcement of the Data Protection Provisions* (revised 1 February 2021) at p 28: "In calibrating the financial penalties, the PDPC considers the specific circumstances and the conduct of the organisation in each case."

9 Personal Data Protection Commission, *Guide on Active Enforcement of the Data Protection Provisions* (revised 1 February 2021) at p 29.

10 [2019] PDP Digest 376.

11 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [142].

12 *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376 at [142]–[144].

III. Comparative approaches: Assessing financial penalties in the UK, Germany and the Netherlands

6 The approach in Singapore differs from the approaches taken to assessing financial penalties in other jurisdictions. In this part, the authors set out the different approaches taken by regulators in the UK, Germany and the Netherlands.[13]

A. UK

(1) UK's current five-step framework

7 In the UK, the Information Commissioner's Office ("ICO") adopted a prescriptive five-stage framework in quantifying fines in its Regulatory Action Policy.[14] This five-stage framework was implemented in the ICO penalty notices involving British Airways ("BA")[15] and Marriott International ("Marriott")[16] and involves the following stages:

> (a) Stage 1: Determining if an "initial element" needs to be added to remove any financial gain arising from the breach.
> (b) Stage 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at ss 155(2)–155(4) of the UK Data Protection Act 2018[17] ("DPA") (similar to Art 83(2) of the General Data Protection Regulation[18] ("GDPR")).

13 See, for example, Art 83(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR") which requires the imposition of fines to be "effective, proportionate and dissuasive".

14 Information Commissioner's Office, *Regulatory Action Policy* at p 27.

15 Information Commissioner's Office, *Penalty Notice: British Airways plc* COM0783542 (16 October 2020).

16 Information Commissioner's Office, *Penalty Notice: Marriott International Inc* COM0804337 (30 October 2020).

17 c 12.

18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

(*continued on next page*)

(c) Stage 3: Adding in an element to reflect any aggravating factors.

(d) Stage 4: Adding in an amount for deterrent effect to others.

(e) Stage 5: Reducing the amount (save for the "initial element" at Stage 1) to reflect any mitigating factors, including ability to pay (*eg*, financial hardship).

8 Prior to the ICO's final decision to fine BA and Marriott some £20m and £18.4m respectively, both BA and Marriott challenged the ICO's initial decision regarding the quantum of the fines[19] on the basis that the Information Commissioner had unlawfully applied an unpublished draft internal procedure in setting the penalty, using turnover bands to supplement the stages set out in the Regulatory Action Policy.[20] The complaint was that the internal document pigeonholed organisations into different penalty "bands" based on their turnovers, and that such a "turnover-based approach" was lacking in basis.[21]

9 While the ICO acknowledged in its final decision that the draft internal document should not have been applied, it disagreed that a "turnover-based approach" was without basis.[22] Specifically, the ICO found

---

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

19 Information Commissioner's Office, "Intention to Fine British Airways £183.39m under GDPR for Data Breach" (8 July 2019); Information Commissioner's Office, "Statement: Intention to Fine Marriott International, Inc More Than £99 Million under GDPR for Data Breach" (9 July 2019).

20 Information Commissioner's Office, "Draft Internal Procedure for Setting and Issuing Monetary Penalty Notices" <https://ico.org.uk/media/about-the-ico/disclosure-log/2616196/irq0856908-disclosure.pdf> (accessed December 2021); Information Commissioner's Office, *Penalty Notice: British Airways plc* COM0783542 (16 October 2020) at paras 7.60–7.66; Information Commissioner's Office, *Penalty Notice: Marriott International Inc* COM0804337 (30 October 2020) at paras 7.61–7.68.

21 Information Commissioner's Office, "Draft Internal Procedure for Setting and Issuing Monetary Penalty Notices" <https://ico.org.uk/media/about-the-ico/disclosure-log/2616196/irq0856908-disclosure.pdf> (accessed December 2021); Information Commissioner's Office, *Penalty Notice: British Airways plc* COM0783542 (16 October 2020) at para 7.68.

22 Information Commissioner's Office, *Penalty Notice: British Airways plc* COM0783542 (16 October 2020) at para 7.71; Information Commissioner's

(*continued on next page*)

that it was justified to use a "turnover-based approach" because the GDPR expresses the maximum penalty in terms of a percentage of turnover.[23]

(2) UK's proposed nine-step framework

10 The ICO recently launched a public consultation on the adoption of a proposed prescriptive nine-stage framework in quantifying fines.[24] This nine-stage framework builds as follows:

> (a) **Stage 1: Assessment of seriousness of the breach**. First, the ICO will consider whether the higher maximum amount or the standard maximum amount is applicable to the breach.[25] Second, the considerations under Art 83(2) of the GDPR and s 155(3) of the DPA[26] would be applied.
>
> (b) **Stage 2: Assessment of degree of culpability of the organisation concerned**. The assessment of culpability accounts for measures

---

Office, *Penalty Notice: Marriott International Inc* COM0804337 (30 October 2020) at para 7.72.

23 Information Commissioner's Office, *Penalty Notice: British Airways plc* COM0783542 at para 7.71(a); Information Commissioner's Office, *Penalty Notice: Marriott International Inc* COM0804337 (30 October 2020) at para 7.72(a).

24 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at pp 19–24.

25 Unlike the Personal Data Protection Act 2012 (Act 26 of 2012), the GDPR adopts a two-tier fining regime where the maximum fine is determined by the specific provisions breached; minor infringements will incur a fine of up to €10,000,000 or 2% of total worldwide annual turnover for the preceding financial year, whichever is higher (Art 83(4) of the GDPR ("standard maximum amount" under s 157(6) of the UK Data Protection Act 2018 (c 12) ("DPA"))); and egregious infringements will incur a fine of up to €20,000,000 or 4% of total worldwide annual turnover for the preceding financial year, whichever is higher (Art 83(5) of the GDPR ("higher maximum amount" under s 157(5) of the DPA)).

26 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 21. The selected sections are ss 155(3)(a), 155(3)(c) and 155(3)(e)–155(3)(j) of the UK Data Protection Act 2018 (c 12).

implemented by the organisation to prevent the breach[27] and whether the breach was committed intentionally or negligently.[28]

(c) **Stage 3: Determination of turnover**. The ICO will review the organisation's accounts and obtain expert financial advice (if necessary) to determine the organisation's turnover.[29]

(d) **Stage 4: Calculation of appropriate starting point**. With reference to the seriousness of the breach (Stage 1) and the degree of culpability (Stage 2), the ICO will determine the relevant percentage for the calculation of baseline fine.[30] The ICO will then apply the relevant percentage to the turnover as determined at Stage 3.

(e) **Stage 5: Consideration of relevant aggravating and mitigating features**. The ICO will consider any other aggravating and mitigating factors applicable to the case and adjust the starting point in Stage 4 accordingly.[31]

(f) **Stage 6: Consideration of financial means**. The ICO will then consider the organisation's ability to pay and whether it would cause undue financial hardship.[32]

(g) **Stage 7: Assessment of economic impact**. The ICO must consider the desirability of promoting economic growth when exercising its regulatory functions and must ensure that it only takes regulatory action when needed.[33]

(h) **Stage 8: Assessment of effectiveness, proportionality and dissuasiveness**. The ICO must ensure that the amount of fine

27 Data Protection Act 2018 (c 12) (UK) s 155(3)(d).

28 Data Protection Act 2018 (c 12) (UK) s 155(3)(b).

29 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 22.

30 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 23.

31 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 23; Data Protection Act 2018 (c 12) (UK) s 155(3)(k).

32 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 24.

33 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 24; Deregulation Act 2015 (c 20) (UK) s 108(1).

proposed is effective, proportionate and dissuasive, and will adjust it accordingly.[34]

(i) **Stage 9: Early payment reduction**. The ICO will reduce the monetary penalty by 20% if it receives full payment of the monetary penalty within 28 calendar days of sending the notice. This discount is not applicable if the organisation decides to exercise its right of appeal.[35]

11 There are a few key differences between the ICO's current and proposed frameworks: first, the proposed framework expressly recognises turnover as a factor in quantifying fines; second, the proposed framework provides a clearer structure on how the baseline fine is calculated (*ie*, based on the severity of the breach, culpability of the organisation and the turnover of the organisation); and third, the proposed framework offers breaching organisations an early payment reduction if they pay the penalty promptly and do not appeal.

B. Germany

12 In Germany, the German Datenschutzkonferenz ("DSK")[36] published a five-stage framework for the calculation of fines under Art 83 of the GDPR in October 2019.[37] Under this framework, a fine will be calculated as follows:

---

34 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 24; Data Protection Act 2018 (c 12) (UK) s 155(3)(l).

35 Information Commissioner's Office, *Statutory Guidance on Our Regulatory Action* (1 October 2020) at p 24.

36 Unlike Singapore or the UK, where the Personal Data Protection Commission and the Information Commissioner's Office are the only competent supervisory bodies, Germany has 17 independent supervisory authorities – one for each of the 16 states – and the Federal Commissioner for Data Protection and Freedom of Information. The Datenschutzkonferenz (hereinafter "DSK") is the joint body of all German data protection authorities.

37 DSK's five-step framework is available at <https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf> (accessed December 2021) (only available in German).

(a) **Stage 1: The company is assigned to a class based on its size, as well as a subgroup relative to size class**. The organisation is assigned to one of four size classes (A to D) on the basis of its worldwide annual turnover for the previous year.[38] The organisation is then allocated to a subgroup within the size class.

(b) **Stage 2: The average annual turnover of the respective subgroup is determined**. This is according to a prescribed table.

(c) **Stage 3: The average daily turnover is then determined**. This is derived from the average annual turnover (Stage 2).

(d) **Stage 4: This value is then multiplied by a factor, the amount of which depends on the seriousness of the infringement**. The seriousness of the infringement is determined by whether the infringement is technical[39] or material,[40] and also whether it is classified as light, medium, serious or very serious depending on the circumstances of the case.

(e) **Stage 5: The amount is adjusted to reflect all circumstances of the individual case which have not yet been taken into account**: for example, the duration of the proceedings, or an imminent insolvency of the company.

13 This five-step framework is similar to the UK's proposed nine-step framework in that both rely on the breaching organisation's turnover when determining the baseline penalty figure. However, key differences still exist. For instance, while the UK approach takes into consideration the seriousness of the breach and culpability when calculating the baseline penalty figure, under the German approach, the baseline penalty figure only takes into consideration turnover.

---

38 Article 83 of the GDPR envisages that fines will be imposed on an "undertaking", and the DSK has noted that the definition of "undertaking" is the same as that in Competition Law (which is imported by Recital 150 of the GDPR). Hence, an "undertaking" consists of parent companies and subsidiaries, so that the total turnover of the group of companies would be used as the basis for calculating the fine.

39 Technical infringements are those listed in Art 83(4) of the GDPR for which fines are limited to 2% of the worldwide annual turnover for the preceding year or €10m.

40 Material infringements are those listed in Arts 83(5) and 83(6) of the GDPR for which the higher fines of up to 4% of worldwide annual turnover for the preceding year or €20m apply.

14 Notably, the above approach has been criticised by Germany's Bonn Regional Court in *1&1 Telecom GmbH v BfDI* ("*1&1 Telecom*") for being "problematic and contrary to the purpose of the fine under Article 83 paragraph 1 GDPR".[41] The court found that, while turnover is a factor for the assessment of fine, it should not assume centre stage and should give way to other fact-based considerations that are set out in Art 83(2) of the GDPR.[42]

C. *The Netherlands*

15 In the Netherlands, the Dutch Data Protection Authority, Autoriteit Persoonsgegevens ("AP"), published a framework on calculating administrative fines on 14 March 2019.[43] Under this framework, the AP classified data protection obligations under the GDPR into four categories: Category I (minor breach) to Category IV (serious breach).[44] For example, a breach of Art 9 of the GDPR, which protects special categories of personal data, is classified as a Category IV breach.[45] Each category sets a baseline fine and corresponding bands within which this amount can be altered.[46]

16 After determining the standard penalty, it would be adjusted with factors in Art 83(2) of the GDPR. While AP will usually stay within the appropriate band of fine, if the circumstances necessitate a higher or lower

41 The decision of *1&1 Telecom GmbH v BfDI* case no 29 OWi 1/20 LG can be retrieved from: <https://openjur.de/u/2310641.html> (accessed December 2021) (only available in German).

42 *1&1 Telecom GmbH v BfDI* case no 29 OWi 1/20 LG.

43 Autoriteit Persoonsgegevens's ("AP's") structured framework can be retrieved ("AP's Policy Paper") from: <https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf> (accessed December 2021) (only available in Dutch). See commentary in English: Wilfred Steenbruggen, Berend Van Der Eijk & Sonja van Harten, "Dutch Regulator Publishes Guidelines for the Calculation of Administrative Fines under the GDPR" *Bird & Bird* (April 2019).

44 See AP's Policy Paper at p 5 *ff*.

45 See AP's Policy Paper at p 6.

46 See AP's Policy Paper at p 1.

fine, then it would move to the next higher or lower category accordingly.[47] For example, in scenarios where the maximum fine in Category IV is deemed not dissuasive enough, AP can fine an amount higher than €1m and up to the maximum permitted by Art 83 of the GDPR. Unlike the UK's proposed nine-stage framework and Germany's five-stage framework, turnover of the organisation does not feature in the Dutch framework.

IV. Staged framework for calculating financial penalties?

17 The more highly detailed frameworks adopted by the UK, Germany and (to a lesser extent) the Netherlands present interesting alternatives to Singapore's present framework for calculating financial penalties for data breaches.

18 Proponents of having a staged framework may argue that it would provide greater clarity and guidance for organisations and individuals on the likely quantification of fines. In doing so, this may be said to promote transparency and fairness. Proponents may also argue that, from the regulator's perspective, having such a framework may serve to assist in increasing the consistency and finality of decisions issued by providing an analytical structure that can be consistently applied (and seen to be applied) across different decisions.

19 However, these advantages may be more muted in practice. For instance, the experiences of the UK and Germany cast doubt on whether having such prescriptive guidelines will in fact promote the finality and consistency of the regulator's decisions. The cases of BA, Marriott and 1&1 Telecomm, as highlighted above,[48] demonstrate that the application of a prescribed staged framework may not be straightforward and does not *ipso facto* mean that organisations will be less willing to initiate appeals.[49]

---

47 Wilfred Steenbruggen, Berend Van Der Eijk & Sonja van Harten, "Dutch Regulator Publishes Guidelines for the Calculation of Administrative Fines under the GDPR" *Bird & Bird* (April 2019).

48 See paras 8–9 and 14 above.

49 In fact, it has been observed that one takeaway from the British Airway and Marriott decisions is that "mounting a robust challenge to an ICO enforcement notice or notice of intent seems to be very worthwhile, especially when there is the risk of a substantial fine": see Anne Todd, "Lessons from the

(*continued on next page*)

20 The relative success of the appeals mounted in these cases may also suggest that supposed benefits such as clarity, transparency and fairness may be overstated – and that just having a prescribed stage framework is no guarantee that these principles would necessarily be served.

21 As Singapore becomes more of a technology hub, it is likely that the PDPC will have to contend with more complex and serious data violations, where the limits of the new maximum penalties may be explored. In those cases, there is likely to be more scrutiny of decisions that are issued, and challenges may become more common. To that end, it may be worth considering whether developing a more formal structured framework for determining financial penalties under the PDPA would be beneficial and in line with policy objectives.

V. Potential considerations in developing a staged framework

22 There are a multiplicity of considerations relevant to developing such a framework. In this part, the authors explore several such potential considerations.

A. Penalty guidelines issued by the Competition and Consumer Commission of Singapore

23 One potential consideration is the extent to which inspiration may be drawn from the penalty regime adopted by the Competition and Consumer Commission of Singapore ("CCCS") in dealing with competition law infringements. Notably, the penalty regime under the GDPR was also inspired by the system of fines in European competition law.[50]

ICO's Decisions to Reduce the BA and Marriott GDPR Fines" *Macfarlanes* (6 November 2020).

50 See Paul Nemitz, "Fines under the GDPR" (October 2018) at p 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3270535> (accessed December 2021). For example, Recital 150 of the GDPR makes explicit reference to Arts 101 and 102 of the Treaty on the Functioning of the European Union (25 March 1957; effective 1 January 1958), the key treaty provisions on competition law, for the definition of an "undertaking".

24 The CCCS's *Guidelines on the Appropriate Amount of Penalty in Competition Cases 2016*[51] ("Penalty Guidelines") includes the following steps:[52]

> (a) **Step 1: Calculation of base penalty**. The base penalty will be determined having regard to the seriousness of the infringement (expressed as a percentage rate) and the relevant turnover of the undertaking.
>
> (b) **Step 2: Adjustment for the duration of infringement**. The base penalty will be multiplied by the duration of the infringement.
>
> (c) **Step 3: Adjustment for aggravating and mitigating factors**. The financial penalty may be adjusted when there are aggravating factors or mitigating factors.
>
> (d) **Step 4: Adjustment for other relevant factors**. The financial penalty may be increased to achieve the objective of deterring infringing undertakings and other undertakings from engaging in anti-competitive practices.
>
> (e) **Step 5: Adjustment if the statutory maximum penalty is exceeded**. The financial penalty will be adjusted to ensure the statutory maximum is not exceeded.
>
> (f) **Step 6: Adjustment for immunity, leniency reductions and/or fast-track procedure discounts**.

25 The CCCS's Penalty Guidelines may serve as a useful starting point for the conceptualisation of a more structured framework for assessment of financial penalties under the PDPA.[53] For instance, having regard to the seriousness of the infringement *and* turnover as key factors in calculating a base penalty may be worthy of consideration as a first step in any such framework. Thereafter, other relevant aggravating and mitigating factors may be considered. The specific stage at which these factors are considered, including how the base penalty should be adjusted to take into account these factors, will depend on the policies underpinning such a framework: *eg*, whether to focus on conduct, culpability, deterrent effect, *etc*.

---

51 Effective 1 December 2016.

52 Competition and Consumer Commission of Singapore, *Guidelines on the Appropriate Amount of Penalty in Competition Cases 2016* (effective 1 December 2016) at paras 2.1–2.22.

53 Competition Act (Cap 50B, 2006 Rev Ed).

26 It bears noting that, not only do both penalty regimes have similar maximum fines based on the turnovers of organisations,[54] but they are also underpinned by fundamentally similar policy objectives – namely, to ensure that the financial penalty is proportionate to the seriousness of the infringement and serves as a sufficient deterrent to the breaching organisation.[55]

27 Further, as a matter of practice, a staged framework inspired by the CCCS's framework may be more easily understood and adopted by organisations which may already be familiar with the existing CCCS Penalty Guidelines.[56]

B. How should turnover of an organisation be taken into account?

28 Another key consideration is how the turnover of an organisation should be factored into any potential framework, including the stage at which turnover should be taken into account.

29 While the UK and Germany take into account an organisation's turnover in determining what the baseline penalty should be, the Netherlands has taken a different approach that is largely independent of an

---

54 Competition Act (Cap 50B, 2006 Rev Ed) s 69(4) – the financial penalty may not exceed 10% of the turnover of the business of the undertaking for each year of infringement up to a maximum of three years; Personal Data Protection (Amendment) Bill 2020 (Bill 37 of 2020) cl 24(a) – if the organisation whose annual turnover in Singapore exceeds S$10m, the financial penalty may not exceed 10% of the annual turnover in Singapore of the organisation.

55 Competition and Consumer Commission of Singapore, *Guidelines on the Appropriate Amount of Penalty in Competition Cases 2016* (effective 1 December 2016) at para 1.7 – the financial penalty should be proportionate to the seriousness of the infringement and sufficiently deterrent to the infringing organisation.

56 For example, the application of the six-step framework had been explored and applied by both the Competition and Consumer Commission of Singapore (*Acquisition of Uber's Southeast Asian Business by Grab and Uber's Acquisition of a 27.5 Per Cent Stake in Grab* 500/001/18 (24 September 2018) at paras 373–438) and the Competition Appeal Board (*Uber Singapore Technology Pte Ltd v Competition and Consumer Commission of Singapore* [2020] SGCAB 2 at [189]–[202]) for the case of the Grab–Uber merger.

organisation's turnover and focused on the severity of the violation. Even between the UK and Germany, there are differences. For instance, the UK's ICO also takes into account the seriousness of the breach and culpability of the organisation while determining the baseline penalty, whereas Germany's DSK merely looks at turnover to determine this, leaving factors such as seriousness of the breach to be considered at a later stage.

30 The stage at which turnover should be considered is more a question of optics – it can have significant impact on the actual quantum of the fines calculated. For instance, if turnover is used as the key factor to determine the baseline fine, then organisations with large turnovers may suffer as their baseline fine will be high even if the seriousness of the breach was low. While it may be possible for the baseline figure to be subsequently adjusted on account of other factors (such as culpability and/or the seriousness of the breach), these other factors will still need to dislodge what is in the first instance a significantly higher number. This was recognised by the German court in *1&1 Telecom GmbH*, where it criticised such an approach for potentially leading to disproportionately high fines against organisations with high turnovers that commit minor violations.[57]

31 How turnover is to be accounted for is also an important consideration. While the UK's ICO will look at the turnover of the specific breaching organisation, Germany's DSK would look at the average turnover of organisations falling within the same turnover category as the breaching organisation. These approaches can lead to significantly different results, depending on the size of the categories and where the breaching organisation falls within the specific category. These considerations and others will need to be taken into account in deciding which would be the right approach to adopt.

C. *How detailed should the framework be?*

32 The level of detail to be incorporated into the framework is another issue that merits consideration. In the authors' view, the certainty of

57 Susanne Werry, "German Court Slashes GDPR Fine in a Clear Rejection of Turnover Focused German Fine Model: Cuts Fine to Less Than 10% of the Original Amount" *Clifford Chance: Talking Tech* (8 February 2021).

providing a more detailed framework should not come at the expense of expediency and undermining other equally important policy objectives.

33 From a policy perspective, there is a trade-off between the level of detail and the adaptability of the framework. A highly detailed framework, which may potentially provide more certainty, may not be suited to dealing with novel or complex data incidents which may require a more flexible approach. On the flipside, it would also not be efficient or expedient to apply a detailed multi-stage framework to every case – many of which will involve smaller data incidents.

34 Further, an exhaustive framework allowing organisations to predict the costs of their breaches *ex ante* may encourage opportunistic behaviour whereby organisations internalise such issues as a worthwhile business risk instead of seeking to comply with the regulations. This may end up depriving fines of their deterrent effect. For example, the CCCS noted in Grab–Uber's enforcement decision that the two undertakings had structured a mechanism prior to the merger to apportion the eventual financial penalties and costs for any antitrust investigations.[58]

VI. Conclusion

35 The PDPC's current approach to calculating financial penalties involves consideration of, amongst others, the various factors set out in s 48J(6) of the PDPA (as further supplemented by the PDPC's advisory guidelines). While regulators in other jurisdictions have adopted more structured frameworks that detail how penalties should be calculated, it can be seen that these come with their own set of challenges and are consistently being refined. Given that the recent amendments to the PDPA provide for maximum penalties which may rise to 10% of an organisation's annual turnover, it may be sensible to consider whether it would be beneficial to adopt a similar framework in Singapore. If so, then it is hoped that the above considerations and lessons learned from other jurisdictions would be helpful in formulating such a framework.

---

58 *Acquisition of Uber's Southeast Asian Business by Grab and Uber's Acquisition of a 27.5 Per Cent Stake in Grab* 500/001/18 (24 September 2018) at para 378.

THE VITAL ROLE OF THE DATA PROTECTION OFFICER*

CHUA Ying-Hong
LLB (National University of Singapore),
LLM (University of Cambridge)

1 The data protection officer ("DPO") in any organisation plays a vital role in ensuring the organisation's compliance with the PDPA. It is surprising that, despite the Personal Data Protection Act 2012[1] ("PDPA") having been in effect since July 2014, the enforcement decisions issued by the Personal Data Protection Commission ("PDPC") in 2020 still included reports of organisations which had yet to appoint a DPO. This inevitably led to the organisations breaching other obligations under the PDPA, most notably, the requirement to develop and implement data protection policies and processes under s 12(*a*), and the Protection Obligation under s 24.

2 This article takes an in-depth look at the legal requirements for the appointment of a DPO and their underlying rationale, before exploring the DPO's roles and responsibilities. Finally, this article examines the key attributes and elements that are necessary for the DPO to effectively discharge his functions, namely, the right technical skills, due empowerment by senior management, autonomy in the discharge of his responsibilities and adequate resourcing. It is the author's hope that this article will serve as a useful point of reference for organisations as they establish or review their data protection programmes.

I. Appointing a data protection officer is mandatory under the Personal Data Protection Act

A. Legislative framework for the appointment of a data protection officer

3 Appointing a DPO is critical to an organisation's fulfilment of its obligations under the PDPA. So central is this requirement that it is set out

* Any views expressed in this article are the author's personal views only and should not be taken to represent those of her employer. All errors remain the author's own.

1 Act 26 of 2012.

in the PDPA immediately after the provision stating that an organisation is responsible for personal data in its possession or under its control.[2] Section 11(3) of the PDPA states that an organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA.

4 The language of s 11(3) allows flexibility. There is no requirement that the DPO be an employee. There is also no requirement that ensuring the organisation's compliance with the PDPA be the designated individual's sole function. It is therefore open to an organisation to designate an external service provider, or an employee who holds other concurrent job functions, as its DPO. Where necessary, the organisation may also designate multiple DPOs.

5 Further, s 11(4) of the PDPA allows the individual designated under sub-s (3) to delegate to another individual the responsibility conferred by that designation. Thus, an organisation can designate one employee as its DPO, with this employee delegating his responsibility to another employee or even an outsourced service provider. The PDPC recognises that organisations with manpower constraints may outsource operational aspects of the DPO function to a service provider, although the overall DPO function remains the management's responsibility.[3]

6 The above legislative framework is a commendable nod to organisations' commercial need for flexibility in complying with their PDPA obligations. Smaller organisations may prefer to engage an outsourced service provider with expertise in data protection, while larger organisations may appoint a senior employee as its DPO, with the day-to-day functions discharged by a supporting in-house team. Yet another permutation is to appoint an employee as the DPO, with support provided by an outsourced service provider.

---

2 Personal Data Protection Act 2012 (Act 26 of 2012) s 11(2).

3 Personal Data Protection Commission, "Data Protection Officers" <https://www.pdpc.gov.sg/Overview-of-PDPA/Data-Protection/Business-Owner/Data-Protection-Officers> (accessed 3 August 2021).

B. Failing to appoint a data protection officer readily leads to breaches of other obligations under the Personal Data Protection Act

7 Despite the central importance of appointing a DPO, and the flexibility allowed for the implementation of this obligation, there continue to be reports of organisations which have yet to appoint a DPO. Significantly, these organisations' failure to appoint a DPO have led or contributed to their breaches of other obligations under the PDPA.

8 This is evident from the PDPC's enforcement decisions in, for example, *Re Spize Concepts Pte Ltd*[4] ("*Spize*"), *Re AgcDesign Pte Ltd*,[5] *Re Majestic Debt Recovery Pte Ltd*[6] ("*Majestic*") and *Re Jigyasa*.[7] All four organisations were found to have breached their obligation under s 11(3) of the PDPA by failing to appoint a DPO. Unsurprisingly, they were also found not to have any data protection policies, thus breaching s 12 of the PDPA as well.[8]

9 In addition, Spize Concepts Pte Ltd ("Spize") was found to have breached its Protection Obligation under s 24 of the PDPA. A link on Spize's online portal had been made publicly accessible, such that the personal data of approximately 148 customers could be viewed by the public. Spize had outsourced the hosting, support and maintenance of its online ordering system to Novadine Inc ("Novadine"), and lacked knowledge of the security arrangements that were in place in the Novadine system to protect the personal data that was being processed on its behalf. In fact, Spize did not have any staff to manage the relationship between Spize and Novadine, and lacked records documenting Spize's arrangements with Novadine. It also did not have proper password or administrator account management policies.

10 Given that Spize did not have a DPO at the material time, such lapses were not unexpected. Had a DPO been appointed, at the minimum, he would have kept proper records documenting the security arrangements

---

4 [2020] PDP Digest 311.

5 [2020] PDP Digest 322.

6 [2020] SGPDPC 7.

7 [2020] SGPDPC 9.

8 See also *Re O2 Advertising Pte Ltd* [2020] PDP Digest 398; *Re Executive Link Services Pte Ltd* [2020] PDP Digest 381; *Re ChampionTutor Inc* [2020] PDP Digest 342; and *Re Horizon Fast Ferry Pte Ltd* [2020] PDP Digest 357.

with Novadine to protect the personal data that was being processed on Spize's behalf and would have been able to address the PDPC's queries on this. The DPO would also have put in place data protection policies and practices. Accountability is a fundamental principle underlying the PDPA. Not only must organisations ensure compliance with the PDPA; they must also be able to demonstrate such compliance. DPOs have a critical role to play in both respects.[9]

11 Interestingly, unlike organisations which had appointed DPOs as part of the suite of remedial measures undertaken voluntarily, Jigyasa was directed by the PDPC to appoint a DPO.[10] In its application for a reduced financial penalty, Jigyasa argued that, as it was a sole proprietorship with only one part-time employee, the sole proprietor had automatically assumed that she was also the DPO and therefore did not effect any formal appointment.[11] This argument was not accepted by the PDPC. The PDPC held that this submission may carry more weight in a scenario where the sole proprietor does not have any employees. However, in Jigyasa, the organisation had one employee. Since there were employees, the law made no assumptions as to who amongst them was the DPO. The PDPC also noted that organisations, including sole proprietors, may also appoint external professional DPOs with the requisite expertise and experience. A deliberate appointment is thus necessary.

12 Although Jigyasa's argument holds some superficial attraction, the PDPC's logic is incontrovertible. Apart from the uncertainty over who actually has conduct of the DPO role (is it the sole proprietor, her employee or an external service provider?), the act of appointing a DPO should also not be regarded as a mere formality. The act of appointment itself has value in reminding all stakeholders of the importance of this role, and the DPO himself of the responsibilities which come with the appointment. This is an important first step towards an organisational

---

9 In fact, in Canada's Personal Information Protection and Electronic Documents Act (SC 2000, c 5) ("PIPEDA"), the data protection officer's function is defined in terms of accountability. Principle 1 in Sch 1 requires an organisation to "designate an individual or individuals who are accountable for the organization's compliance" with the PIPEDA principles.

10 See *Re Jigyasa* [2020] SGPDPC 9 at [33(b)]. See also *Re O2 Advertising Pte Ltd* [2020] PDP Digest 398 and *Re Champion Tutor Inc* [2020] PDP Digest 342.

11 *Re Jigyasa* [2021] SGPDPCR 1 at [5(c)].

culture that values and prioritises data protection, which is ultimately the cornerstone of any successful data protection programme.

II. Role and responsibilities of a data protection officer

13 While the function of the DPO may seem obvious, there is utility in unpacking his role and responsibilities further, so as to better appreciate not only the breadth of his duties but also their significance. Broadly, the role and responsibilities of the DPO can be grouped into three categories, according to the stakeholder group involved. The first category relates to the organisation and internal stakeholders such as the organisation's employees and contractors. The second and third categories relate to external stakeholders, namely, the regulator (*ie*, the PDPC) and the organisation's data subjects, respectively.

A. The organisation and its employees and contractors

14 The DPO's first set of responsibilities relates to the organisation itself, and its employees and contractors. Section 12(*a*) of the PDPA requires every organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. This is the DPO's core role, namely, to develop and implement data protection policies and practices that are tailored to the operational needs of the organisation and appropriate for the volume and types of personal data in the possession or control of the organisation. The DPO must communicate these policies and processes to the employees and contractors of the organisation and train them to comply.

15 In *Re M Star Movers & Logistics Specialist Pte Ltd*[12] ("*M Star Movers*"), PDPC's deputy commissioner agreed with the position set out in the joint guidance note[13] issued, *inter alia*, by the Office of the Privacy

12 [2018] PDP Digest 259 at [35].

13 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* (April 2012).

Commissioner of Canada on the role and responsibilities of a DPO (or Privacy Officer in the Canadian context):[14]

> [T]he 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.

Further, as noted by the PDPC in its *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*[15] ("Advisory Guidelines"), apart from developing and implementing data protection policies and practices, the DPO may also produce a personal data inventory, conduct impact assessments, monitor and report risks, provide internal training, engage with stakeholders on data protection matters and generally act as the primary internal expert on data protection.[16] Depending on the organisation's needs, the DPO may also work with (or have additional responsibilities relating to) the organisation's data governance and cybersecurity functions, and support the organisation's innovation.

16 More generally, the DPO needs to build the data protection culture in the organisation. The organisation, and its employees and contractors, should come to see the DPO as a trusted partner in data protection, and should seek the DPO's advice in projects which may have a data protection impact. Senior management should look to the DPO to flag significant risks, and provide the DPO with the necessary support to ensure the organisation's PDPA compliance.

---

14 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* (April 2012) at p 7.

15 Revised 1 October 2021.

16 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 21.4.

B. The regulator

17 The DPO plays an important intermediary role between the organisation and the regulator, and functions as the liaison during any inquiry or investigation. While the DPO may not be able to act as the organisation's advocate in legal proceedings (given his role as an independent adviser),[17] he will nevertheless be an important source of information for the regulator.

18 Thus, many regulators either encourage or require organisations to notify them of their DPO. For example, Art 37(7) of the European Union's General Data Protection Regulation[18] ("GDPR") requires organisations to communicate their DPOs' information to the supervisory authority.[19] In Singapore, the PDPC encourages organisations to register their DPO's information through their Accounting and Corporate Regulatory Authority profile[20] or an online portal.

C. The data subjects

19 Finally, the DPO plays an important public-facing role, in being the first point of contact for data subjects. Section 11(5) of the PDPA specifically requires organisations to make available to the public the business contact information of at least one of its DPOs or individuals delegated with the DPO's responsibilities.[21] As stated in the Advisory

---

17 See Principle 8 of the Dutch Data Protection Authority's guidance on the role of the data protection officer: see Jeroen Terstegge, "Notes from the IAPP Europe, 2 July 2021" *IAPP* (1 July 2021). Note also the language of s 201(1)(c) of New Zealand's Privacy Act 2020 (2020 No 31) that a privacy officer's responsibilities include "working with" the Privacy Commissioner in relation to investigations under the Act.

18 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").

19 See also s 55(2) of South Africa's Protection of Personal Information Act, 2013 (Act No 4 of 2013).

20 Through the Bizfile eService.

21 Article 37(7) of the GDPR contains a similar requirement. See also ss 20(1)(*c*) and 20(5)(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012), which require an organisation to inform the individual of, on request by an

(*continued on next page*)

Guidelines, the business contact information should be readily accessible from Singapore and operational during Singapore business hours; telephone numbers should be Singapore telephone numbers.[22] This is to facilitate a prompt response by the organisation to any complaint or query by data subjects; for example, as to the organisation's policies and processes for data protection.[23] Access and correction requests must be made to the DPO,[24] and the DPO needs to develop procedures for handling such requests and complaints.[25]

III. Key attributes of an effective data protection officer

20 Appointing a suitably qualified DPO is an important first step in every organisation's data protection programme. However, this alone does not suffice. For a DPO to be effective and successful in ensuring the organisation's compliance with the PDPA, he must be not only empowered to discharge his responsibilities with independence but also appropriately resourced.

A. Technical knowledge and skills

21 The PDPA does not prescribe the technical knowledge and skills which DPOs are required to have, although the Advisory Guidelines state that the DPO should be "sufficiently skilled and knowledgeable".[26] In a similar vein, Art 37(5) of the GDPR states that the DPO shall be

---

individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of his personal data.

22 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 21.7.

23 See s 12(*d*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

24 Personal Data Protection Regulations 2021(S 63/2021) reg 3(2)(*b*).

25 See s 12(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

26 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) ("Advisory Guidelines") at para 21.5. The Advisory Guidelines cite, for example, the Practitioner Certificate for Personal Data Protection (Singapore) co-issued by the Personal Data Protection Commission ("PDPC") and the International Association for Privacy Professionals.

designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks set out in Art 39.

22 The level of expertise required of a DPO should be commensurate with the volume and sensitivity of the data in the organisation's possession or control. This calibrated approach is aligned with the general reasonableness standard enshrined in s 11(1) of the PDPA. Useful reference can also be made to the DPO Competency Framework and Training Roadmap[27] developed by the PDPC.

B. Empowerment

23 Data protection is a core part of managing enterprise risk. It is therefore important for the DPO to be able to directly apprise the board and senior management of key risks, and secure their continued support for the organisation's data protection policies and practices.

24 Thus, the DPO should ideally be part of the organisation's management team. As the PDPC's deputy commissioner stated in his keynote speech on 24 July 2017:[28]

> An organisation that wishes to be effectively accountable to its customers for the personal data that it holds has to begin the transformation from within. The direction and impetus must come from the top: the board of directors and the CEO. With strong management support, the DPO can be empowered to bring about the changes that are necessary. Ideally, he should be part of the management team because he has a mammoth challenge.

---

27 Personal Data Protection Commission, "DPO Competency Framework and Training Roadmap" <https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap> (accessed 3 August 2021).

28 Yeong Zee Kin, Deputy Commissioner, Personal Data Protection Commission, keynote speech at the IAPP Asia Privacy Forum (24 July 2017). See also Hong Kong, Office of the Privacy Commissioner for Personal Data, *Privacy Management Programme: A Best Practice Guide* (February 2014), which states that top management support is key to a successful privacy management programme and essential for a privacy respectful culture. Depending on the organisational structure, top management or its delegated authority should appoint the data protection officer.

If the DPO is not part of the management team, he should at least have direct access to them. In *M Star Movers*, Deputy Commissioner Yeong stated: "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."[29] This is echoed in Art 38(3) of the GDPR, which states that the DPO shall directly report to the highest management level of the organisation.[30]

C. Independence

25 There are several aspects to securing the independence of the DPO. The PDPA is not prescriptive in this regard, but useful guidance can be gleaned from the GDPR and the *Guidelines on Data Protection Officers*[31] adopted by the Article 29 Data Protection Working Party ("the Guidelines"). Recital 97 of the GDPR states that DPOs "should be in a position to perform their duties and tasks in an independent manner". Specifically, Art 38 of the GDPR provides that:

> (a) the organisation shall ensure that the DPO does not receive any instructions regarding the exercise of his tasks.[32]
>
> (b) the DPO shall not be dismissed or penalised by the organisation for performing his tasks;[33] and
>
> (c) the DPO may fulfil other tasks and duties, and the organisation shall ensure that any such tasks and duties do not result in a conflict of interests.[34]

---

29 *Re M Star Movers & Logistics Specialist Pte Ltd* [2018] PDP Digest 259 at [33].

30 The precise party to whom the data protection officer reports may vary depending on the size and structure of the organisation. According to International Association of Privacy Professionals and Ernst & Young, *IAPP-EY Annual Privacy Governance Report 2019* at p 15, privacy leaders at small firms more often report to the chief executive officer, and less often to the chief compliance officer, than those at large firms.

31 13 December 2016; revised 5 April 2017.

32 GDPR Art 38(3).

33 GDPR Art 38(3).

34 GDPR Art 38(6).

26 The Guidelines elaborate that DPOs must not be instructed how to deal with a matter; for example, what result should be achieved, how to investigate a complaint or whether to consult the authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law; for example, a particular interpretation of the law. This seems almost so obvious as to go without saying. Yet, there is utility in reiterating this, given that the DPO may face considerable pressure from business units to take a view aligned with commercial imperatives. Here, s 11(6) of the PDPA serves as a useful reminder that the appointment of a DPO does not relieve the organisation of its PDPA obligations – there is thus little to be gained in seeking to sway the DPO to a particular view.

27 To further assure their autonomy, DPOs must be protected from retribution for the dutiful discharge of their functions. As noted in the Guidelines, penalties may take a variety of forms and may be direct or indirect. Penalties can include the absence or delay of promotion, denial of benefits and dismissal. Significantly, the Guidelines note that a mere threat of these penalties would suffice, even if they are not carried out.

28 Relatedly, given that the DPO may concurrently hold other job functions, it is important that he is not placed in a position of a conflict of interest. Concurrent roles involving the use and processing of personal data are liable to give rise to a conflict of interest. In its Guidelines, the Article 29 Data Protection Working Party cites, as a rule of thumb, senior management positions (such as chief executive, chief operating officer, chief financial officer, head of the marketing department, head of human resources) as positions of potential conflict.[35]

D. Adequate resourcing

29 Finally, the DPO needs to be adequately resourced. Given the competing resource demands, it was unsurprising that the majority (62%) of respondents in the International Association of Privacy Professionals and Ernst & Young *Annual Privacy Governance Report 2019* felt that their

35 Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers* (13 December 2016; revised 5 April 2017) at section 3.5.

organisation's privacy budget was less than sufficient to meet their privacy obligations.[36]

30 Yet, adequate resourcing[37] for the DPO and his team is important to ensure not only that they are able to effectively develop and implement appropriate policies and practices, train employees to adhere to them, continually monitor risks and generally ensure compliance on an ongoing basis; adequate resourcing must also be provided for the DPO and his team to receive training and development as data protection professionals, so that they can keep abreast of the latest developments in this field.[38]

IV. Conclusion

31 Ultimately, organisations must recognise that safeguarding personal data is not just about complying with rules and regulations. Rather, safeguarding personal data fosters consumer trust and strengthens organisations' reputation, and is ultimately in their own self-interest.[39] Thus, the appointment of a DPO should not be regarded as a mere paper exercise. Serious thought needs to be given, not only to the technical competencies of the DPO, but also to where and how the DPO is placed in the organisational structure so that he is properly empowered and insulated from undue interference, as well as appropriately resourced and supported.

---

36 International Association of Privacy Professionals and Ernst & Young, *IAPP-EY Annual Privacy Governance Report 2019* at p 37.

37 Specifically, an adequate portion of the risk management budget ought to be allocated to the data protection officer function so that it can be appropriately staffed and resourced with, *inter alia*, the necessary information technology tools.

38 See Art 38(2) of the GDPR, which requires organisations to provide data protection officers with resources necessary to, *inter alia*, maintain their expert knowledge.

39 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

INDIVIDUALS' RIGHTS UNDER THE AMENDED PERSONAL DATA PROTECTION ACT: BALANCING INDIVIDUAL CONTROL AND ORGANISATIONAL ACCOUNTABILITY*

David N ALFRED†
LLB (Hons), LLM (National University of Singapore);
MBA (University of Chicago);
Advocate and Solicitor (Singapore); Solicitor (England and Wales);
CIPP/A, CIPM, CIPT, FIP

Janice LEE‡
LLB (Hons) Law with Chinese Law (University of Nottingham);
LLM (University of Melbourne); Advocate and Solicitor (Singapore);
CIPP/E, CIPM

I. Introduction

1 Like many data protection laws and regulations around the world today, the Personal Data Protection Act 2012[1] ("PDPA") is broadly consistent with the data protection principles in the Organisation for Economic Co-operation and Development ("OECD") *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[2] ("OECD

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent the views of their employer or any other party. All errors remain the authors' own.

† Formerly Director and Co-Head, Data Protection, Privacy & Cybersecurity Practice, Drew & Napier LLC and Co-Head and Programme Director, Drew Data Protection & Cybersecurity Academy. This article was written while Janice was a director at Drew & Napier LLC.

‡ Director, Data Protection, Privacy & Cyber-security Practice Group; Technology, Media & Telecommunications Practice Group, Drew & Napier LLC.

1 Act 26 of 2012.

2 The Organisation for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines") were first published in 1980 and a revised edition of the OECD Guidelines, the OECD Framework, was published in 2013.

Guidelines"). The OECD Guidelines emphasise individual control and procedural safeguards for data handling. They adopt an approach that relies heavily on "notice-and-consent", *ie*, the law gives individuals the right to receive notice of the proposed collection, use and disclosure of personal data and the right to decide whether to consent to such processing.[3] This places the individual at the centre of decision-making over the use of their personal data.[4]

2 However, one distinct feature of the PDPA is its explicit recognition that data protection regulation is as much about ensuring that organisations can use and harness personal data for legitimate and reasonable purposes as it is about protecting the personal data of individuals. This is encapsulated in s 3 of the PDPA which states that the purpose of the PDPA is to:

> … govern the collection, use and disclosure of personal data by organisations in a manner that recognises both *the right of individuals to protect their personal data* and the *need of organisations to collect, use or disclose personal data* for purposes that a reasonable person would consider appropriate in the circumstances. [emphasis added]

3 In seeking to strike a balance between the protection of personal data and the need of organisations to collect, use and disclose personal data, the PDPA has generally relied on a consent-centric approach, albeit one with a number of exceptions to allow organisations to collect, use or disclose personal data without consent. However, with the growth of new technologies such as the Internet of Things devices, machine learning and artificial intelligence, personal data today is increasingly not just information obtained from the individual, but also information about the individual acquired passively from external sources such as sensors or produced through predictive analytics. This presents significant challenges for consent-based approaches to data protection.[5]

---

3 Privacy scholar Daniel J Solove refers to the current approach to privacy regulation as "privacy self-management": Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126(7) Harv L Rev 1880 at 1880.

4 World Economic Forum, *Redesigning Data Privacy: Reimagining Notice & Consent for Human-technology Interaction* (White Paper, July 2020) at p 6.

5 Ministry of Communications and Information and Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection*

(*continued on next page*)

4 On 2 November 2020, Parliament passed the Personal Data Protection (Amendment) Act 2020[6] ("Amendment Act"), which is the culmination of the first comprehensive review of the PDPA since its enactment in 2012. The amendments to the PDPA under the Amendment Act reflect a shift towards a risk-based accountability approach to data protection. Its stated aims are to strengthen consumer trust through organisational accountability in respect of the handling and processing of personal data, enhance the flexibility and effectiveness of the Personal Data Protection Commission's ("PDPC's") enforcement efforts, enhance consumer autonomy, and support business innovation by providing organisations with greater clarity on the use of personal data.[7]

5 This article looks at the rights of individuals (*ie*, data subjects) under the PDPA and considers how the amendments to the PDPA have impacted those rights. Specifically, it considers whether the amendments have strengthened or weakened the protection afforded to personal data as a whole.

II. Overview of individuals' rights under the Personal Data Protection Act

6 The PDPA provides individuals with a "bundle" of rights that give them greater control over how their personal data is collected, used, disclosed and processed (collectively, "processing"). This bundle of rights is generally the most direct means for individuals to understand how organisations have been processing their personal data and hence plays an important role in fostering trust between individuals (as data subjects) and organisations (as data users).

(Amendment) Bill (14 May 2020) at paras 3 and 4; President's Council of Advisors on Science and Technology, *Report to the President – Big Data and Privacy: A Technological Perspective* (May 2014) at p 5; Jens-Erik Mai, "Big Data Privacy: The Datafication of Personal Information" (2016) 32(3) *The Information Society* 192 at 194.

6 Act 40 of 2020.

7 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information).

7 Under the PDPA (as amended by the Amendment Act), individuals' rights in relation to personal data in an organisation's possession or control generally include:

(a) the right to access their personal data;

(b) the right to correct their personal data;

(c) the right to data portability, that is, to have their personal data transferred from the organisation to another organisation; and

(d) the right to give and withdraw consent for the collection, use and disclosure of their personal data.

8 Under s 21 of the PDPA, individuals have the right to request access to their personal data in the organisation's possession or control, as well as to information about the ways in which their personal data has been or may have been used or disclosed by the organisation within a year before the date of the request. Unless any of the exceptions in s 21 of or the Fifth Schedule to the PDPA apply, organisations generally have a duty to respond to the individual's requests to access their personal data as accurately and completely as necessary and reasonably possible (referred to by the PDPC as the Access Obligation).

9 In this regard, the amendments to the PDPA have strengthened the Access Obligation by introducing a new requirement on organisations to preserve copies of personal data. Under the new s 22A, an organisation which refuses to provide access to the personal data requested by an individual under an access request must now preserve a complete and accurate copy of the personal data concerned for not less than the prescribed period (generally 30 days after the date of its rejection of the access request).[8] This requirement will help ensure that individuals who have successfully sought recourse for the rejection of their request are not denied access to their personal data simply because the organisation had already deleted the personal data.

10 The Access Obligation is an important right that individuals have under the PDPA because, as mentioned above, the PDPA is premised on the individual control paradigm of personal data protection which relies

8 There will be a similar obligation to preserve personal data or a copy thereof with regard to data requested pursuant to a data porting request when the data portability provisions come into force.

heavily on the "notice-and-consent" approach. This approach assumes that individuals can read and understand the data protection notices or policies posted by organisations and will follow a rational decision-making process to engage only with organisations that they believe offer an acceptable level of protection.[9] Given that consent legitimises almost all data handling practices, individuals take on the "burden of responsibility for the outcomes of the set of actions" that they consent to.[10] The right to access is therefore an important tool for individuals to find out what personal data an organisation has collected about them and to review whether their personal data has been processed in accordance with what has been represented.

11 In a similar vein, s 22 of the PDPA plays an important role in safeguarding individuals' interests given the increasingly data-driven nature of most decision-making processes. Under s 22, individuals have the right to request that an organisation correct any errors or omissions in their personal data that is in the organisation's possession or control. Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation is required to (a) make the correction as soon as possible; and (b) where the corrected data will be used for any legal or business purposes, send the corrected or updated personal data to specific organisations to which the personal data was disclosed within a year before the correction (referred to by PDPC as the Correction Obligation). Where an organisation is satisfied on reasonable grounds that a correction should not be made, the organisation must annotate the personal data in its possession or under its control with the correction that was requested but not made.[11]

12 The amendments to the PDPA have also introduced a new right to data portability. Under the new Part VIB of the PDPA, specifically, s 26H, individuals may request an organisation to transmit a copy of their personal data that is in the organisation's possession or control to another organisation in a commonly used machine-readable format. Organisations

9 Joel R Reidenberg *et al*, "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding" (2015) 30(1) Berkeley Tech LJ 39 at 41.

10 Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126(7) Harv L Rev 1880 at 1880; Daniel Susser, "Notice after Notice-and-Consent: Why Privacy Disclosures Are Valuable Even if Consent Frameworks Aren't" (2019) 9 *Journal of Information Policy* 37 at 49.

11 Personal Data Protection Act 2012 (Act 26 of 2012) s 22(5).

which receive such a data porting request must transmit the relevant data (referred to in the PDPA as the applicable data) to the receiving organisation in accordance with any prescribed requirements (the Data Portability Obligation). Part VIB of the PDPA has not yet been brought into effect but it is anticipated that the new Data Portability Obligation will give individuals greater autonomy, control and choice over how organisations process their personal data.

13 Finally, given that the PDPA is a consent-centric regime, the right to withdraw consent for the collection, use and disclosure of personal data is arguably the most important right that individuals have under the PDPA.[12] In particular, not only can individuals choose whether to give consent when an organisation wishes to collect their personal data; individuals may also withdraw consent on giving reasonable notice to the organisation. Section 16(3) of the PDPA provides that an organisation may not prohibit an individual from withdrawing consent, although this does not affect the legal consequences of such withdrawal. Although this right is commonly characterised as part of organisations' obligation to obtain consent for the collection, use and disclosure of personal data (the Consent Obligation), it further strengthens the control individuals have over their personal data.

14 Unlike some other countries' data protection laws, the PDPA does not include a right for individuals to be informed of how an organisation is processing their personal data. However, the PDPA requires organisations to make information about their data protection policies and practices publicly available (referred to in the PDPA as the Accountability Obligation). Similarly, to obtain valid consent, organisations are required to notify individuals of the reasonable purposes[13] for which their personal data will be collected, used or disclosed on or before such collection, use or disclosure (referred to in the PDPA as the Notification Obligation).

---

12 Under s 16 of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA"), individuals have the right to withdraw any consent given, or deemed to have been given under the PDPA, in respect of the collection, use or disclosure of their personal data by giving reasonable notice.

13 Under s 18 of the Personal Data Protection Act 2012 (Act 26 of 2012), an organisation may only collect, use or disclose personal data about an individual for purposes that "a reasonable person would consider appropriate in the circumstances", and (if applicable) for purposes that the individual has been informed of.

15 The next part will consider how the amendments to the PDPA have impacted individuals' control over their personal data and, specifically, in relation to the right to withdraw consent.

III. Amendments to the Personal Data Protection Act

16 Unless the collection, use or disclosure of an individual's personal data is required or authorised under the PDPA or any other written law, consent has always been (and remains) the primary basis for collecting, using and disclosing personal data under the PDPA.[14] However, to facilitate data sharing, reduce compliance costs and give organisations more flexibility in terms of how they can use and process personal data for business purposes, the amended PDPA introduced several new provisions which allow organisations to collect, use and disclose individuals' personal data without their express consent.

17 First, the amended PDPA has expanded the circumstances where "deemed consent" would apply to include deemed consent by contractual necessity and deemed consent by notification. Under the new s 15(3) of the PDPA, an individual who provides personal data to an organisation with a view of entering a contract with that organisation is deemed to consent to the following, where it is "reasonably necessary" for the conclusion of the contract between them:

> (a) the disclosure of that personal data by the organisation to a second organisation;
> (b) the collection and use of that personal data by the second organisation; and
> (c) the disclosure of that personal data by the second organisation to a third organisation.

---

14 Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") s 13. Even though the amendments to the PDPA have, in effect, created alternative bases for organisations to collect, use and disclose personal data, unlike Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC which recognises consent as but one of six bases for processing personal data, the PDPA has generally characterised the other "bases" as exceptions to the requirement to obtain consent.

18 Section 15A of the PDPA in turn introduces a new basis for organisations to collect, use and disclose personal data. Under deemed consent by notification, organisations may notify customers of new purposes for which they intend to use and disclose individuals' personal data and provide a reasonable period for them to opt out. An individual will be deemed to have consented to the organisation's collection, use and disclosure of their personal data for the new purposes notified if the following conditions are satisfied:

> (a) Before collecting, using or disclosing any personal data about the individual, the organisation must conduct a risk assessment to determine that the proposed collection, use and disclosure is not likely to have an adverse effect on the individual.
>
> (b) The organisation must take reasonable steps to bring the information below to the individual's attention:
>
> > (i) the organisation's intention to collect, use or disclose the personal data;
> >
> > (ii) the purpose for which the personal data will be collected, used or disclosed; and
> >
> > (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that he does not consent to the proposed collection, use or disclosure of his personal data.
>
> (c) The individual does not notify the organisation before the expiry of the reasonable period that he does not consent to the proposed collection, use or disclosure of his personal data.

19 Second, the amended PDPA has introduced two broad exceptions to the consent requirement, namely the legitimate interests exception and the business improvement exception. Unlike the previous exceptions which were generally limited to a specific context or set of circumstances (*eg*, where the collection, use or disclosure of personal data is necessary for any investigation or proceedings, or for an organisation to recover a debt owed to the organisation or for the organisation to repay a debt owed to the individual), the new exceptions are meant to "cater to situations where

there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate".[15]

20 The legitimate interests exception allows organisations to collect, use or disclose personal data without consent where the need to protect legitimate interests that have economic, social, security or other benefits for the public (or a section thereof) outweighs any adverse effect on the individual. Such circumstances could include the purposes of detecting or preventing illegal activities (*eg*, fraud, money laundering) or threats to physical or information technology and network security, where it is not viable to seek individuals' consent for the collection, use or disclosure of their personal data for such purposes.[16]

21 Given the potentially wide range of circumstances and purposes that could fall within this exception, organisations are required to conduct an assessment to identify any adverse effects that the proposed collection, use or disclosure is likely to have on the individual, and identify and implement reasonable measures to eliminate, reduce the likelihood of, or mitigate the adverse effect before collecting, using or disclosing personal data in reliance on the legitimate interests exception. Organisations are also required to provide the individual with reasonable access to information about the organisation's reliance on the legitimate interests exception (*ie*, to disclose the organisation's reliance on the legitimate interests exception and the situation or purpose that qualifies as a legitimate interest).

22 The new business improvement exception allows organisations to use (but not collect or disclose) personal data that was collected in accordance with the data protection provisions without consent for certain business improvement purposes. Such purposes can be broadly characterised into the following categories: (a) to make operational efficiency and service improvements; (b) for product and service development; or (c) to know customers better. However, organisations can only rely on the business improvement exception if the purpose cannot reasonably be achieved without the use of the personal data in an individually identifiable form,

---

15 Ministry of Communications and Information and Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection (Amendment) Bill* (14 May 2020) at para 40.

16 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 1 October 2021) at para 12.63.

and the use of personal data is for a business improvement purpose that a reasonable person would consider to be appropriate in the circumstances.[17]

IV. How will the amendments to the Personal Data Protection Act impact individuals?

23 By expanding the circumstances under which organisations can collect, use or disclose personal data without the individual's explicit consent, the amendments to the PDPA have arguably diminished the role of consent under the PDPA. Given that consent is closely tied to the notion of control over one's personal data, by reducing the amount of direct control that individuals have over their personal data, the amendments to the PDPA would appear to have a negative impact on the rights of individuals.

24 However, the notion that consent gives individuals control over their personal data and control is the best way to protect personal data is premised on questionable assumptions. While "notice-and-consent" gives individuals the illusion of choice and control over their personal data, this approach has come under sustained criticism. First, it assumes that the essence of consumer weakness stems from information deficits and that information is all a consumer needs to be able to make meaningful choices regarding the use of their personal data.[18] This ignores the extremely complex data collection and sharing relationships of today and disregards the power and information asymmetries that exist between individuals and organisations.[19] Research has also shown that there are various cognitive biases and natural constraints on human rationality and decision-making which drastically limit the ability of individuals to understand and assess the

17 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, Part 2, Div 2.

18 Mateusz Grochowski *et al*, "Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Remises" (2001) 8(1) *Critical Analysis of Law* 43 at 62 and 63.

19 Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order" (2014) 63(3) ICLQ 569 at 593.

potential harm that may arise from the use of their data.[20] Further, as mentioned above, because consent legitimises nearly any form of collection, use and disclosure of personal data, the notice-and-consent model of data protection places a disproportionate burden on individuals to self-manage their personal data and weigh the costs and benefits of agreeing to the data practices.

25 More importantly, the amended PDPA has introduced several new provisions that are aimed at increasing organisational accountability and strengthening the PDPC's enforcement powers alongside enhancements to the framework for collection, use and disclosure of personal data. Organisational accountability places more responsibility on organisations that are collecting and using data to not just implement comprehensive personal data protection programmes that govern all aspects of the collection, use and disclosure of personal data, but to also be able to demonstrate the existence and effectiveness of such programmes upon request.[21] As such, rather than having a negative impact on individuals' rights, it is arguable that the amended PDPA has in fact strengthened the safeguards for individuals' interests and provides more meaningful protection for individuals' personal data than before.

26 First, although organisations now have more latitude to collect, use and disclose personal data without consent under deemed consent by notification and the legitimate interests exception, they can only do so for purposes that they have assessed are unlikely to have an adverse effect on the individual. In the authors' view, this strikes a better balance by affording individuals more meaningful protection and giving organisations the ability and flexibility to harness personal data for legitimate purposes. The requirement to carry out a risk assessment also places the primary burden for protecting personal data on organisations to assess and take reasonable measures to mitigate the risks or adverse effects before collecting, using or disclosing the personal data. Further, because this risk-based approach requires that organisations differentiate between the types of

---

20 Mateusz Grochowski *et al*, "Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Remises" (2001) 8(1) *Critical Analysis of Law* 43 at 62 and 63.

21 Centre for Information Policy Leadership, "Seven Global Personal Data Protection Priorities for 2020" *DPO Connect* (March 2020).

processing that pose a bigger risk to individuals and those that pose a smaller risk, it enables organisations to prioritise and allocate their resources and efforts to ensure protections in high-risk areas.[22]

27 Second, under the new mandatory data breach notification regime, organisations are required to notify not just the PDPC[23] but also the individuals affected by a notifiable data breach where the data breach results or is likely to result in significant harm to the affected individuals.[24] Data breach notifications are central to organisational accountability because they encourage organisations to establish risk-based internal monitoring and reporting systems to detect data incidents.[25] This ensures that organisations are accountable to individuals for the proper handling and safekeeping of their personal data. The requirement to notify affected individuals will also allow individuals to take steps to protect themselves upon being notified (*eg*, changing passwords, cancelling credit cards, and monitoring and reporting scams or fraudulent transactions).[26]

28 Third, the amendments have introduced new offences for the egregious mishandling of personal data in an organisation's possession or control[27] and expanded the scope of the Protection Obligation to include the requirement to put in place reasonable security arrangements to prevent

22 Centre for Information Policy Leadership, "Seven Global Personal Data Protection Priorities for 2020" *DPO Connect* (March 2020).

23 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(1).

24 Personal Data Protection Act 2012 (Act 26 of 2012) s 26D(2). Unless either one of the following exceptions apply: (a) where the organisation has taken remedial actions that render it unlikely that the notifiable data breach will result in significant harm to the affected individual; or (b) where the personal data that was compromised by the data breach is subject to technological protection (*eg*, encryption) that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

25 Ministry of Communications and Information and Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection (Amendment) Bill* (14 May 2020) at para 13.

26 Ministry of Communications and Information and Personal Data Protection Commission, *Public Consultation on the Draft Personal Data Protection (Amendment) Bill* (14 May 2020) at para 16.

27 Personal Data Protection Act 2012 (Act 26 of 2012) ss 48D, 48E and 48F.

"the loss of any storage medium or device on which personal data is stored".[28]

29 Along with the increased emphasis on organisational accountability, the amended PDPA has also strengthened the PDPC's enforcement powers by increasing the maximum financial penalty that the PDPC may impose for breaches of the PDPA and granting the PDPC the power to require a person to make a statement or to refer parties to mediation. These serve as strong deterrents and provide the PDPC with more flexibility in imposing financial penalties based on the circumstances and seriousness of the breaches.

30 Moreover, as the PDPA shifts away from the individual control paradigm of data protection towards an approach that relies more on organisational accountability, the enhanced enforcement measures play an important role in strengthening individuals' trust and confidence in the protection of their personal data.

V. Conclusion

31 The amended PDPA has both increased the rights that individuals have in some respects (*eg*, the introduction of the data portability obligation) and decreased the amount of direct control that individuals have over how their personal data is collected, used and disclosed in other respects (*eg*, the introduction of new grounds of deemed consent and exceptions to the Consent Obligation). Individuals' rights and consent remain key aspects of effective data protection regulation, particularly in areas such as direct marketing where consumers should be given the right to exercise choice and control. That said, on balance, it is arguable that the increased emphasis on organisational accountability and enhanced enforcement powers have in fact strengthened the safeguards for individuals' interests and provide more meaningful protection for individuals' personal data than before.

32 While it remains to be seen how organisations will rely on the new grounds for processing and whether those that fail to comply with the risk assessment requirements will be held to account, it appears that the

28 Personal Data Protection Act 2012 (Act 26 of 2012) s 24(*b*).

amended PDPA has found a balance that is more fit-for-purpose in today's digital and data-driven age.

DATA PORTABILITY: THE SINGAPORE APPROACH AND A COMPARATIVE STUDY OF SELECTED JURISDICTIONS*

Amira Nabila BUDIYANO†
LLB (Singapore Management University),
Grad Dip (IP and Innovation Management) (Singapore University of Social Sciences); CIPP/A; Advocate and Solicitor (Singapore)

Jonathan KAO‡
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore)

I. Introduction

A. Data portability (as a principle) and what it means

1 Data portability is a relatively new development in a number of jurisdictions. While it is commonly rooted in data protection legislation, it touches upon other areas including consumer protection and competition law. The approaches undertaken by each jurisdiction are also driven by interests in these various areas of law. While there are some similarities in the approaches taken by various jurisdictions, each approach tends to be specific to that jurisdiction addressing specific concerns and interests.

2 Data portability, as a principle, can be thought of as both an extension of the right to access and a potential means to foster innovation in data-driven economies. Most, if not all, jurisdictions require that data in an organisation or controller's control or possession be transmitted to another organisation at the direction of the individual whose data is concerned. Depending on the jurisdiction, this obligation is subject to a number of considerations including:

---

* The views expressed in this article are the authors' personal views and may not be representative of the views of their respective employers.

† Amira was formerly an Associate Director at Gateway Law Corporation, Singapore. She is presently an attorney at Kyndryl (Singapore) Pte Ltd.

‡ Senior Associate, Bird & Bird ATMD LLP, Singapore.

(a) how the data came into the organisation's/controller's control or possession (*eg*, whether data was provided directly by the individual, derived from the individual or other sources, *etc*);

(b) the basis upon which the organisation/controller came into control or possession of the data (*eg*, whether consent was given and in what form, and/or if exceptions to consent such as investigative or evaluative purposes apply);

(c) the state of the personal data (*eg*, whether in physical records or electronic form); and

(d) the potential impact on the organisation/controller and third parties, where applicable (*eg*, intellectual property rights and trade secrets).

3 Being a relatively new obligation, regulatory instruments and practical implementation of the obligation are still being refined especially where the ported data is expected to be in a format that is common or interoperable across organisations.

B. Objective

4 This article seeks to study the upcoming data portability obligations in Singapore in light of further consultations having been conducted by the Personal Data Protection Commission ("PDPC") since 2019. In coming to a better understanding and appreciation of Singapore's approach, a comparative study is done with selected jurisdictions, namely the European Union ("EU"), Australia and Canada.

5 The jurisdictions selected are deliberate in that all three jurisdictions are indeed in different stages of implementation. For instance, the EU can be said to have legislatively implemented data portability obligations across all member states and industries, but practical implementation is still ongoing. In contrast, Australia's data protection obligations have yet to come into effect for all industries and sectors. Nevertheless, the amount of guidelines and regulations surrounding just the first sector is enormous and undoubtedly much more prescriptive than even the EU. The last jurisdiction, Canada, is in the midst of passing its laws involving data portability, and quite clearly has some rather distinguishing features when compared to its EU and Australian counterparts. The differences in fact go beyond the nomenclature selected (data *mobility* rather than data *portability*). Given the varying stages of development and implementation

in these jurisdictions, it could signal that Singapore ought to be akin to Canada in its approach when juxtaposed against all three. However, this article proposes that Singapore's approach will probably stand in its own league.

II. Singapore's data portability obligations

A. How it is looking to shape into

6 In a joint discussion paper by the PDPC and the Competition and Consumer Commission of Singapore ("CCCS"),[1] data portability was noted to have the "potential to bring great benefits to consumers and businesses alike through the increased flow of data in the economy".[2] Among other potential benefits, the flow of data that would be enabled by data portability holds the promise of lowering the cost of switching, potentially enhancing competition by lowering the barriers to entry, and facilitating innovation especially where complementary products and/or services are involved. This would nonetheless have to be measured against the consumer's control and access to data, and costs to businesses in conforming with this right.

7 Data portability under Singapore's approach is described as an obligation where "an organisation must, at the request of the individual, provide the individual's data that is in the organisation's possession or under its control, to be transmitted to another organisation in a commonly used machine-readable format".[3] This is distinct from the Access Obligation as this only requires the transmission of data from one organisation to another, and the porting organisation is not required to

1 Personal Data Protection Commission in collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability* (25 February 2019).

2 Personal Data Protection Commission in collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability* (25 February 2019) at para 5.1.

3 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 2.1.

provide a copy of the ported data to the individual or allow the individual to verify the data to be ported.[4]

(1) Organisations subject to the obligation

8 The "organisation" referred to here is as defined in the Personal Data Protection Act 2012[5] ("PDPA"). Such an organisation must have a presence in Singapore, being "either formed or recognised under the law of Singapore, or having a place of business, in Singapore".[6] The onus is placed on the porting organisation to decide whether a receiving organisation has a presence in Singapore.

9 The proposed data portability obligation would not apply to data intermediaries in relation to the data they process on behalf and for the purposes of another organisation.[7] Depending on their agreements with the organisation, data intermediaries may nonetheless have a role to play in identifying and preparing the data for porting.

(2) Data subject to the obligation

10 Data that is subject to the data portability obligation would be data held in electronic form of individuals with whom the porting organisation has a direct and existing relationship,[8] and is: (a) provided by the individual to the organisation (user provided data); or (b) generated by the individual's activities in using the organisation's product or service (user activity data). It was further proposed that business contact information would form part

---

4 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 4.9.

5 Act 26 of 2012.

6 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 2.7.

7 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 2.2.

8 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 3.8 read together with para 3.1.

of the portable data as "there is value for both individuals and receiving organisations for such data to be portable".[9]

11 Certain limitations have also been proposed on the scope of the data that can be ported over, such as:

(a) a set of exceptions similar to those for the Access Obligation to ensure consistency across similar obligations;

(b) a set of exceptions for data collected in reliance on an exception to the consent obligation;

(c) a set of exceptions for data that would reveal confidential commercial information that could harm the competitive position of the porting organisation;

(d) a set of exceptions for "derived data", that is, new data created through the processing of other data by applying business-specific rules; and

(e) that the data portability obligation would only apply to "white-listed datasets" of standard data categories to be developed in consultation with industry stakeholders.

12 Data about third parties can also be included in the ported data without obtaining their consent subject to appropriate safeguards. These safeguards include requiring the porting organisation to ensure that:

(a) the requested data is under the control of the requesting individual;

(b) the data porting request is for the requesting individual's own personal or domestic purposes; and

(c) the third party's personal data is collected for the purpose of providing the product or service which the requesting individual had given consent (or is deemed to have given consent) for, and not for any other purposes.

9 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 3.8.

(3) Data format

13 The proposed data protection obligations contemplate that the data will be ported in a "commonly used machine-readable format". This has not been defined and specifications are not provided as yet, but the PDPC has indicated that "open data formats, security standards and transmission protocols" will be included in guidelines or regulations following further consultation with industry stakeholders.[10] These are intended to enable interoperability between organisations porting and receiving the data.

14 Similar to other jurisdictions, there are concerns over compliance costs if these remain too vague as there does not appear to be sufficient consensus across industries, much less across different jurisdictions.

(4) Obligations of the porting organisation

15 The time frame for a porting organisation to respond to a porting request has yet to be confirmed. It was initially proposed that this would be "within a reasonable period" and up to seven days but following feedback during consultations, the time frame is being reviewed and is yet to be confirmed.

16 It was clarified that porting organisations are not required to introduce an additional step of allowing individuals to verify their data before porting. The PDPC noted that organisations are already subject to the Accuracy Obligation and would already need to have policies and practices to ensure the accuracy of the ported data. Porting organisations would also be allowed to reject porting requests under certain circumstances such as where the burden or expense to do so would be unreasonable (including where it may not be technically feasible), or if the porting organisation is unable to verify the requesting individual's identity.[11]

17 The PDPC's response to the feedback suggests that porting organisations would not be responsible or liable for breaches of ported data

10 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 4.11.

11 Personal Data Protection Commission in collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability* (25 February 2019) at para 3.10.

as the receiving organisation would already be subject to the Protection Obligation in relation to the data that is now in their possession or under their control.[12] However, this does not clearly address whether the Protection Obligation applies to the porting organisation in this situation and whether and what steps porting organisations would need to take to ensure that the receiving organisation will have or has policies and practices in place to protect the ported data.

B. Meeting its objectives but more clarity needed

18 Together with the data innovation provisions that have already come into effect, the data portability obligations do appear to have the potential for making it easier for data to be made available to different organisations, potentially allowing greater use of the data and insights to be derived from the same. The limiting of the obligation to data in electronic form and the ongoing engagement with stakeholders to specify technical and process details reflect a practical approach and recognition by the PDPC that these are potential hurdles. There may be technical arguments that only subjecting data in electronic form to the obligation means organisations can potentially avoid the obligation by keeping data in machine-readable but non-electronic form. The argument may not have much practical significance as it is likely that production data will be in electronic form due to cost and efficiency considerations; non-electronic records (for example, archival data or from more paper-intensive industries) may be valuable but this may not outweigh the costs involved in mandating that organisations digitise and make such records available.

12 Personal Data Protection Commission, *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions* (20 January 2020) at para 4.10.

19 The proposed "white-listed dataset" approach and only requiring data to be ported between organisations are in line with the stated objective of empowering individuals to "try out or move to new or competing service offerings".[13] Based on the public consultation[14] and response, it does not appear that the obligation is limited to porting between organisations in the same industry, potentially facilitating greater innovation by enabling data to be ported across industries whether or not related. This also suggests that the porting organisation may not need to cease providing services to the individual after porting the data such as where an individual may wish to obtain similar services from multiple service providers. The position may be clearer once the regulations and guidelines are released.

20 Without the ability to obtain a copy of the ported data, individuals do not appear to have the opportunity to switch service providers or determine what other organisation can receive the data without disclosing that receiving service provider or organisation to the porting organisation. Singapore will also be excluding confidential commercial information and derived data from data portability obligations to prevent unfair competition from "fast followers".[15] Innovators that wish to obtain data from individuals and conduct market research and feasibility studies using such data prior to market entry without alerting potential competitors will likely have to rely on other means such as having individuals request for and provide their data obtained through the Access Obligation.

III. Comparative study

21 In this part, the authors will be making a jurisdictional comparison of various data portability regimes around the world to Singapore's. In particular, the authors will study and note some distinguishing features of

13 Personal Data Protection Commission in collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability* (25 February 2019) at para 5.1.

14 Personal Data Protection Commission, *Public Consultation on Review of the Personal Data Protection Act 2022 – Proposed Data Portability and Data Innovation Provisions* (22 May 2019), example at para 2.34.

15 Personal Data Protection Commission in collaboration with Competition and Consumer Commission of Singapore, *Discussion Paper on Data Portability* (25 February 2019) at para 3.10.

the EU's General Data Protection Regulation[16] ("GDPR") as well as Australia's Consumer Data Right. To give a good comparison with another jurisdiction that is also on the cusp of implementation of a new data portability right, reference to Canada's new Consumer Privacy Protection Act ("CPPA") will be made.

A. European Union

22 In discussions of data protection, the GDPR is often an important reference primarily because it is the first comprehensive piece of data protection law and has impacted data protection laws and practices globally. Singapore's data portability obligations in their proposed form do not differ too distinctly from data portability under the GDPR. Data portability was introduced as part of the GDPR along with the *Guidelines on the Right to Data Portability under Regulation 2016/679*[17] ("WP29 Portability Guidelines") developed by the Article 29 Data Protection Working Party. There has also been a related development in the form of the European Interoperability Framework, a set of recommendations specifying how organisations communicate with each other within the EU and between member states.

23 Data portability holds promise for supporting the free flow of personal data within the EU and fostering the development of new services in the context of the EU's digital single market strategy. Nevertheless, work remains ongoing on the practical application of the data portability rights and, for organisations that operate in multiple jurisdictions, the interaction of the data portability rights and obligations under the GDPR with similar rights and obligations in other jurisdictions.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").

17 5 April 2017. Endorsed by the European Data Protection Board as part of the GDPR-related Article 29 Working Party Guidelines.

(1) General Data Protection Regulation Article 20

24 The right to data portability in the GDPR can be found within Art 20 and Recital 68. These are read with the WP29 Portability Guidelines. The WP29 Portability Guidelines note that this right aims at "empowering data subjects regarding their own personal data as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another".[18]

(2) Compared to access rights

25 Under the GDPR, data subjects already have the access rights to their data and can require that their data be provided in a commonly used electronic form.[19] The data portability obligation expands how the data is to be accessed or ported but narrows the scope of the data that is subject to the obligation.

26 Compared to the access rights, the scope of data that is subject to the portability obligation is narrower and includes personal data that is:

(a) processed by automated means;

(b) provided by the data subject to the controller; and

(c) processed on the basis of consent, processed to fulfil a contract or leads to a contract.

(3) Scope of data

27 Data "provided by" the data subject very broadly includes data actively and knowingly provided by the data subject: for example, data provided in forms. This also includes observed data that is "provided" by the data subject in the use of the services or device: for example, search history, location data, purchase history, and raw data such as data from health and fitness trackers.

28 The WP29 Portability Guidelines draw a distinction between "inferred data" and "derived data" from data that is "provided by" the data subject. "Inferred data" and "derived data" are created by the data

18 Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability under Regulation 2016/679* (5 April 2017) at p 4.

19 GDPR Art 15.

controller based on data "provided by" the data subject: for example, a credit score or a profile developed from the analysis of the data subject's behaviour. This additional layer of abstraction excludes "inferred data" and "derived data" from the scope of the right to data portability. Metadata presents some challenges and the WP29 Portability Guidelines recommend that the ported data should be provided with as much metadata as possible at the best possible level of granularity, which preserves the precise meaning of exchanged information. Accordingly, the specific circumstances will need to be examined in order to determine if and to what extent metadata is to be included in the provided data, and this presents an area of uncertainty for data controllers.

29 Where the data relates to multiple individuals, the WP29 Portability Guidelines suggest that the data should nonetheless be provided as part of the right to data portability. However, the porting data controller would not be responsible for ensuring that recipient complies with applicable data protection laws in relation to that data.[20]

30 Noting that the right to data portability "shall not adversely affect the rights and freedoms of others", the porting data controller may have to implement a means to provide the data without disclosing or compromising its intellectual property rights and trade secrets. However, the porting data controller's protection of its intellectual property rights and trade secrets alone should not be the basis to refuse to answer the request.[21] There are other access rights beyond the GDPR, such as under the Payment Services Directive[22] and, to some extent, the Digital Content Directive.[23] The WP29 Portability Guidelines also suggest that GDPR data portability

20 Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability under Regulation 2016/679* (5 April 2017) at p 5.

21 Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability under Regulation 2016/679* (5 April 2017) at p 10.

22 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

23 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

obligations do not apply if the individual is clearly exercising access rights beyond the GDPR.

(4) Data format

31 The GDPR specifies that the requested data be provided "in a structured, commonly used and machine-readable format".[24] Individuals should also be able to "transmit those data to another controller without hindrance from the controller to which the personal data have been provided",[25] and can also require the data controller to transmit the data directly to another controller where it is technically feasible to do so.

32 While the foregoing suggests some degree of harmonisation with terms such as "commonly used", and transmission to another controller "without hindrance", the WP29 Portability Guidelines note that the desired outcome is "interoperability" of the data format rather than "compatibility" of controllers' systems and encourage industry stakeholders and trade associations to work together to develop interoperable standards and formats. "Interoperability" is recognised and defined in the EU and efforts remain ongoing for broad adoption of the new European Interoperability Framework.

33 The new European Interoperability Framework encourages the design and delivery of services that are:

(a) digital-by-default;
(b) cross-border-by-default;
(c) open-by-default;
(d) privacy-by-design; and
(e) interoperability-by-design.

(5) Further obligations on the porting organisation

34 Data controllers are required to provide the personal data "without undue delay" and "within one month of receipt of the request",[26] with the possibility of extensions subject to certain conditions. Even if the data

24 GDPR Art 20(1).
25 GDPR Art 20(1).
26 GDPR Art 12(3).

controller can validly refuse the request, that refusal must be communicated within those timelines as well.

35 The data controller porting the data is also generally expected to secure the data to be ported. This would include taking steps to verify the request, securing access to and transmission of the data, and ensuring the correct recipient receives the data.[27]

B. Australia

(1) Consumer data right

36 Australia's equivalent of data portability rights are found in a segment of larger legislation dealing with broader issues under competition and consumer rights, called the Competition and Consumer Act 2010 ("Australian CCA"). This segment is known as consumer data right ("CDR"),[28] which took effect in February 2020. CDR creates the right for consumers to require data holders to share specified categories of data relating to such consumers to trusted recipients, *ie*, accredited persons, in a secure manner; and to access such data about themselves in a machine-readable form. To put it simply, sharing of such data is only even possible if the organisation porting such data and the organisation waiting to receive such data are both accredited. Further, one important tenet of the CDR is that consumers themselves have the right to obtain such data about themselves, and porting can happen even without the inter-organisation element. It is also noteworthy that consumers can include businesses too and not just individuals, so long as one is reasonably identifiable from the specified data.

---

27 Article 29 Data Protection Working Party, Guidelines on the *Right to Data Portability under Regulation 2016/679* (5 April 2017) at p 15, making reference to Art 5(1)(f) of the GDPR.

28 The Australian government introduced consumer data right in Australia on 26 November 2017. It was passed in 2019 and is set out in Part IVD of the Competition and Consumer Act 2010 (Cth).

37 Australia's CDR is currently being implemented in stages by industry, starting with the banking sector, followed by the energy[29] and telecommunications sectors. It is co-regulated by the Australian Competition & Consumer Commission ("ACCC") and the Office of the Australian Information Commissioner. Additional CDR rules and standards will be prescribed and implemented for each industry sector. This in itself already makes it stand apart from the approaches taken by Singapore as well as the EU. There is no one blanket law that allows for uniform application to all sectors although there are general provisions on data portability under the CDR and a framework known as "Privacy Safeguards", which will be discussed in further detail below.[30]

38 The CDR is unabashedly driven by economic and competition factors, but from the perspective of the consumer. In other words, the system is consumer driven.[31] It is anticipated to give consumers greater access to and control over their data and will improve consumers' ability to compare and switch between products and services. It is further hoped to encourage competition between service providers, leading not only to better prices for customers but also more innovative products and services.[32]

39 The subject of CDR known as "CDR data" comprises either information within a class of information specified (*ie*, data outlined in the instrument designating a sector); or information wholly or partly derived from the foregoing class of information specified.[33] CDR data can include product information or records of usage of a good or service.[34] Nevertheless, there are limits on the data that data holders may be required to give access to. For data that relates to a CDR consumer, a data holder can only be required to disclose that data to an accredited person, designated gateway or the consumer themselves. In this circumstance, the data is also limited to

29 The consumer data right was extended to the energy sector formally on 26 June 2020.

30 See paras 46–52 below.

31 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at para 1.308.

32 Australian Competition & Consumer Commission website <https://www.accc.gov.au/>.

33 Competition and Consumer Act 2010 (Cth) ss 56AI and 56AC(2).

34 Treasury Laws Amendment (Consumer Data Right) Bill 2019 Explanatory Memorandum, para 1.113.

data that is specified in the instrument and does not include data that is derived from data specified in the instrument.[35] On the other hand, for data about a product, good or service, a data holder can only be required to disclose data about the eligibility criteria, terms and conditions, price, availability or performance of the product, good or service. Disclosure about the availability or performance can only be mandated where this data is publicly available.[36] CDR data also is subject to geographical limitations, namely there should be a connection to an Australian person. In practical terms, if the CDR data was collected or generated outside of Australia and the transaction occurred overseas, provided that the data holder is registered in Australia and such CDR data relates to an Australian consumer, the CDR regime applies.

(2) The consumer data right relationship and principle of reciprocity

40 Given the above background to the CDR regime, it is important to understand the parties in a CDR relationship. They are the (a) accredited person (data holder); (b) accredited person (data recipient); (c) designated gateway; and (d) CDR consumer.

41 Be it as a data holder or data recipient, such accredited persons must meet the strict accreditation criteria prior to becoming accredited. In essence, they must have been able to demonstrate that they are a fit and proper person or organisation to manage CDR data;[37] have taken steps to adequately protect data from misuse, interference, loss, unauthorised access, modification or disclosure; have internal dispute resolution processes meeting the requirements of the CDR rules;[38] belong to a relevant external

35 Competition and Consumer Act 2010 (Cth) s 56BD(1).

36 Competition and Consumer Act 2010 (Cth) s 56BF(1).

37 To be deemed a fit and proper person, essentially one must not have had past convictions or found to be contravening any law domestically or otherwise; and none of the directors for a body corporate must have ever been disqualified or banned from managing a company. For the full requirements see Australian Competition & Consumer Commission, Consumer Data Right Accreditation Guidelines (Version 3 (draft), 27 October 2021) at part 6.1.

38 For the banking sector, this means their processes must comply with provisions of the Australian Securities and Investments Commission's *Regulatory Guide 165 – Licensing: Internal and External Dispute Resolution* (July 2020).

dispute resolution scheme;[39] have adequate insurance to compensate CDR consumers for any loss that might occur from a breach of the accredited data recipient's obligation;[40] and have an Australian address for service.

42 A designated gateway is one that is specified as a gateway by the Government (for each sector).[41] It is thus unlikely that businesses will be designated gateways; rather, government-controlled bodies or entities would be designated instead. The designated gateway will transfer data between the data holder and an accredited data recipient. This party can be seen as a facilitator and is meant to exercise some form of control over a data holder or data recipient in a CDR relationship, where possible. One can probably think of this designated gateway as a data intermediary. It is therefore clear that not all porting cases would require a designated gateway's involvement; some can be transferred directly between the data holder and recipient.

43 A CDR consumer is the person or entity that holds the rights to access the data held by a data holder and to direct that this data be shared with an accredited person. Whether a person or entity is a CDR consumer depends on the data in question; whether the person or entity can be identified, or reasonably identified, from that data or from data that is already held by the data holder or accredited data recipient; and whether it relates to that person or entity.[42]

44 In deciding whether a person can be "reasonably" identified from the data would depend on the factual circumstances at hand including the nature and amount of information, other information that may be available

---

39 Australian Competition & Consumer Commission, Consumer Data Right Accreditation Guidelines (Version 3 (draft), 27 October 2021) at part 6.3.

40 No particular insurance product type is prescribed, and this is very much left to each prospective applicant for accreditation. Nevertheless, other policy types either in isolation or in conjunction with other insurance policies may satisfy the insurance obligation. Such policies may include professional indemnity insurance and cyber insurance. For a more detailed explanation on this requirement, see generally Australian Competition & Consumer Commission, *Consumer Data Right: Supplementary Accreditation Guidelines – Insurance* (25 May 2020).

41 Competition and Consumer Act 2010 (Cth) s 56AL.

42 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at para 1.102.

to the persons who will have access to the information, and the practicability of using that information to identify a person. It is said that:[43]

> … [an] important consideration in whether data can be considered to relate to a 'reasonably identifiable' person is what motivations there may be to attempt re-identification. [In this respect, a] person will be reasonably identifiable [in the following situations]:
>
> - it is technically possible for re-identification to occur (whether from the information itself, or in combination with other information that may be available), and
> - there is a reasonable likelihood of re-identification occurring.

45 The CDR rules may also provide that a consumer can direct an accredited data recipient to provide access to certain CDR data to the consumer or other accredited persons. This is termed "principle of reciprocity", which imports elements of fairness and allows consumers to request access to or transfer of additional datasets. The principle of reciprocity may apply in three circumstances: (a) where an entity is included in a designation instrument but there is not a consumer data rule requiring that data holder to disclose that information; (b) where an accredited data recipient is not included in the designation but holds data that it has generated or collected itself outside of the CDR regime; and (c) where the ACCC writes rules requiring accredited data recipients to disclose data that they have received through the CDR regime to another accredited person at the consumer's request.[44]

(3) Privacy safeguards

46 The security and integrity of the CDR regime is currently maintained by 13 privacy safeguards. These safeguards are legally binding statutory obligations, and the specific requirements for certain privacy safeguards are set out in the CDR rules. At this juncture, it is important to point out that the Australian Privacy Act 1988 continues to remain in force, and the

---

43 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at para 1.104.

44 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at paras 1.122–1131 generally.

Australian Privacy Principles[45] ("APPs"), a principles-based law that makes up the framework for the Australian Privacy Act, apply to a certain extent.

47 These safeguards are set out in the table below alongside some accompanying details.[46] Some observations on the possibility of there being similar adoptions under the Singapore approach are also appended below.

S/N	Privacy safeguard	Description of coverage of safeguard and limitation	Possibility of a similar safeguard for Singapore?
1.	Open and transparent management of CDR data	• To provide consumers with the ability to inquire or complain about the manner in which their CDR data is being handled by a CDR participant, all data holders, accredited data recipients and designated gateways, must have policy, procedures and systems in place that ensure compliance with the CDR regime and management of CDR data. • For easy access, the CDR privacy policy must be made available free of charge and in an appropriate form: for example, online or in a booklet which can be sent to a CDR consumer or other participant.	May be more limited in scope if this is implemented in the data portability regulations. In particular, it is unlikely that there will be extra impositions on porting organisations in Singapore, apart from the usual data protection obligations that would now also have to cover data being ported.
2.	Anonymity and pseudonymity	• Generally, a CDR consumer will be provided with the option of utilising a pseudonym if that is considered appropriate for	Probably unlikely for an individual to have the option to choose a pseudonym, unless this is the system or

45 Privacy Act 1988 (Cth) Sch 1.

46 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at paras 1.308–1.381 generally.

		the sector. In this respect, it is possible for a CDR consumer to interact anonymously or pseudonymously with a CDR participant and yet still be reasonably identifiable from the circumstances, unless the CDR rules specify otherwise.[47] • This does not apply to data holders or a designated gateway. The Australian Privacy Act and APPs will apply to data holders.	methodology applied by the porting organisation anyway.
3.	Seeking to collect CDR data from CDR participants	• Collection of CDR Data can be done in accordance with the CDR regime if the CDR consumer has given a valid request accordingly. Collection can be made directly from another CDR participant or via a designated gateway. • An accredited person can collect data for other purposes if it is allowed by another law but must not purport that the collection is being made under the CDR regime. • Contravention of this safeguard may be subject to a civil penalty.	Apart from the role played by a designated gateway, which concept does not exist in Singapore's approach, this safeguard will more likely be incorporated into Singapore's data portability regime in that a valid request has to be made to trigger the porting transaction.

47 The Explanatory Memorandum to the Treasury Laws Amendment (Consumer Data Right) Bill 2019 clarifies that the Government would not expect that a consumer could use a pseudonym when exercising their consumer data right in the banking sector. A consumer cannot typically engage with the banking sector without identifying themselves.

4.	Dealing with unsolicited CDR data	• An accredited person cannot retain unsolicited CDR data except if required to do so under an Australian law or by order of a court or tribunal, regardless of whether the accredited data recipient collected the data via a designated gateway or directly from a data holder. • Contravention of this safeguard may be subject to a civil penalty.	It is unlikely that there will be unsolicited data collected in the first place that is not already in contravention of the PDPA. Accordingly, anything akin to this safeguard is unlikely to be addressed further for Singapore.
5.	Notifying of the collection of CDR data	• If an accredited person collects data in accordance with Safeguard 3 above, it must advise the CDR consumer about the collection of such data. • Contravention of this safeguard may be subject to a civil penalty.	The requirement to notify data subjects (regarding collection, use and/or disclosure) is already part of the Consent, Purpose Limitation and Notification obligations. These obligations are inevitably extended to cover ported data as well.
6.	Use or disclosure of CDR data	• An accredited data recipient must not disclose CDR data unless disclosure is required under the CDR rules in response to valid consent by the consumer.[48] A designated gateway must not use CDR data unless the use is authorised by CDR rules or	Proper regulations on disclosure under data portability are awaited. Nevertheless, from a conceptual perspective, this safeguard is similar to the fundamental requirements expected of a porting

48 It is emphasised that consumer consent for use of their consumer data right ("CDR") data, including subsequent disclosure, is at the heart of the CDR system. See Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at para 1.332.

		is required or authorised by another Australian law (except the APPs) or a court of tribunal. • Further, use or disclosure of CDR data is only allowed if it is consistent with a requirement of authorisation under the CDR rules. • An accredited data recipient and/or a designated gateway must make a written note where it uses or discloses the CDR data under an Australian law or an order of a court or tribunal. • Contravention of this safeguard may be subject to a civil penalty.	organisation – that is, to port over only when a consumer requests.
7.	Use or disclosure of CDR data for direct marketing by accredited data recipients and designated gateways	• Use of CDR data for direct marketing purposes is not permitted unless authorised or required by the CDR rules and specifically consented to by the CDR consumer. • This does not apply to use of CDR data in the hands of the original data holder, which would be required to comply with APPs in relation to direct marketing. • Contravention of this safeguard may be subject to a civil penalty.	Consent is needed before direct marketing can be done to an individual. As such, this is similar to the Australian approach.
8.	Overseas disclosure of CDR data by accredited data recipients	• An overseas entity may be able to be accredited; thus, disclosure of CDR data may occur to accredited data recipients located outside of Australia.	Accreditation in order to be allowed to port data is not a requirement in Singapore. This is one of the major conceptual

		• Accreditation is deemed as sufficient protection to ensure that the accredited persons (even if overseas) would not breach the safeguards. • If an overseas entity is not accredited, disclosure is still possible if the accredited data recipient takes reasonable steps to ensure the recipient does not breach the relevant privacy safeguards. Otherwise, the accredited data recipient must believe that the recipient is subject to a law or scheme that provides at least the equivalent protections as the privacy safeguards and the CDR consumer will be able to enforce those protections. • Contravention of this safeguard may be subject to a civil penalty.	differences between both countries' approaches to data portability.
9.	Adoption or disclosure of government-related identifiers by accredited data recipients	• Government-related identifiers are not permitted to be used by an accredited data recipient as an identifier of a CDR consumer who is an individual or for disclosure to be made. • The exception is where the use is allowed under an Australian law (other than the CDR rules), an order of a court or tribunal, or where APPs apply. • The above limitation does not apply where the CDR consumer is not an individual.	To the extent that government-related identifiers include Singapore's national registration identification card ("NRIC") numbers, there will probably be some divergence from the Australian approach. It is anticipated that the forthcoming data portability regulations will address the treatment of NRIC in further detail.

		• Contravention of this safeguard may be subject to a civil penalty.	
10.	Notifying of the disclosure of CDR data	• Applies to data holder as well as accredited data recipient. • Where a data holder or accredited data recipient has disclosed CDR data consistent with the CDR rules, it must notify the consumer as required. • Obligation to notify applies even if disclosure was made via a designated gateway. • Contravention of this safeguard may be subject to a civil penalty.	The requirement to notify data subjects (regarding collection, use and/or disclosure) is already part of the Consent, Purpose Limitation and Notification obligations. These obligations are inevitably extended to cover ported data as well.
11.	Quality of CDR data	• Applies to data holder as well as accredited data recipient. • Where disclosure of CDR data is made, the data holder or accredited data recipient must ensure that it is accurate, up to date and complete for the purpose for which it is held. • APPs relating to quality of personal information do not apply to a data holder who is subject to this safeguard. • Contravention of this safeguard may be subject to a civil penalty.	The current data protection obligations under the PDPA do not address "quality" of data *per se*. Nevertheless, it is implicit that user-provided data ought to be correct and complete. There is an overlap with the requirement listed below under Privacy Safeguard 13. For user-generated data, it is probably implicit as well for such data to be correct and complete to meet the justifications of data portability in Singapore.
12.	Security of CDR data and	• Onus is on accredited data recipients and designated	The requirement to protect data is already

	destruction or de-identification of redundant CDR data	gateways to ensure that CDR data is protected from misuse, interference and loss as well as from unauthorised access, modification or disclosure. • Further, if CDR data is no longer needed for the purposes permitted by the CDR rules or for the purposes as allowed under the CDR regime, then the redundant data must be destroyed or de-identified according to the CDR rules. • Exceptions apply if a person is required to keep the data under an Australian law (aside from the APPs) or as a result of an order of a court or tribunal. • Contravention of this safeguard may be subject to a civil penalty.	part of the Protection Obligation. On the other hand, the Retention Limitation Obligation would already deal with data that is no longer required for the purposes collected. These obligations are inevitably extended to cover ported data as well.
13.	Correction of CDR data	• The CDR consumer has correction rights for CDR data that has been disclosed by a data holder. APPs relating to correction of personal information do not apply to a data holder who is subject to this safeguard. • The data holder must correct the data when requested, or include a statement with the data to ensure that the purpose for which it is held is accurate, up to date, complete and not misleading. • The data holder must also give a statement about the	The requirement to correct data and ensure that it is correct, complete and up to date is already part of Access and Correction as well as Accuracy obligations. The obligations are inevitably extended to cover ported data as well.

		correction or why a correction was not necessary. • The above also applies to accredited data recipients when CDR consumers request for data to be corrected. • Contravention of this safeguard may be subject to a civil penalty.	

48 As evident from the comparison of the various safeguards, some aspects will definitely diverge from the Singapore approach. For instance, Privacy Safeguard 2 was provided for given the privacy landscape in Australia, which prioritises a consumer being able to choose the extent to which one is identifiable by an accredited person. It was found that there can be benefits to anonymity and pseudonymity because consumers may be more likely to inquire about products and services under the CDR regime if they are able to do so without being identified, and the risk of a data breach is reduced as less consumer data is collected.[49] It may not be immediately intuitive as to why this is important in a data portability relationship. Accordingly, it is useful to consider some given examples of when this safeguard would be useful, including when asking for the consumer's consent to collect, use and/or disclose their CDR data; providing a consumer with a consumer dashboard; communicating with the consumer (for example, when providing a CDR receipt to the consumer or notifying of collection under Privacy Safeguard 5; using the consumer's CDR data to provide the requested goods or services to the consumer, and the consumer electing that their redundant data be deleted under CDR rules.[50]

49 Another difference as shown is Privacy Safeguard 8, which deals with overseas disclosure where an overseas data recipient is accredited as well. Accreditation appears unique to Australia when compared to other jurisdictions featured in this article. Under the Singapore approach, porting and receiving organisations need only comply with several data protection

49 Office of the Australian Information Commissioner, *Consumer Data Right: Privacy Safeguard Guidelines* (Version 3.0, June 2021) at paras 2.9 and 2.10.

50 Office of the Australian Information Commissioner, *Consumer Data Right: Privacy Safeguard Guidelines* (Version 3.0, June 2021) at para 2.14.

obligations and the upcoming regulations, but there is no need for accreditation. Under the EU approach, in contrast, there is some form of framework for porting and receiving organisations to adhere to. However, the Australian approach goes further to require local entities to be accredited first, and accreditation is also extended to foreign entities. This underscores the kind of quality control that the authorities have sought to undertake, which is usually left to private parties to self-govern in the other jurisdictions.

50 Penalties for misconduct under the CDR can be significant and serve as a deterrent against treating misconduct and penalties as a mere cost of doing business. Where the offence is committed by a body corporate, the offence is punishable by a fine of either AU$10m, up to three times the value of the benefit gained from committing the offence, or 10% of the annual turnover of the body corporate. On the other hand, where the offence is committed by a person other than a body corporate, the offence is punishable by no more than five years' imprisonment or a fine of not more than AU$500,000, or both.

51 Other enforcement and remedies are extended to the CDR regime. For instance, the ACCC can make orders and awards relating to pecuniary penalties, injunction, damages, adverse publicity orders or even to disqualify a person from managing corporations, amongst many others.[51]

52 It would thus appear that Australia's approach to data portability obligations is one which is consumer-centric, and the regime is highly regulated. The extent of enforcement actions that can be taken by the authorities would also underscore the gravity of the CDR regime in Australia. It undoubtedly sends a strong message to all on how important the right to collect, use and/or disclose information relating to consumers within the CDR parameters is, and is one that all parties ought to be prepared for before embarking on such privilege.

(4) Extraterritoriality of consumer data right

53 The CDR regime has been created to apply both within and outside Australia. For CDR data held within Australia, obligations apply regardless

51 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at para 1.406.

of nationality. For CDR data held outside of Australia, there only needs to be some nexus to Australia (*eg*, acts or omissions by or on behalf of an Australian person, or an Australian person likely to suffer financial or other disadvantage).[52] A diagrammatic illustration of the extraterritorial operation of the CDR regime can be found in the Explanatory Memorandum to the Treasury Laws Amendment (Consumer Data Right) Bill 2019.[53]

54 It is clear that the anticipated data portability right in Singapore does not go beyond its shores. In this respect, the Australian approach may be more akin to the EU's instead. This is understandable given the legislative history of Australian privacy laws and frameworks which has created deep-rooted privacy principles and fundamentals into Australian society. In contrast, Singapore's first foray into data protection is its PDPA, which was borne out of very different considerations.

55 The above study of the Australian approach also shows what could happen in an alternate reality if the Singapore approach were also consumer-driven. Whilst sectors become heavily regulated, the consumer would also need to be more sophisticated to fully appreciate the options presented to oneself.

C. *Canada*

(1) Bill C-11 – Consumer Privacy Protection Act

56 Bill C-11, also known as the Digital Charter Implementation Act 2020[54] (or "Digital Charter"), is an Act to enact the CPPA[55] and the Personal Information and Data Protection Tribunal Act. It is also intended to repeal parts of the Personal Information Protection and Electronic

52 Competition and Consumer Act 2010 (Cth) s 56AO(3).

53 Treasury Laws Amendment (Consumer Data Right) Bill 2019, Explanatory Memorandum at para 1.154.

54 Bill C-11 was first read on 17 November 2020.

55 The Consumer Privacy Protection Act is enacted as an Act to support and promote e-commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities.

Documents Act[56] ("PIPEDA") and cause other consequential and related amendments to other Acts.[57]

57 There are ten principles of the Digital Charter, one of which deals with portability. In particular, the fourth principle states: "Transparency, Portability and Interoperability: Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden."[58] Data portability therefore falls under this fourth principle.

58 The stated purpose of the CPPA is:[59]

> … to establish – in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information – rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Similar to the other jurisdictions, this frames the CPPA as striking a balance between the interests of individuals, and the needs, presumably including commercial needs, of organisations.

---

56 SC 2000, c 5.

57 Other legislations that are affected include the Access to Information Act (RSC, 1985, c A-1); Aeronautics Act (RSC, 1985, c A-2); Canada Evidence Act (RSC, 1985, c C-5); Canadian Radio-television and Telecommunications Commission Act (RSC, 1985, c C-22); Competition Act (RSC, 1985, c C-34); Canada Business Corporations Act (RSC, 1985, c C-44); Public Servants Disclosure Protection Act (SC 2005, c 46); Chapter 23 of the Statutes of Canada, 2010; and Transportation Modernization Act (SC 2018, c 10).

58 Innovation, Science and Economic Development Canada, "Canada's Digital Charter: Trust in a Digital World" *Government of Canada* (12 January 2021).

59 Bill-C11 cl 5.

(2) Present entrenchments versus *the Consumer Privacy Protection Act*

59 It is said that, in theory, Canadian data subjects already have "clear and manageable access" to their personal data.[60] For instance, under s 8 of the PIPEDA, one may make requests to private sector businesses to have access to personal information. When dealing with federal government institutions and agencies, a right of access is provided under s 12 of the Privacy Act.[61] Upon reading these provisions, it would be quite clear that they are in spirit very similar to s 21 of the PDPA. It is arguable that such right of access would naturally allow for a data subject to be "free to share or transfer [personal data] without undue burden".[62] However, what these provisions therefore do not cover is the mechanism or the possibility of porting over personal data from one organisation to another. In other words, the prospect of ease of transfer is not dealt with.

60 Accordingly and under the heading of "Mobility of Personal Information", the CPPA aims to address the above scenario more expressly. Section 72 of the CPPA deals with data mobility right and is reproduced as follows:

> **Disclosure under data mobility framework**
> **72** Subject to the regulations, on the request of an individual, an organization must as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations.

(3) Scope of data mobility right

61 Is there then a difference between data *portability* and data *mobility*? A report produced from a private organisation's Data Mobility Infrastructure Sandbox[63] suggests that there could be a conceptual

---

60 British Columba Freedom of Information and Privacy Association, "The Right to Data Portability" (20 January 2020) <https://fipa.bc.ca/the-right-to-data-portability/> (accessed December 2021).

61 RSC, 1985, c P-21.

62 Canada's Digital Charter Principle 4.

63 In 2019, a UK-based organisation, Ctrl-Shift, created the Data Mobility Infrastructure Sandbox to bring together businesses, consumers and consumer organisations, government, regulators, and data facilitators to collaborate on

(*continued on next page*)

difference between the two, and specifically that data mobility goes beyond data portability. In this respect, the report found that with data mobility, personal data flows safely and efficiently to where it can create maximum value. These flows are controlled by the individual ensuring that personal, social and economic benefits are distributed fairly, in contrast to data portability where processes tend to be done manually and on an *ad hoc* basis.[64] It is noted as well that the same private organisation had separately indicated that unless data is mobile – available immediately, delivered via application programming interfaces rather than via a one-off batch transfer, and structured in a genuinely interoperable format rather than just machine-readable one – much of the value cannot be realised.[65] At this juncture, it is not quite clear whether Canada's data *mobility* right (if one were to use the terminology of s 72 of the CPPA) or data *portability* right (if relying on the wording of the fourth principle as used in the Innovation, Science and Economic Development Canada's ("ISEDC's") report) are anything but interchangeable terms. It would further appear that in ISEDC's 2019 paper[66] ("PIPEDA Modernization paper"), the main motivation of the Canadian government is to introduce new data mobility

addressing data mobility-related issues, within an independent, facilitated environment. Sandbox participants include Barclays, the British Broadcasting Corporation, British Telecom, Centrica, Facebook and digi.me, as well as other independent observers. See Ctrl-Shift, *Data Mobility Infrastructure Sandbox: Report* (June 2019).

64 Ctrl-Shift, "Personal Data Protection Commission, Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions: Response from Ctrl Shift" (17 July 2019) <https://www.pdpc.gov.sg/Guidelines-and-Consultation/2019/05/Public-Consultation-on-Data-Portability-and-Data-Innovation-Provisions/Responses-Received-on-17-July-2019> (accessed December 2021).

65 Ctrl-Shift, "Personal Data Protection Commission, Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions: Response from Ctrl Shift" (17 July 2019) <https://www.pdpc.gov.sg/Guidelines-and-Consultation/2019/05/Public-Consultation-on-Data-Portability-and-Data-Innovation-Provisions/Responses-Received-on-17-July-2019> (accessed December 2021).

66 Innovation, Science and Economic Development Canada, "Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronic Documents Act" *Government of Canada* (21 May 2019).

opportunities to enhance individuals' control over information by providing an explicit right for individuals to direct that their personal information be moved from one organisation to another in a standardised digital format, where such a format exists. Even though at the time of writing this article the enabling regulations have yet to become available, it is doubtful as to whether the Canadian government had intended for the data mobility right under s 72 of the CPPA to go beyond what data portability is understood to stand for.

62 It is notable that the key elements[67] to Canada's data mobility right involve the following aspects:

(a) that it is the individual that directs the sharing;

(b) that personal information ought to be shared as soon as feasible;

(c) that a data mobility framework should first be in place prior to inter-organisation sharing; and

(d) that the information subject to the mobility right would probably be restricted to the personal information that the organisation has collected from the individual.

63 Two main differences between Canada's and Singapore's approaches that can be observed at this juncture would be the existence of a data mobility framework as well as the type of data that can be ported over. With respect to the former, it would appear that the porting organisation in Singapore would probably be subjected to the usual data protection obligations including ensuring reasonable technical arrangements are in place, without more. This is unlike what is expected of a porting organisation in Canada, which would have had to additionally establish a data mobility framework in accordance with the anticipated requirements and regulations, though it is yet unclear what these are at the moment. In respect of the type of data that can be ported over, Singapore's approach appears to go beyond simply what data has been collected by the porting organisation and includes user generated data.

67 Kirsten Thompson & Tracy Molino, "CPPA: An In-depth Look at the Data Mobility Provisions in Canada's Proposed New Privacy Law" *Dentons Data* (19 January 2021).

64 It would be interesting to see the final materialisation of Canada's data mobility right once the CPPA is in force and enabling regulations are released.

IV. Conclusion

65 Data portability is shaping up to be a tenet of data protection and privacy and no jurisdiction can mature in this realm without incorporating data portability as a right into its data protection and privacy regime. It may also be an opportunity for some degree of harmonisation across jurisdictions on the data formats.

66 The EU has included this right into its GDPR, but without giving it special rights above and beyond the others. Australia, on the other hand, has, it seems, carved it out separately in another legislation apart from its primary privacy law. It is also evident that the Australian approach is complex, with heavy regulations surrounding the data portability regime and interactions with existing privacy laws, but, without a doubt, pro-consumer at its core.

67 In contrast, the Canadian approach, which is a work in progress at the moment, seems to be a cautious endeavour to delicately balance competing objectives, and yet remain accountable to the wishes of the Canadian public. Singapore's data portability right is similarly still at its inception stage today. Although efficiency and pragmatism bolster its development, comfort can be taken from the fact that the virtues of trust and reliability in safeguarding and moving personal data are still upheld.

68 An area of concern for organisations/controllers operating in multiple jurisdictions is potential compliance costs involved if different solutions have to be implemented in response to different data formats and technical and process requirements needed to comply with data portability obligations. This presents an opportunity for regulators and stakeholders to harmonise their approach to and recognition of common data formats, potentially lowering barriers to entry for market entrants and access to customers and customer data.

DATA LITIGATION: PRACTICAL AND LEGAL DIFFICULTIES IN THE RIGHT OF PRIVATE ACTION*

Janice GOH
LLB (National University of Singapore)

Sarah HEW
LLB (National University of Singapore)

TAN Tian Yi
BA (Jurisprudence) (Oxford), LLM (Harvard)

I. Introduction

1 Section 48O of the Personal Data Protection Act 2012[1] ("PDPA") encapsulates the right of private action against an individual or organisation for a breach of the PDPA. While this statutory right[2] offers claimants a cause of action against wrongdoers, it has not been popular among claimants. Since the enactment of the PDPA in 2012, there have only been two reported decisions in Singapore which discuss s 32 of the previous enactments of the PDPA,[3] *ie*, the predecessor of s 48O.

2 By contrast, data litigation is common and has gained significant traction in other common law and European jurisdictions. Many of these litigation matters are high-profile class actions. For example, in 2020 itself, a significant number of data claims were issued in the English courts. Following British Airways' announcement in 2018 that there had been a breach of its security systems leading to more than 500,000 customers' data being leaked, claimants have issued claims which could be worth up to

---

* Any views expressed in this article are the authors' personal views only and should not be taken to represent those of their employer. All errors remain the authors' own.

1 Act 26 of 2012.

2 First enacted as s 32 of the Personal Data Protection Act 2012 (Act 26 of 2012).

3 See *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 and *IP Management Pte Ltd v Alex Bellingham* [2019] SGDC 207.

£3bn.[4] In *Lloyd v Google LLC*,[5] a representative action on behalf of an estimated 4.4 million individuals (at £750 per individual), Google's potential liability was for £3.3bn, excluding costs. After a data breach affecting Starwood Hotels' guest reservation database led to the loss of 300 million individuals' data, an action has been commenced against Marriott International which could cost it £1.7bn.[6]

3 In this article, the authors discuss the reasons this cause of action has not gained popularity with claimants in Singapore. In addition, the authors explore the possibility of claimants bringing representative actions for data breaches under O 15 r 12 of the Rules of Court.[7] In the authors' view, the overarching reason for the scarcity of private civil actions commenced pursuant to the PDPA is a *cultural* one. Prior to 2021, a private civil action could only be commenced by natural persons (and not companies) or "data subjects". Data protection and data privacy laws in Singapore are relatively new, and attitudes towards data privacy in the general population are still developing. Just not too many years ago in the 1990s or early 2000s, there still existed publicly available telephone directories called *Yellow Pages*, where one could search for a specific individual's telephone number and residential address.

4 In addition to overarching cultural reasons, there are also other *practical* and *legal* difficulties that claimants may face in seeking recourse under s 48O of the PDPA. These include, *inter alia*, proof and valuation of loss and damage, costs of litigation, uncertainty of the law and the availability of other remedies. However, as the jurisprudence on data protection law develops, and the general population's attitude towards data privacy matures, the authors are of the view that personal data litigation in Singapore may well become more common in the years to come.

---

4 Ellen Milligan, "British Airways Faces Biggest Class-action Suit over Data Breach" *Bloomberg* (13 January 2021).

5 [2019] EWCA Civ 1599.

6 Joanna Partridge, "Marriott International Faces Class Action Suit over Mass Data Breach" *The Guardian* (19 August 2020).

7 Cap 322, R 5, 2014 Rev Ed.

II. Right of private action under section 48O of the Personal Data Protection Act

5 Section 48O of the PDPA gives any person who suffers "loss or damage", as a result of contraventions of certain provisions in the PDPA, a right of action for relief in civil proceedings in a court. Such action may be brought against an organisation or "persons", which include natural persons and individuals, as well as corporate bodies.[8] Recent case law has also confirmed that it is a statutory tort.[9] Further, as the learned authors of "Civil Proceedings under the Personal Data Protection Act 2012"[10] observed, such a right of private action is not unusual from a data protection perspective, with similar rights of private action having been included in new US consumer privacy legislation, and in European data protection legislation.

6 The right of private action under s 48O of the PDPA complements the Personal Data Protection Commission's ("PDPC's") investigative and regulatory powers, as the PDPC is not empowered to award damages or other relief to a complainant.[11] While the right of private action was previously only available to individual "data subjects", *ie*, natural persons, it has been recently extended to organisations and public agencies that suffer direct loss or damage arising from contraventions of the new business-to-business obligations in the amended PDPA.[12]

---

8 See s 2 of the Interpretation Act (Cap 1, 2002 Rev Ed).

9 See *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [49]: "Section 32(1) PDPA is described as a right of private action but I agreed with Mr Liu that it creates a statutory tort."

10 Alexander Yap *et al*, "Civil Proceedings under the Personal Data Protection Act 2012" [2020] PDP Digest 154 at 157, para 5.

11 Personal Data Protection Commission, *Advisory Guidelines on Enforcement of the Data Protection Provisions* (revised 1 February 2021) at para 34.3.

12 *Parliamentary Debates, Official Report* (2 November 2020), vol 95 "Second Reading Bills: Personal Data Protection (Amendment) Bill" (S Iswaran, Minister for Communications and Information):

> The new section 48O under clause 23 of the Bill updates the current right of private action by a person who suffers loss or damage directly as a result of a breach of the data protection provisions. The right of private action will be extended to organisations and public agencies that suffer direct loss

(*continued on next page*)

A. Breaches of the Personal Data Protection Act which would give rise to potential action under section 48O

7 A private action under s 48O of the PDPA may be commenced against an organisation where the organisation contravenes any provision of Part IV, V, VI, VIA or VIB of the PDPA. Broadly speaking, these sections of the PDPA set out, *inter alia*:

(a) prohibitions against the collection, use and/or disclosure of personal data without consent;

(b) statutory requirements governing the access to and correction of personal data;

(c) statutory requirements relating to the care of personal data, *ie*, the accuracy, protection, retention and transfer of personal data outside Singapore;

(d) statutory requirements relating to "data porting"; and

(e) statutory requirements surrounding the notification of data breaches.

8 The action may also be brought against a person who breaches any provision of Division 3 of Part IX, or Part IXA of the PDPA. These sections of the PDPA prohibit, *inter alia*, sending advertising or promotional messages to telephone numbers listed in the Do Not Call Registry, as well as the use of dictionary attacks and address-harvesting software. This means that *individuals* may now be sued in a private civil action under s 48O of the PDPA for breaches of specific provisions in the PDPA; *eg*, sending advertising or promotional messages to telephone numbers listed in the Do Not Call Registry.

9 Previously, s 32 of the PDPA provided that: "Any person who suffers loss or damage directly as a result of a contravention of any provision in Part IV, V or VI *by an organisation* shall have a right of action for relief in civil proceedings in a court" [emphasis added].

B. Loss or damage

10 In order to commence a private action under s 48O of the PDPA, a claimant needs to show that he or she suffered "loss or damage". While

---

or damage arising from contraventions of the new business-to-business obligations in the Bill.

the PDPA does not contain statutory definitions of the concepts of "loss" or "damage", a recent Singapore High Court decision confirmed that these concepts were to be understood narrowly with reference to the usual common law understanding of loss and damage such as pecuniary loss, damage to property and personal injury.

11 In *Bellingham, Alex v Reed, Michael*[13] ("*Alex Bellingham (HC)*"), the court considered the loss or damage required for a private action to be brought against an organisation for a breach of the PDPA. While this matter was decided under s 32 of the PDPA in force as of 2018, the reasoning is equally applicable to s 48O of the present PDPA, which broadens the scope of the right of private action under s 32 of the PDPA.

12 In *Alex Bellingham (HC)*, the issue was whether "loss or damage" includes emotional distress and loss of control over personal data, or whether it should be interpreted narrowly to refer to the heads of loss or damage under common law (pecuniary loss, damage to property, personal injury, *etc*).[14]

13 Having surveyed relevant legislative provisions in Canada, New Zealand, Hong Kong and the UK, the court noted that the data protection legislation in those jurisdictions contained express references to some form of emotional harm (humiliation, loss of dignity, injury to feelings and distress). By comparison, in Singapore, Parliament decided to refer only to "loss and damage" in s 32(1) (now s 48O) of the PDPA, without any reference to any form of emotional harm or loss of control over personal data. The court found this suggestive of parliamentary intention to *exclude* emotional harm and loss of control over personal data.

14 The court also observed that the policy rationales underlying the PDPA in Singapore were distinct from those in New Zealand, Hong Kong, the European Union ("EU") and the UK, where data protection laws are driven primarily by the need to recognise the right to privacy. In this regard, the court agreed that the PDPA was not driven by a recognition of the need to protect personal privacy as an absolute or fundamental policy. Instead, the purpose of the PDPA was "as much to enhance Singapore's competitiveness and to strengthen Singapore's position as a trusted business

13 [2021] SGHC 125.

14 *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [43].

hub as it was to safeguard individuals' personal data against misuse".[15] This is an important distinction which the court articulated, and which should be borne in mind when interpreting the PDPA. It also echoes the overarching *cultural* factors and attitudes which were outlined above.[16]

C. Private action can only be commenced after conclusion of the Personal Data Protection Commission's action

15 However, the right of private action is subject to the limitation in s 48O(2) of the PDPA:

> [i]f the Commission has made a decision under this Act in respect of a contravention specified in [s 48O(1)], an action accruing under [s 48O(1)] may not be brought in respect of that contravention until after the decision has become final as a result of there being no further right of appeal.

This means that if the PDPC has made a decision on the breach, a private action *cannot* be commenced until the PDPC's action has concluded and there are no further avenues of appeal.

D. Reliefs sought

16 Where a breach is established, the innocent party may commence civil proceedings seeking all or any of the following reliefs: (a) relief by way of injunction or declaration; (b) damages; or (c) any further relief as the court may deem fit.[17]

III. Practical and legal reasons that may deter claimant from relying on section 48O

17 Since s 32 of the PDPA was enacted, there have only been two reported cases arising from the same fact pattern. As mentioned above,[18] there are *cultural* reasons why the right of private action under the PDPA has not gained traction in Singapore.

---

15 *Bellingham, Alex v Reed, Michael* [2021] SGHC 125 at [73].

16 See para 3 above.

17 Personal Data Protection Act 2012 (Act 26 of 2012) s 48O(3).

18 See para 3 above.

18 In the authors' opinion, besides these broad *cultural* factors, there are practical and other legal reasons that may deter potential claimants from relying on s 48O. These include, *inter alia*, the difficulties with valuation of loss, the litigation costs involved in suing the wrongdoer, the uncertainty in this area of law, the availability of other causes of action, *etc*.

A. Locus standi*: Prior to 2021 amendments, section 32 of the Personal Data Protection Act (equivalent of section 48O) did not allow for private actions to be commenced by organisations*

19 *First*, prior to the recent round of amendments to the PDPA, s 32 of the PDPA (the equivalent of the amended s 48O) did not allow for private actions to be instituted by organisations. In *IP Investment Management Pte Ltd v Alex Bellingham*,[19] *ie*, an application brought by an investment management firm under s 32 of the PDPA arising from the alleged disclosure of certain investors' personal data by a former employee, the District Court disallowed the application on the ground that s 32 of the PDPA does *not* give a right of action to parties other than the data subject, *ie*, the person to whom the personal data has been misused relates.[20]

20 Section 48O of the PDPA now allows for companies to commence action for the breach of business-to-business data obligations.[21] Therefore, an increasing trend in such actions going forward is expected.

B. Difficulties with proof and valuation of loss and/or damage

21 Further, as explained above,[22] a claimant (or group of claimants) who commences a private action under s 48O of the PDPA must demonstrate that he has suffered loss or damage, being pecuniary losses, damage to property, personal injury, *etc*. Heads of damage which are not generally recognised under the common law (*eg*, emotional distress) will not suffice as legal and factual grounds for a private action under s 48O of the PDPA.

---

19 [2019] SGDC 207.

20 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [111].

21 See para 6, n 13 above.

22 See para 9 above.

22 This is in contrast to the heads of damage that have been allowed under the EU General Data Protection Regulation[23] ("GDPR"), the primary data protection legislation in the EU and UK. Article 82 of the GDPR allows a person who has suffered "material or non-material damage" to obtain monetary compensation, and several EU national courts have interpreted "non-material damage" as including emotional distress, anxiety and stress.[24] In fact, s 168 of the UK Data Protection Act 2018,[25] which supplements the GDPR in the UK, expressly specifies that "non-material damage" in Art 82 of the GDPR "includes distress". Further, in the US, claimants may be awarded punitive damages.

23 On the other hand, potential claimants face inherent difficulties in proving loss or damage, and in the valuation of such loss and/or damage in light of the traditional interpretation of loss and damage which would apply to private actions in Singapore under s 48O of the PDPA.

24 To begin with, it is relatively rare for easily identifiable pecuniary losses to be suffered as a result of personal data breaches. Taking a simple scenario of a personal data leak of one's passport number, for example, it would be difficult to prove that the data breach caused actual pecuniary loss or damage to property, unless, for instance, such data was used by a fraudster to commit fraud or identity theft, and caused actual financial loss to the data subject.

25 In *Grinyer v Plymouth Hospitals NHS Trust*,[26] decided under the UK Data Protection Act 1998[27] ("DPA 1998"), the court awarded the claimant compensation for pecuniary loss of earnings of £4,800, treatment costs of £1,434 and some nominal travel costs, consequent on the exacerbation of the claimant's serious mental health condition caused by breaches of the DPA 1998. However, this was a case on its unique facts involving a

23 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

24 See the Austrian case authority of *OLG Innsbruck* – 1 R 182/19b (13 February 2020).

25 c 12.

26 [2012] EWCA Civ 1043.

27 c 29.

patient's claim against a National Health Services trust after a nurse had improperly accessed his medical records over a period of four and a half years.

26 In general, the authors remain of the view that on a personal and individual level, loss and damage for breach of the obligations under the PDPA is difficult to establish and, even if proven, is potentially difficult to quantify.

27 However, in light of the most recent amendments to the PDPA which now allow for a private right of action under s 48O for the breach of *business-to-business* data obligations,[28] such recourse may well be more attractive to businesses who, as a result of data breaches committed by their vendors who provide data storage or processing services (such as cloud computing) or other third parties, suffer measurable loss and damage (likely in the form of pecuniary losses associated with reputational damage).

28 That being said, it remains to be seen whether the s 48O private action will indeed become more popular amongst corporate claimants, as such litigants will still need to overcome the obstacles conventionally associated with the valuation of loss and damage, in particular, losses due to reputational harm.

C. Costs of litigation, uncertainty of the law, availability of other alternative causes of action

29 In addition to the challenges surrounding the proof and valuation of loss and damage, the costs of litigation may also discourage potential claimants from commencing a private action under s 48O of the PDPA where the law in this area is relatively new and therefore uncertain. For individual claimants, the loss and damage suffered, even if measurable, may not justify the costs of litigation. Even if an individual claimant takes the view that litigation is preferable on a cost-benefit analysis, he or she may instead decide to pursue more well-established causes of action at law, such as breach of contract (if available), breach of confidence or general negligence under common law.

---

28 See n 12 above.

30 That being said, as mentioned above,[29] with the most recent amendments allowing for corporates to commence civil actions under s 48O of the PDPA for breaches of business-to-business data obligations, there may well be an increase in such actions in future, given that such corporates have greater access to funds and resources for litigation, and are more incentivised to pursue such litigation in light of the higher economic stakes at play.

31 As the authors of "Civil Proceedings under the Personal Data Protection Act 2012" observed,[30] extending the application of a private action to companies could "practically enhance a company's right to collect, use and disclose personal data since this would give companies greater recourse in the event of loss or damage arising directly from a breach of the PDPA by a third party (hacker)". Moreover:

> … [t]he availability of civil proceedings as an avenue of protection from loss or damage arising from a third party's breach of the PDPA may lower the risk of having to absorb such loss or damage themselves, or at least allow their insurers some measure of recovery.

32 As data protection laws and the regulatory framework continue to mature, the financial consequences of data breaches may become more significant, and result in a greater number of such litigation actions.

IV. Representative actions for data breaches in Singapore

33 In this part, the authors explore the possibility of representative actions for data breaches in Singapore.

34 While Singapore does not have an established class-action regime akin to that in the US or Australia, the Singapore civil procedural rules do allow for the commencement of "representative proceedings". Under O 15 r 12(1) of the Rules of Court, where "numerous persons" have the "same interest in any proceedings", such proceedings may be begun and, unless the court otherwise orders, continued, by or against any one or more of them as representing all or as representing all except one or more of them.

---

29 See para 25 above.

30 Alexander Yap *et al*, "Civil Proceedings under the Personal Data Protection Act 2012" [2020] PDP Digest 154 at 164, para 23.

35 Order 15 r 12(3) further provides:

> A judgment or order given in proceedings under this Rule shall be binding on all the persons as representing whom the plaintiffs sue or, as the case may be, the defendants are sued, but shall not be enforced against any person not a party to the proceedings except with the leave of the Court.

36 Despite the availability of representative proceedings under the civil procedural rules, representative actions are relatively rare in the Singapore context. Since 2013, there have only been two representative actions which have been allowed to proceed in the Singapore courts. In this regard, Singapore courts typically adopt a two-stage approach in deciding whether a representative action should be allowed to proceed – *first*, whether the persons have the "same interest" in the proceedings; and *secondly*, whether the circumstances of the case justify continuing the proceedings as a representative action.

37 In *Koh Chong Chiah v Treasure Resort Pte Ltd*,[31] the court applied a strict test to the "same interest" requirement in holding that members of a country club who had become members of the club at different times and under different arrangements would not have the "same interest" in the proceedings.

38 The court also observed that although representative actions offered a practical and economical method of asserting and enforcing a claim, this had to be weighed against prejudicial consequences for the defendant in a representative action. Further, the court ought to strive to strike a balance between the interests of parties bearing in mind the purpose of the O 15 r 12 regime, which was to facilitate access to and the efficacious administration of justice.[32]

39 Moreover, representative proceedings will only be allowed where there are "numerous persons" with the same interest in the proceedings, either as plaintiffs or defendants. In *Syed Nomani v Chong Yeow Peh*,[33] the Singapore High Court dismissed an application to convert court proceedings to a "representative action" where there were only 11 potential defendants. The

---

31 [2013] 4 SLR 1204.

32 *Koh Chong Chiah v Treasure Resort Pte Ltd* [2013] 4 SLR 1204 at [34]–[36] and [38].

33 [2017] 4 SLR 1064.

court held that while there was no minimum number as to what constituted "numerous persons" in O 15 r 12(1), as there were only 11 potential representative defendants, representative proceedings would not have led to significant procedural efficiency.[34]

40 In theory, it is possible for data litigation proceedings to be commenced pursuant to the representative proceedings framework envisaged under O 15 r 12 of the Rules of Court, read together with s 48O of the PDPA. However, it is unclear to what extent such actions will gain popularity in Singapore, given the limited uptake of representative proceedings to begin with (as compared to class-action lawsuits in the UK, EU and US) and the lack of support or platforms that encourage claimants to form a class, as well as the relative novelty of data protection law in Singapore.

41 Singapore's limited uptake of representative proceedings is more apparent when contrasted with the proliferation of representative actions for data breaches that have been brought in the UK, EU and US in recent years.

42 Since the introduction of the GDPR, the number of representative actions that have been brought for data breaches in the UK and EU has increased. There are several reasons for this. *First*, the GDPR confers greater rights upon its data subjects and provides them with a clear basis for legal claims. *Second*, the increase in class-action data lawsuits under the GDPR involving high-profile companies in recent years has also led to greater awareness amongst data subjects.[35]

43 While the increase in class-action data lawsuits in the UK and EU is a relatively recent phenomenon, class-action lawsuits have long provided consumers in the US with a means to obtain redress in cases where individual suits would be inefficient or impractical.[36] This may be attributed to the fact that the US has long adopted an opt-out framework for class-action lawsuits, *ie*, *all persons falling within the represented class form part of the litigation without having to elect to join, and are only excluded if they opt out*. This makes bringing data protection actions worthwhile, as it

34 *Syed Nomani v Chong Yeow Peh* [2017] 4 SLR 1064 at [14].

35 See para 2 above.

36 See Federal Trade Commission, *Consumers and Class Actions: A Retrospective and Analysis of Settlement Campaigns* (September 2019).

inadvertently secures the participation of as many potential claimants as possible, which would render the potential sum of damages large enough to merit the costs of bringing the action, and maximise the value of the action.[37] This also eases the administrative difficulty of commencing a class-action lawsuit, as claimants do not have to identify and enlist willing litigants to commence the representative action.

44 By contrast, in Singapore, all potential claimants must opt in to join the representative proceedings to obtain redress, *ie*, *they must take proactive steps to join the claim*. This means that potential litigants would need to identify sufficient claimants who are willing to participate in the representative proceedings.

45 Further, contingency fee arrangements are permitted in the US but not in Singapore. This reduces any upfront financial costs which class-action litigants in the US need to be responsible for. Conversely, in Singapore, given that contingency fee arrangements are prohibited, the upfront costs of litigation may well discourage potential claimants from participating in representative proceedings, including any representative proceedings arising from data breaches.

V. Conclusion

46 In conclusion, it is unlikely that data class-action lawsuits will gain significant popularity in Singapore in the near future, as Singapore's data protection laws lack the features that UK and US data protection legislation possess, and which make representative actions more accessible and efficient for claimants.

47 As the parliamentary reports demonstrate, the PDPA is meant to increase Singapore's attractiveness as a business/data hub and is not targeted specifically at the protection of individuals' rights to privacy. This is as opposed to the US, UK and the EU, whose notions of data privacy appear to be based on the concept of individual rights to privacy. From a broader economic perspective, and in line with Singapore's public policies, it would be in Singapore's interests to ensure that appropriate safeguards are in place to prevent data class actions from gaining popularity, as the proliferation of data class actions could lead to increased business risks and costs. This may

37 Federal Rules of Civil Procedure (US) rule 23.

result in Singapore becoming a less attractive destination for businesses, especially those which regularly handle large volumes of personal data.

WHISTLE-BLOWING SYSTEMS: BALANCING LEGITIMATE CORPORATE GOVERNANCE INTERESTS AND DATA SUBJECT RIGHTS*

Carren THUNG
LLB (Hons) (Singapore Management University);
CIPP/A, CIPP/E; Advocate and Solicitor (Singapore)

1 Whistle-blowing systems have long been seen as an internal mechanism of choice to root out illegal practices or policy breaches. In the US, the adoption of the Sarbanes-Oxley Act[1] in 2002 imposed requirements for companies to establish internal procedures for the receipt and processing of confidential, anonymous concerns regarding "questionable accounting or auditing matters".[2] Other jurisdictions such as Australia, Canada, Malaysia and New Zealand have also enacted national whistle-blower legislation. Singapore has yet to see overarching corporate whistle-blowing legislation; however, for specific types of illegal conduct there are statutes such as the Prevention of Corruption Act[3] and the Workplace Safety and Health Act[4] that provide for the protection of whistle-blowers.[5]

2 Since then, the adoption of whistle-blowing systems has gained global popularity as a means by which a company can demonstrate transparency and a commitment to corporate governance. While they are most often thought of as internal controls against illegal accounting practices, money-laundering or corruption, the scope of a whistle-blowing policy can encompass various types of deleterious conduct. To cite a non-exhaustive list, companies in recent years have set up whistle-blowing systems to

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent those of her employer. All errors remain the author's own.

1 Pub L 107–204, 116 Stat 745 (30 July 2002).

2 Sarbanes–Oxley Act of 2002 (Pub L 107–204, 116 Stat 745 (July 30, 2002)) § 301.

3 Cap 241, 1993 Rev Ed.

4 Cap 354A, 2009 Rev Ed.

5 Prevention of Corruption Act (Cap 241, 1993 Rev Ed) s 36; Workplace Safety and Health Act (Cap 354A, 2009 Rev Ed) s 18(2)(*b*).

receive reports of employee harassment, abuses of power, fraud, malpractice, anti-competitive conduct, racial or gender discrimination, and even practices that may result in environmental harm.

I. Interplay with the Personal Data Protection Act

3 Whistle-blowing systems typically centre around two tenets: (a) the assured confidentiality of the whistle-blower; and (b) the protection of the whistle-blower against retaliatory measures. The rationale is obvious; an employee is more likely to report illegal conduct once assured protection against reprisal. To encourage participation, whistle-blowing policies often allow whistle-blowers to make their reports anonymously. If the whistle-blower chooses to reveal their identity to the organisation, the organisation will undertake not to inform the accused employee of the whistle-blower's identity without the whistle-blower's consent.[6]

4 The information provided to the organisation in a whistle-blower's complaint constitutes personal data as it would in most cases record or describe the actions of identifiable individuals. Apart from describing the accused employee's actions in the workplace, whistle-blowing reports could include documentary evidence such as forwarded correspondence, screenshots or photographs taken without the data subject's knowledge.

5 While generally accepted as a necessary component of corporate governance, whistle-blowing systems nonetheless trigger concerns from a data protection perspective. The collection, use or disclosure of an employee's personal data without the consent of the employee is neither required nor authorised by any written law. Therefore, to collect or use such data for the purpose of a whistle-blowing system, an organisation would need to obtain the consent of its employees or rely on an exception in the Personal Data Protection Act 2012[7] ("PDPA").

6 Organisations collecting personal data through whistle-blowing channels are likely to argue that the employees had consented to the collection of their data (and in turn, the submission of their personal data to the organisation by anonymous whistle-blowers). In *Re German*

---

6 See Singapore Institute of Directors, *Statement of Good Practice: Whistleblowing Policy* (SGP No 13/2014) at paras 2 and 3.5.

7 Act 26 of 2012.

European School Singapore,[8] it was found that parents of students attending a school had impliedly consented to the school's collection of students' hair samples for drug testing; the school had outlined its practice of random drug testing and the consequences of a positive test in its by-laws and the parents had consented to abide by the school's by-laws at the time of the students' enrolment.[9] Therefore, an organisation should clearly communicate to employees the existence of their whistle-blowing policy and set out with specificity how personal data contained in whistle-blower reports is processed.[10] As a matter of best practice, it should also require all new joiners to confirm they consent to their collection of their data for the purposes of the same.

7 However, this approach has limitations, as the organisation may not be able to comprehensively predict and explain to employees the circumstances in which potential whistle-blowers may collect and disclose data to the organisation. In addition, an employee may want to withdraw his consent, citing privacy concerns. The organisation could attempt to argue that imposing a requirement to obtain the consent of an employee to an anonymous whistle-blowing scheme is unreasonable (and therefore supports a defence under s 11(1) of the PDPA) as many would opt out if they had the option, thereby undermining the efficacy of the channel. However, there could be counter-arguments that having such a channel is neither a necessary nor desirable tenet of an organisation's governance, particularly where it is not mandated by statute or where employees are not in trust-critical roles that would warrant invasive surveillance.

8 Alternatively, an organisation would need to be able to rely on an exception in the First and Second Schedules to the PDPA in order to receive and process reports pertaining to that employee.

A. Necessary for investigation or proceedings

9 An organisation is not obliged to seek the consent of the subject of a whistle-blower's complaint if the collection, use or disclosure of personal

8 [2020] PDP Digest 198.

9 *Re German European School Singapore* [2020] PDP Digest 198 at [16]–[26].

10 See also Monetary Authority of Singapore, *Code of Corporate Governance* (6 August 2018) at para 10.1(f).

data contained in the complaint is necessary for any investigation or proceedings. Interestingly, the terms "investigation" and "proceedings" are specifically defined in the PDPA as that which relates to (a) a breach of an agreement; (b) a contravention of any written law, rule of professional conduct, or other requirement imposed by any regulatory authority; or (c) a wrong or breach of duty that may result in a remedy or relief becoming available under any law. This suggests that the exception would only apply to complaints pertaining to breaches that are clearly actionable in law, as opposed to isolated incidents that may not amount to a codified offence, such as a failure to use best practices or abide by industry standards that do not have the force of law. Hence, broader practices that do not restrict the subject matter of the complaints may not benefit from this exception.

B. Necessary for evaluative purposes

10 Alternatively, the processing of data received through a whistle-blower's report without the accused employee's consent could be deemed to be necessary for an evaluative purpose, and therefore permissible under Item 2 of Part 3 of the First Schedule to the PDPA.

11 However, the PDPA defines an "evaluative purpose" in an employment context as "determining the suitability, eligibility or qualifications of an individual"[11] for (a) employment or appointment to office; (b) promotion or continuance of employment; or (c) removal from employment or office. This does suggest that the exception does not allow the organisation to use the collected data to evaluate if an employee ought to face disciplinary measures other than termination or the denial of a promotion.

C. Legitimate interests of the organisation

12 The organisation could also assert that the collection, use or disclosure of personal data through whistle-blowing reports is in the legitimate interests of the organisation and its stakeholders and therefore allowable under para 1 of Part 3 of the First Schedule to the PDPA. The identification and prevention of illegal acts or other unsalutary behaviour is

11 Personal Data Protection Act 2012 (Act 26 of 2012) s 2.

undoubtedly a legitimate interest of the organisation. However, in order to rely on this exception, the organisation must also conduct an assessment to determine if its legitimate interests outweigh any adverse effect on the potential accused employees and provide its employees with reasonable access to information about the whistle-blowing procedures and how their personal data may be collected, used or disclosed.[12] Over and above this, the PDPA obliges the organisation to identify and implement reasonable measures to eliminate, reduce the likelihood of or mitigate any adverse effects on the accused employees.[13]

13 It is therefore relevant to consider the types of harm to the data subject rights of accused employees that could result from the misuse of whistle-blowing systems, and how they might be avoided.

II. Interaction with data subject rights

14 In 2006, the European Union's ("EU's") Working Party set up under Art 29 of Directive 95/46/EC[14] to deal with issues relating to the protection of privacy and personal data ("WP29") released an advisory opinion on how internal whistle-blowing schemes ought to be implemented to comply with European data protection rules.[15] The opinion noted that there was a real likelihood that employees named in anonymous, confidential whistle-blowing reports would face "stigmatisation and victimisation" even before they were aware that they had been incriminated.[16]

15 The same considerations continue to be relevant today.

---

12 Personal Data Protection Act 2012 (Act 26 of 2012) First Schedule, Part 3, Items 1(2)(*a*) and 1(2)(*b*).

13 Personal Data Protection Act 2012 (Act 26 of 2012) First Schedule, Part 3, Items 1(3)(*a*) and 1(3)(*b*).

14 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (repealed).

15 See Article 29 Data Protection Working Party, *Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight against Bribery, Banking and Financial Crime* (00195/06/EN, 1 February 2006) (hereinafter "WP29 2006 Opinion").

16 WP29 2006 Opinion at p 7.

(a) **Lack of consent and notification**. In most cases, the whistle-blower's collection and disclosure of the accused employee's personal data to the organisation would take place outside of the accused employee's knowledge. While the accused employee may be aware of their employer's whistle-blowing policy and the possibility of having their actions reported to the investigating committee by co-workers, the information contained within the whistle-blowing report could extend to actions or communications taking place outside of the context of the workplace. For example, allegations of intra-employee harassment or bribery often describe actions taking place outside of working hours or in a more casual context in which the accused employee might not reasonably expect to be subject to surveillance by their employer (*eg*, "[Employee] was seen behaving inappropriately with a vendor's relative at a club two weeks ago").

The accused employee would not be aware of the submission of the complaint unless and until informed by the organisation. The organisation's investigating committee may withhold knowledge of the complaint from the accused employee to protect the whistle-blower from reprisals where the identity of the whistle-blower can be easily inferred from the circumstances described in the complaint. In other cases, the organisation may also choose not to inform the accused employee of the investigation in the initial stages of the investigation in order to facilitate the gathering of evidence.

(b) **Limitations on accuracy, rights of access and rectification**. Anonymous whistle-blowing schemes raise concerns of the potential of abuse by bad actors. The Singapore Institute of Directors advises that often whistle-blower reports "lack sufficient detail to warrant a full investigation or may even be false information" and that to counter this, "confidential investigations must first be carried out to establish whether there is any evidence to support the whistle-blower allegations. Where this is not possible, then the specific issue reported can be monitored".[17] Naturally, if the anonymous complaint does not contain sufficient information to support the charge at first instance, there would be difficulties in verifying the substance of the allegations during the confidential investigation or to ask follow-up questions.

17 Singapore Institute of Directors, *Statement of Good Practice: Whistleblowing Policy* (SGP No 13/2014) at para 3.6.

The organisation may be constrained to investigate the issue for a prolonged period without informing the accused employee of the existence of the complaint if doing so could compromise the integrity of the investigation. The accused employee would not be able to access information relating to the investigation while it is ongoing, which would in turn restrict her ability to correct any factual inaccuracies in the complaint. If a significant amount of time has passed before the accused employee is informed of the complaint, it is likely that she would experience difficulty gathering the necessary evidence to refute the allegations, particularly if the source of the complaint is anonymous.

(c) **Retention and purpose limitations**. If the organisation decides that there is insufficient basis upon which to proceed with a disciplinary hearing or other measures, there would rightly be concerns as to if (or when) the complaint ought to be expunged from the accused employee's record or if it is permissible for the organisation to retain the information on file indefinitely for its internal audit requirements and/or for evaluative purposes.

16 Unfortunately, many whistle-blowing policies adopted by local organisations do not go beyond catering for the confidentiality and protection of the whistle-blower. While such protections are necessary and laudatory, the confidential nature of the whistle-blowing process would create a potential for disproportionate risk to the data subject rights of the accused employees if the parameters of the whistle-blowing policy are not clearly defined.

III. Mitigating measures and best practices

17 Attempts at enunciating best practices for organisations implementing whistle-blowing schemes have been made by institutions such as the Singapore Institute of Directors and the Singapore Exchange Regulation ("SGX RegCo").[18] However, such efforts are largely focused on the protection and incentivising of whistle-blowers. More could be done to

18 See Singapore Institute of Directors, *Statement of Good Practice: Whistleblowing Policy* (SGP No 13/2014) and Singapore Exchange Regulation, *Consultation Paper on Enhancements to Enforcement and Whistleblowing Frameworks* (6 August 2006) Appendix 3.

guide organisations in identifying measures to prevent undue harm to the interests of employees incriminated through whistle-blowing complaints.

18 Some guidance may be obtained from the deliberations and initiatives of EU states.

A. Deadline to inform accused employee of existence of complaint and rights of access and rectification

19 Articles 12 and 14 of the General Data Protection Regulation[19] ("GDPR") obliges data controllers to provide to data subjects information relating to the collection of their personal data within one month of the collection of the data. Such information would include the purposes for which the data will be processed, the recipients of the data, the period for which the data will be stored, the source of the data, as well as the existence of the employee's right to access, rectify and/or request erasure of the data.[20]

20 In 2016, the European Data Protection Supervisor ("EDPS") confirmed that the GDPR obliges organisations to inform employees implicated in a whistle-blowing report. However, the organisation should decide on a case-by-case basis if provision of specific information may need to be deferred; for example, if it can be proven that giving the accused employee access to the data collected would compromise the investigation or undermine the rights and freedoms of others. Any such reasons ought to be documented before the decision to restrict or defer access is taken.[21]

B. Restriction on areas or categories of persons subject to whistle-blowing system

21 In 2006 the WP29 recommended that organisations consider limiting the number of persons eligible to make whistle-blower reports, or the classes of persons that could be the subject of a whistle-blower's report, taking into

19 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR").

20 GDPR Arts 12(3) and 14(3).

21 European Data Protection Supervisor, *Guidelines on Processing Personal Information within a Whistleblowing Procedure* (July 2016) at para 20.

consideration the seriousness of the alleged offences to be reported.[22] It also advised that organisations setting up whistle-blowing systems clearly define the type of information to be submitted by whistle-blowers, and limit submissions to those relating to the fields of accounting, auditing, financial crime and anti-bribery concerns. If submissions related to a concern falling outside this scope, the WP29 suggested that they be forwarded to more appropriate channels.[23]

22 Initially, the French Data Protection Authority, the Commission nationale de l'informatique et des libértes ("CNIL"), adopted an Expedited Approval Procedure granting pre-approval to automated processing whistle-blowing procedures, provided that such procedures related only to a restricted number of areas such as finance, accounting practices, banking and anti-bribery concerns.[24] Post adoption, the CNIL and French courts have on several occasions invalidated corporate whistle-blowing policies for exceeding the scope of the pre-approval procedure.[25] In 2019, the CNIL released a new standard ("2019 standard"), which now envisages organisations receiving whistle-blowing reports pertaining to a wider range of areas, such as the organisation's own charter or internal code of ethics. However, the organisation would need to demonstrate a legitimate interest in implementing a system that goes beyond its statutory obligations.[26] The organisation would need to explicitly state in its whistle-blowing policy all the subject areas that the whistle-blowing system is meant to target and to

22 WP29 2006 Opinion at p 10.

23 WP29 2006 Opinion at p 12.

24 Autorisation Unique n°AU-004 (8 December 2005).

25 Dassault Systemes, Civil Supreme Court (8 December 2009). See generally Commission nationale de l'informatique et des libertés, *Guideline Document Adopted by the "Commission nationale de l'informatique et des libertés" (CNIL) on 10 November 2005 for the Implementation of Whistleblowing Systems in Compliance with the French Data Protection Act of 6 January 1978, as Amended in August 2004, Relating to Information Technology, Data Filing Systems and Liberties* (10 November 2005) (hereinafter "CNIL 2005 Guidelines"). See also Commission nationale de l'informatique et des libertés, *Activity Report 2011*, "Ethical Business Alert (Whistleblowing)" at pp 46–48.

26 Commission nationale de l'informatique et des libertés, *Référentiel Relatif Aux Traitements de Donnees a Caractere Personnel Destines a la Mise en Œuvre d'un Dispositif d'Alertes Professionnelles* (18 July 2019) (hereinafter "CNIL 2019 Standard") section 3 at p 4.

distinguish the subject areas required by law, from those voluntarily adopted by the organisation.[27]

23 The German Data Protection Authorities ("DPAs") stated in their advisory opinion on whistle-blowing hotlines that receiving whistle-blowing reports pertaining to the traditional subject areas such as financial irregularity, accounting or auditing matters, corruption, human rights violations and ethical concerns were permissible. Additionally, reports of discrimination would also be permissible under Art 6(1)(f) of the GDPR in so far as such concerns could result in claims for damages and cause reputational harm for the organisation.[28]

24 However, it advised that reports pertaining to other areas such as violations of an internal code of conduct or "soft factors" ought to be admitted only on a case-by-case basis taking into account employment law principles, and whether there is an identifiable connection between the alleged violation and harm to the company.[29]

C. *Discouragement of anonymous reports*

25 Prior to the implementation of the GDPR, the WP29 took the position that anonymous reporting ought to be discouraged as anonymity prejudiced an organisation's ability to ask follow-up questions, and could potentially create a culture of anonymous, malevolent reports thereby harming the social climate within the organisation. It was also considered that anonymity would not prevent the accused employee from inferring the identity of the whistle-blower and would in fact detract from the organisation's ability to protect the whistle-blower from retaliation even if such protections were guaranteed by law.[30]

---

27 See CNIL 2019 Standard section 3 at p 4, Example 3.

28 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, *Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines* (14 November 2018) (hereinafter "DSK 2018 Guidelines") section D 3.2 at p 5.

29 DSK 2018 Guidelines section D 3.2 at p 6.

30 WP29 2006 Opinion at pp 10–11.

26 In its *Guidelines on Processing Personal Information within a Whistleblowing Procedure*,[31] the EDPS reiterated that in principle, whistle-blowers ought to be encouraged to identify themselves, both to avoid abuse of the procedure and to better enable the organisation to ensure the effective protection of the whistle-blower.[32] More recently, the CNIL has clarified that while anonymous whistle-blower alerts ought to be treated with special caution, the admittance of the alert ought not to be made conditional on the identification of the author of the alert.[33]

27 In this respect, the German DPAs' position has been the subject of some controversy. The Datenschutzkonferenz's *Guidelines for Whistle-blowing Hotlines*[34] interpret Art 14 of the GDPR as imposing an obligation on organisations operating whistle-blower schemes to reveal the identity of the whistle-blower (if the report is not anonymous) to accused employees within one month of receipt of the whistle-blower's report.[35] Organisations may only postpone doing so if disclosure would (a) compromise the investigation; (b) breach an obligation of professional secrecy in written law; or (c) be overridden by the legitimate interests of a third party.[36] This stance encourages anonymous reporting. If a whistle-blower is minded to reveal her identity to the organisation, the organisation would have to inform her that her identity would eventually be disclosed to the accused employee. The whistle-blower would be entitled to revoke her consent up to one month after the submission of the report,[37] which helps to mitigate the chilling effect that this would otherwise have. However, commentators have noted that this is often too short a time for the whistle-blower to avoid identification.[38]

---

31 July 2016.

32 European Data Protection Supervisor, *Guidelines on Processing Personal Information within a Whistleblowing Procedure* (July 2016) at para 12.

33 CNIL 2019 Standard section 5.4 at p 6.

34 14 November 2018.

35 DSK 2018 Guidelines section E 3 at p 9.

36 DSK 2018 Guidelines section E 4.1 at p 10.

37 DSK 2018 Guidelines section E 3 at p 9.

38 Baker & McKenzie, "GDPR – German Data Protection Authorities Establish New Rules for Whistleblowing Hotlines: Call for Action – Update" (January 2019) at p 3.

D. Restrictions on handling of reports

28 The WP29 advised that organisations carefully consider how whistle-blowing reports are collected and handled. If an internal committee is set up to process the reports, such committee should be strictly separated from other departments of the company, and the data contained within reports should only be transmitted to those persons within the committee. The persons comprising such a committee, as well as any third-party service providers, should be specifically trained and bound by contractual confidentiality obligations.[39]

E. Limitation on retention of data in reports to that which is relevant, accurate and non-excessive.

29 In its 2005 Guidelines,[40] the CNIL advised that the medium through which whistle-blowing reports are received should only collect data formulated in a format that directly relates to the scope of the scheme such that only relevant data is recorded. Further, the format ought to expressly state that the facts described are merely alleged at the time of recording.[41] The CNIL further advised that the organisation clearly state in its policies that any abuse of the whistle-blowing procedure would result in disciplinary proceedings and/or judicial proceedings, although complaints would not result in sanctions if made in good faith.[42]

30 In its 2019 standard, the CNIL further advised that personal data collected through whistle-blowing reports found to be irrelevant ought to be destroyed without delay. If no action is taken on a report, the data ought not to be stored more than two months from the close of an investigation

---

39 WP29 2006 Opinion at p 15. See also European Data Protection Supervisor, *Guidelines on Processing Personal Information within a Whistleblowing Procedure* (July 2016) at paras 8 and 32–35.

40 Commission nationale de l'informatique et des libertés, *Guideline Document Adopted by the "Commission nationale de l'informatique et des libertés" (CNIL) on 10 November 2005 for the Implementation of Whistleblowing Systems in Compliance with the French Data Protection Act of 6 January 1978, as Amended in August 2004, Relating to Information Technology, Data Filing Systems and Liberties* (10 November 2005).

41 CNIL 2005 Guidelines at p 5.

42 CNIL 2005 Guidelines at p 5.

unless it is necessary to store such data for future disciplinary or legal proceedings, or if a legal obligation to archive such data applies. If the organisation chooses to retain such data, such as for business improvement purposes, it ought to take steps to anonymise the data.[43]

IV. Conclusion

31 The implementation of a robust whistle-blowing system will be increasingly expected of corporations of all sizes. In December 2019, the EU issued a new directive requiring member states to enact national laws compelling all companies comprising more than 50 employees to implement whistle-blowing protocols and to provide protection for *bona fide* whistle-blowers.[44] Strides are being made locally as well. In August 2020, SGX RegCo called for a public consultation on its proposal to code into the Mainboard Rules and Catalist Rules requirements for issuers to include a statement addressing its compliance with best practices on whistle-blowing in their annual reports. Regrettably, the list of best practices identified in the consultation paper is limited and largely confined to the protection of whistle-blowers.[45]

32 It is to be expected that more corporations will choose to adopt their own whistle-blowing procedures in order to maintain consistency with their international counterparts and comply with best practices. While there may be a temptation to keep the system as broad and inclusive as possible, companies should be reminded to assess if they have the means to adequately safeguard data protection rights and if the systems are proportionate to their needs. Whistle-blowing systems would have more legitimacy if organisations can assure stakeholders that the systems are well thought out and that incriminated employees would be treated fairly and accorded due process. To this end, authoritative guidance on relevant

43 CNIL 2019 Standard sections 7.1 and 7.2.

44 See Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law Art 8.

45 Singapore Exchange, *Consultation Paper: Enhancements to Enforcement and Whistleblowing Frameworks* (6 August 2020) Part III at pp 9–11. See also Appendix 3.

considerations and best practices on safeguards to implement can only be welcome.

MCI (P) 053/02/2022