(2022) 23 SAL Ann Rev 245
(Published on e-First 14 April 2023)

11. CONFIDENTIAL INFORMATION AND DATA PROTECTION

Benjamin **WONG**
LLM (London School of Economics),
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore);
Lecturer, Faculty of Law, National University of Singapore.

I. Confidential information

A. Uday Mehra v L Capital Asia Advisors – *Litigation exception – Equitable remedies*

11.1 *Uday Mehra v L Capital Asia Advisors*[1] ("*Uday Mehra*") was a General Division of the High Court ("High Court (General Division)") case involving ex-employers suing an ex-employee for breach of confidence.

11.2 The first and second defendants were members of a group of companies ("the LCA Group") involved in the business of private equity funds. The plaintiff was an employee of the LCA Group. In 2015, the plaintiff's employment was summarily terminated by the LCA Group for insubordination and misconduct. The plaintiff sued the defendants and made a number of claims against them.

11.3 The LCA Group counterclaimed against the plaintiff for breach of confidence in equity. In their counterclaim, the LCA Group alleged that the plaintiff had forwarded several e-mails from his work e-mail account to his personal e-mail account. These e-mails had been received by the plaintiff in the course of and for the purposes of his employment, and were forwarded without the knowledge or consent of the LCA Group.

11.4 The High Court held that the plaintiff had breached his obligation of confidence towards the LCA Group. The High Court found that the e-mails did contain confidential information and were sent to the plaintiff by the LCA Group in circumstances importing an obligation of confidence.[2] The plaintiff breached this obligation of confidence by forwarding the e-mails to his personal e-mail account.[3]

1 [2022] 5 SLR 113. This case was decided on 28 January 2022.
2 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [254].
3 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [257].

11.5 There are two notable aspects of *Uday Mehra*.

11.6 First, the High Court appears to have eliminated a "litigation exception" that was previously established in *Leong Hin Chuee v Citra Group Pte Ltd*[4] ("*Leong Hin Chuee*"). In *Leong Hin Chuee*, the High Court had held that it was not a breach of confidence for an obligor to disclose confidential information "for the purposes of legal proceedings" against the obligee.[5] The plaintiff in the present case sought to rely on *Leong Hin Chuee*, submitting that it was not a breach of confidence for him to have copied the confidential information and disclosed the same to his solicitors in order to use that information in litigation against the defendants.

11.7 The High Court rejected the plaintiff's submission for two reasons. First, *Leong Hin Chuee* was inconsistent with the later cases of *LVM Law Chambers LLC v Wan Hoe Keet*[6] ("*LVM*") and *I-Admin (Singapore) Pte Ltd v Hong Ying Ting*[7] ("*I-Admin*") in which the Court of Appeal had recognised that the obligee has a wider range of legitimate interests beyond merely the interest in preventing detrimental misuse.[8] Second, the position taken in *Leong Hin Chuee* was "against the weight of authority" as there were English cases reaching the opposite conclusion.[9] The High Court favoured the English position, pointing out that the position in *Leong Hin Chuee* was tantamount to permitting an employee to take his employer's confidential information whenever he faced potential proceedings against his employer.[10]

11.8 Second, the High Court made it clear that, in a claim for breach of an equitable obligation of confidence, the only remedies available are equitable remedies, and those equitable remedies are granted at the court's discretion.[11] The remedial burden of proof is on the party seeking the equitable remedies, and it is entirely possible that the court will choose not to award any of the remedies sought, despite a finding of breach of confidence. In the instant case, for example, the LCA Group failed to persuade the High Court to award any of the equitable remedies sought for the plaintiff's breach of confidence.[12]

4 [2015] 2 SLR 603.
5 *Leong Hin Chuee v Citra Group Pte Ltd* [2015] 2 SLR 603 at [228]–[229].
6 [2020] 1 SLR 1083.
7 [2020] 1 SLR 1130.
8 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [263].
9 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [264].
10 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [265].
11 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [248].
12 *Uday Mehra v L Capital Asia Advisors* [2022] 5 SLR 113 at [268]–[273].

B. Lim Oon Kuin v Rajah & Tann LLP – *Test for breach of confidence*

11.9 *Lim Oon Kuin v Rajah & Tann LLP*[13] ("*Lim Oon Kuin*") was a Court of Appeal case involving an application for an injunction to restrain a law firm from acting for certain clients.

11.10 The appellants were Lim Oon Kuin ("OK Lim"), Evan Lim Chee Meng ("CM Lim") and Lim Huey Ching ("HC Lim") (collectively "the Lims"). The Lims were the key management figures of two related companies ("the Companies"), namely, Hin Leong Trading (Pte) Ltd ("HLT") and Ocean Tankers (Pte) Ltd ("OTPL"). In 2020, the Lims and the Companies appointed the respondent law firm ("R&T") to advise them on insolvency matters. Shortly after that, both Companies were placed under interim judicial management, and then subsequently under judicial management. R&T continued to act for the Companies under judicial management.

11.11 While the Companies were under interim judicial management, CM Lim and HC Lim (who remained directors of the Companies) caused the Companies to apply for injunctions to restrain R&T from advising and acting for the Companies and their judicial managers. It was argued that the injunction applications were necessary to protect confidential information disclosed to R&T by the Lims and the Companies. Later, the Lims applied to be joined as applicants to the injunction applications.

11.12 At first instance, the High Court dismissed the joinder application as there was no basis for the Lims to assert confidentiality over the information in question (and thus no basis for the Lims to be joined as plaintiffs in the injunction applications).[14] The Lims appealed to the Court of Appeal against the High Court's dismissal of their joinder application. The Court of Appeal allowed the Lims' appeal on the basis that it was "just and convenient" to add the Lims to the injunction application proceedings; in this regard, the Court of Appeal found that the Lims did disclose information which appeared to be confidential, although this was "subject to further investigation at trial".[15]

11.13 *Lim Oon Kuin* is an important landmark in the law of confidence because the Court of Appeal also took the opportunity to clarify the test

13 [2022] 2 SLR 280. This case was decided on 4 April 2022 and arose from an appeal against the decision of the High Court (General Division) in *Ocean Tankers (Pte) Ltd v Rajah & Tann Singapore LLP* [2021] SGHC 144.

14 *Ocean Tankers (Pte) Ltd v Rajah & Tann Singapore LLP* [2021] SGHC 144 at [49].

15 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [29].

for breach of confidence. Here, this chapter will briefly summarise the recent developments leading up to *Lim Oon Kuin*, and then discuss the Court of Appeal's opinion in *Lim Oon Kuin*.

11.14 To begin with, the traditional test for breach of confidence has been the test laid out in *Coco v AN Clark (Engineers) Ltd*,[16] comprising three elements to be established by the plaintiff: first, "the information must possess the quality of confidentiality"; second, "the information must have been imparted in circumstances importing an obligation of confidence"; and third, "there must have been some unauthorised use of that information to the detriment of the party from whom the information originated".[17]

11.15 Then, in 2020, the Court of Appeal issued two decisions (namely, *LVM* and *I-Admin*) which appeared to take the law of confidence in different directions. In *LVM*, the Court of Appeal essentially affirmed the traditional test, albeit with a minor modification to the third element in order to adapt the test to the particular issue at hand.[18] In *I-Admin*, on the other hand, the Court of Appeal made a more radical change to the test for breach of confidence. Under the *I-Admin* approach, the first two elements of the traditional test were retained but the third element was removed – instead, upon the plaintiff's satisfaction of the first two elements, there arose a presumption of breach, which the defendant would have to rebut by showing that his conscience was unaffected.[19] The rationale for the *I-Admin* approach was that, whilst the traditional test did safeguard the plaintiff's "wrongful gain interest" (that is, "a plaintiff's interest in preventing wrongful gain or profit from its confidential information"), it did not adequately safeguard the plaintiff's "wrongful loss interest" (that is, "a plaintiff's interest to avoid wrongful loss … which is suffered so long as a defendant's conscience has been impacted in the breach of the obligation of confidentiality").[20]

11.16 In *Lim Oon Kuin*, the Court of Appeal made a number of helpful clarifications about *LVM* and *I-Admin*, drawing from Ng-Loy Wee Loon's incisive commentary in her textbook.[21] First, under the *I-Admin* approach, the defendant's burden of proof when rebutting the presumption of breach was a legal burden and not merely an evidential

16 [1969] RPC 41.
17 *Clearlab SG Pte Ltd v Ting Chong Chai* [2015] 1 SLR 163 at [20].
18 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [35].
19 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [37].
20 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [36]–[37], read with *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [50] and [53].
21 Ng-Loy Wee Loon, *Law of Intellectual Property of Singapore* (Sweet & Maxwell, 3rd Ed, 2021).

burden.[22] Second, the *I-Admin* approach was never intended to replace the traditional test entirely – instead, it was "intended to specifically fill the lacuna in the law in so far as the legitimate objective of protecting the wrongful loss interest was concerned".[23] The third point, which logically follows from the second, is that the *I-Admin* approach was limited to "taker" cases (that is, cases involving the unauthorised acquisition of confidential information).[24]

11.17 Based on the second and third points mentioned in the paragraph above, it is submitted that the test for equitable breach of confidence in Singapore is *bifurcated* as follows: the *I-Admin* approach will apply in "taker" cases involving the unauthorised taking of confidential information, implicating the wrongful loss interest; the traditional test will continue to apply in "misuse" cases involving the unauthorised use of confidential information, implicating the wrongful gain interest.

11.18 This raises the question: what about cases where *both* the wrongful gain interest and the wrongful loss interest are implicated? For example, what if a defendant had surreptitiously and wrongfully taken the plaintiff's confidential information, and then subsequently misused the confidential information to the detriment of the plaintiff? It is submitted that, in such a scenario, the plaintiff should have to apply the tests in a bifurcated fashion: the *I-Admin* approach in relation to the claim for wrongful taking, and the traditional test in relation to the claim for wrongful use. In effect, the plaintiff would be bringing two separate claims, in respect of two separate wrongdoings by the defendant. This also means that it would be up to the plaintiff to decide whether to bring either claim or both claims, and it would be possible for the plaintiff to succeed on one claim but fail on the other.

C. Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern – *Springboard injunctions*

11.19 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern*[25] ("*Pacific Prime*") was a High Court (General Division) case, wherein ex-employers sought injunctions against their ex-employees in order to protect confidential information that had been taken by the ex-employees.

22 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [40].
23 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [39].
24 *Lim Oon Kuin v Rajah & Tann LLP* [2022] 2 SLR 280 at [41].
25 [2022] SGHC 86. This case was decided on 18 April 2022.

11.20 The first plaintiff, Pacific Prime Insurance Brokers Singapore Pte Ltd ("PPIBS"), and the second plaintiff, CXA Insurance Brokers Singapore Pte Ltd ("CXAIBS"), were registered insurance brokers in Singapore. The first defendant, Lee Suet Fern ("Jez"), and the second defendant, Ng Lee Teng Nellie, were senior employees of CXAIBS. In 2021, CXAIBS was acquired by PPIBS. Shortly after this acquisition, Jez and Nellie resigned, and incorporated the third and fourth defendants ("the Afeli Entities"). The Afeli Entities offered services in competition with PPIBS and CXAIBS.

11.21 The plaintiffs commenced proceedings alleging, in particular, that the defendants had exploited confidential information belonging to the plaintiffs. This confidential information included, among other things, client revenue data (in the form of a revenue spreadsheet that contained information about how much revenue the plaintiffs obtained from each client). The plaintiffs applied for a range of injunctions, including injunctions to "restrain the defendants from soliciting any clients from the plaintiffs and the plaintiffs' group of companies" ("the non-solicitation injunctions").[26]

11.22 The defendants argued that the non-solicitation injunctions sought against Jez and the Afeli Entities were really springboard injunctions, and that the High Court should refuse to grant those injunctions because the requirements for the granting of springboard injunctions were not met. Thus, two questions arose for the High Court:

> (a) Did the non-solicitation injunctions constitute springboard injunctions?
>
> (b) If so, were the requirements for the granting of springboard injunctions met?

11.23 On the first question, the High Court found that the non-solicitation injunctions did constitute springboard injunctions. The High Court clarified that an injunction constitutes a springboard injunction when the *purpose* of the injunction is to remove an "unfair competitive advantage arising from a breach of confidence".[27] The plaintiffs were indeed seeking springboard injunctions because the purpose of the non-solicitation injunctions was to stop the defendants from undercutting the plaintiffs' prices using the plaintiffs' confidential client revenue data (thus, the purpose of the non-solicitation injunctions was to remove an

26 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [9].

27 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [15].

unfair competitive advantage enjoyed by the defendants through their misuse of the plaintiffs' confidential information).[28]

11.24 On the second question, the High Court found that the requirements for the granting of springboard injunctions were satisfied. As set out in *Goh Seng Heng v RSP Investments*[29] ("*Goh Seng Heng*"), to obtain a springboard injunction the plaintiff must show that:[30]

> … (a) confidential information had been misused or is at risk of being misused; (b) such misuse of confidential information had given an unfair competitive advantage to the defendant; (c) the 'unfair advantage' was being enjoyed by the defendant at the time the injunction was sought; and (d) damages would be inadequate to compensate the plaintiff ….

11.25 The High Court held that all four requirements were met. First, there was evidence that the client revenue data had been misused; second, the client revenue data gave the defendants an unfair competitive advantage because it would help the defendants to undercut the plaintiffs and thereby poach the plaintiffs' clients; third, this unfair competitive advantage was still being enjoyed by the defendants; and fourth, damages were inadequate to compensate the plaintiffs because there remained a "very significant number of clients" that could still be poached using the client revenue data.[31]

11.26 The High Court, accordingly, granted the springboard injunctions against the defendants, running for six months from the date of judgment, in line with the principle set out in *Jardine Lloyd Thompson Pte Ltd v Howden Insurance Brokers (S) Pte Ltd*[32] that a springboard injunction should "be in place for such time as it would take the wrongdoer to achieve lawfully what he was hoping to achieve unlawfully, relative to the plaintiff".[33]

11.27 The key insight to draw from *Pacific Prime* is that springboard injunctions are not a "separate species of injunction, nor a special legal tool"; rather, the "springboard" label is simply a descriptor of the purpose

28 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [16].
29 [2017] 3 SLR 657.
30 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [15].
31 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [17]–[19].
32 [2015] 5 SLR 258.
33 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [20].

of the injunction.[34] An injunction will be recognised as a springboard injunction – regardless of whether the plaintiff himself labels it as such – as long as the purpose of the injunction is to remove an unfair competitive advantage enjoyed by the defendant by virtue of the defendant's breach of confidence. If an injunction qualifies as a springboard injunction, then the *Goh Seng Heng* requirements must be met by the plaintiff before the court will grant that injunction.

11.28 To avoid having to satisfy the *Goh Seng Heng* requirements, the plaintiff would have to show that the injunction he is seeking is not a springboard injunction – in other words, the plaintiff must successfully argue that the purpose of the injunction is not to remove an unfair competitive advantage. For example, the plaintiff may argue that the purpose of the injunction sought is simply to enforce a contractual non-solicitation obligation (although this argument of course presupposes the existence of such a contractual obligation).

D. Asia Petworld Pte Ltd v Sivabalan s/o Ramasami – *Employee knowledge and skill*

11.29 *Asia Petworld Pte Ltd v Sivabalan s/o Ramasami*[35] ("*Asia Petworld*") was a High Court (General Division) case involving an ex-employer suing its ex-employee for an alleged breach of confidence.

11.30 The plaintiff was a drop shipper of pet products.[36] The plaintiff's business model was essentially to serve as an intermediary between authorised dealers and online retailers. The plaintiff would purchase pet products wholesale from the authorised dealers; then, when customers placed orders with an online retailer, the online retailer would forward those orders to the plaintiff, who would fulfil the orders by sending the ordered products directly to the customers. One of the online retailers who worked with the plaintiff in this way was Sierra Nevada Pet Company ("SNPC").

11.31 The first defendant served as the plaintiff's warehouse manager. He resigned on 28 February 2021, and shortly after his resignation, he worked for the second defendant as its warehouse manager. The second defendant, which was a company established on 16 February 2021 by the first defendant along with a John Robert Foley, provided wholesale

34 *Pacific Prime Insurance Brokers Singapore Pte Ltd v Lee Suet Fern* [2022] SGHC 86 at [15].

35 [2022] 5 SLR 805. This case was decided on 26 May 2022.

36 "Drop shipping" is a business model wherein a retailer does not maintain stock but instead relies on a drop shipper to fulfil customer orders.

supplies to SNPC. From April 2021, SNPC ceased to use the plaintiff's drop shipping services.

11.32 The plaintiff sued the defendants for breach of confidence, among other things. In particular, the plaintiff alleged that the first defendant had misused four categories of information, namely: (a) the plaintiff's supplier information (that is, who the plaintiff's suppliers were); (b) the plaintiff's "true costs" (that is, the prices charged by the plaintiff's suppliers); (c) the plaintiff's cost factoring (that is, how the plaintiff accounted for factors such as freight costs and exchange rate fluctuations); and (d) the plaintiff's fulfilment rate fees (that is, how the plaintiff determined the fees to charge the online retailers).

11.33 In its decision, the High Court found that there was no express confidentiality obligation binding the first defendant. The first defendant was merely bound by an equitable duty of confidence, which was "derived from his implied duty of good faith and fidelity" in his employment contract with the plaintiff.[37] Therefore, the plaintiff would have to prove that the first defendant had breached his equitable obligation of confidence, which would require the plaintiff to prove (among other things) that the information in question was confidential.

11.34 The High Court found that the plaintiff failed to prove that the information in question had the necessary quality of confidentiality for two reasons. First, the information in question did not constitute trade secrets; therefore, while it would have been a breach of the first defendant's implied duty of good faith to disclose the information to a competitor while he was an employee, the information was no longer protectable after he ended his employment with the plaintiff.[38] Second, it is settled law that "the knowledge and experience that an employee acquires during his employment is not protectable confidential information"; in this case, the first defendant's knowledge of the plaintiff's supplier information, true costs, cost factoring and fulfilment rate fees were all knowledge and experience that the first defendant had accumulated in the course of his work for the plaintiff.[39]

11.35 It is useful to consider how the High Court reached the conclusion that the four categories of information were "employee knowledge and skill" that was not protectable. Three factors appeared to be relevant: first (and most importantly), the information was generally acquired by the first defendant in the course of his work (as opposed to

37 *Asia Petworld Pte Ltd v Sivabalan s/o Ramasami* [2022] 5 SLR 805 at [41].
38 *Asia Petworld Pte Ltd v Sivabalan s/o Ramasami* [2022] 5 SLR 805 at [42] and [54].
39 *Asia Petworld Pte Ltd v Sivabalan s/o Ramasami* [2022] 5 SLR 805 at [43] and [54].

having been imparted to him by the plaintiff); second, the High Court emphasised that the information was all contained in the first defendant's memory, and there was no evidence that the first defendant had taken any documents or information from the plaintiff prior to his departure; and third, in relation to the true costs, the High Court noted that this was information that was readily obtainable from the plaintiff's suppliers upon request.[40]

II. Data protection

A. Reed, Michael v Bellingham, Alex – *Employee exemption – Right of private action – Emotional distress*

11.36 *Reed, Michael v Bellingham, Alex*[41] ("*Reed v Bellingham*") is the first data protection case to be decided by the Court of Appeal. This case involved a private action commenced by an individual against an organisation for breach of the Personal Data Protection Act 2012[42] ("PDPA"). The Attorney-General intervened in this case.

11.37 In this case, the appellant ("Reed") was an investor in an investment fund known as the "Edinburgh Fund". The Edinburgh Fund was set up by two related companies, namely IP Investment Management Pte Ltd ("IPIM") and IP Investment Management (HK) Ltd ("IPIM HK"). The respondent ("Bellingham") was a marketing consultant who was employed by IP Real Estate Investments Pte Ltd ("IPRE"). Bellingham was seconded by IPRE to IPIM HK, wherein he was responsible for managing the Edinburgh Fund. In 2017, Bellingham left the employment of IPRE to join Q Investment Partners Pte Ltd ("QIP"), a competing fund management company. While working in QIP, Bellingham e-mailed investors of the Edinburgh Fund (including Reed) regarding investment opportunities with QIP. Reed disagreed with Bellingham's use of his personal data in this way and e-mailed IPIM as well as Bellingham about the matter. This precipitated a series of e-mail communications among the parties before proceedings were commenced against Bellingham.

11.38 IPIM and IPRE commenced proceedings against Bellingham in the District Court, with Reed joining as plaintiff later on. In these proceedings, it was alleged that Bellingham had breached the Consent

40 *Asia Petworld Pte Ltd v Sivabalan s/o Ramasami* [2022] 5 SLR 805 at [45]–[54].

41 [2022] 2 SLR 1156. This case was decided on 9 September 2022 and arose from an appeal against the decision of the High Court (General Division) in *Bellingham, Alex v Reed, Michael* [2022] 4 SLR 513.

42 2020 Rev Ed.

Obligation and the Purpose Limitation Obligation of the PDPA, in relation to Reed's personal data (namely, his name, personal e-mail address and investment activity in the Edinburgh Fund). The proceedings were commenced pursuant to the right of private action under s 32 of the PDPA, which provided that "[a]ny person who suffers loss or damage directly as a result of a contravention of [a data protection obligation] by an organisation shall have a right of action for relief in civil proceedings in a court".[43]

11.39 At first instance, the District Court found that Bellingham had indeed breached both the Consent Obligation and the Purpose Limitation Obligation.[44] The District Court also found that Reed had suffered the requisite "loss or damage" under s 32 of the PDPA.[45] However, the District Court also found that IPIM and IPRE had no standing to bring action under s 32 of the PDPA, since s 32 of the PDPA only conferred a right of private action on the individual whose personal data was concerned.[46] The District Court granted Reed an injunction restraining Bellingham from using, disclosing or communicating Reed's personal data;[47] the District Court also ordered Bellingham to destroy Reed's personal data.[48]

11.40 Bellingham appealed to the High Court against the District Court's decision. The High Court affirmed the District Court's finding that Bellingham had breached the Consent Obligation and the Purpose Limitation Obligation.[49] However, the High Court found that Reed was not entitled to bring private action under s 32 of the PDPA because he had not suffered a relevant "loss or damage".[50]

11.41 Reed then appealed to the Court of Appeal. Three issues were addressed by the Court of Appeal, and the court's answer to each of these issues present important clarifications to certain aspects of the PDPA.

11.42 The first issue was whether s 4(1)(*b*) of the PDPA ("the employee exemption") exempted Bellingham from liability for breaching the PDPA. Section 4(1)(*b*) of the PDPA provides that the PDPA does not impose data protection obligations on "any employee acting in the course of his or her employment with an organisation".

---

43 Note that the right of private action is now provided for under s 48O of the Personal Data Protection Act 2012 (2020 Rev Ed).
44 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [122].
45 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [136].
46 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [110].
47 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [162].
48 *IP Investment Management Pte Ltd v Alex Bellingham* [2019] SGDC 207 at [172].
49 *Bellingham, Alex v Reed, Michael* [2022] 4 SLR 513 [39].
50 *Bellingham, Alex v Reed, Michael* [2022] 4 SLR 513 [92].

11.43 The Court of Appeal clarified that the employee exemption operates as a defence from liability, and the burden of proof is on the defendant to establish that he falls within the scope of the exemption.[51] Further, the Court of Appeal rejected the Attorney-General's argument that the principles of vicarious liability under common law ought to be imported into the interpretation of the employee exemption.[52] As for whether Bellingham could enjoy the employee exemption in the instant case, the Court of Appeal found that he could not because Bellingham had not adduced relevant evidence to prove that he was an employee acting in the course of his employment (relevant evidence would have included "what was done; what the employment required the employee to do and, in appropriate cases, whether the employee deliberately evaded practices set up by the employer to deter such action").[53] While Bellingham might have collected Reed's personal data in the course of his employment with IPRE, he had separately misused the personal data while employed by QIP, and there was insufficient evidence to show that he had misused the personal data *in the course of his employment* with QIP.[54]

11.44 It is notable that the Court of Appeal considered that the burden of proof for the other exemptions under s 4(1) of the PDPA (such as the "personal or domestic capacity" exemption under s 4(1)(*a*) of the PDPA) should rest with the defendant as well.[55] It is submitted, in agreement, that this would lead to a more coherent reading of s 4(1) of the PDPA. Further, it is argued that the other exemptions under s 4 of the PDPA (such as the "data intermediary" exemption under s 4(2) of the PDPA) should be similarly interpreted as placing the burden of proof on the defendant. This is because much of the Court of Appeal's reasoning – in particular, that the employee exemption operates as a defence, and that the relevant evidence for establishing the requirements under the employee exemption would usually be in the hands of the defendant – applies with equal force to the other exemptions under s 4 of the PDPA.[56]

11.45 The second issue was whether the phrase "loss or damage" under s 32 of the PDPA encompassed emotional distress and the loss of control over personal data. This is a question of practical significance because if emotional damage/loss of control over personal data do fall within the meaning of "loss or damage" under s 32 (now s 48O) of the PDPA, then an individual who has suffered emotional damage/loss of control over

51 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [42]–[45].
52 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [46]–[50].
53 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [51].
54 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [53]–[54].
55 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [42].
56 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [42] and [44].

personal data (as a result of a breach of the PDPA) would have standing to sue under s 32 (now s 48O) of the PDPA.

11.46 The Court of Appeal agreed with the High Court's view that s 32 of the PDPA created a statutory tort for breach of the PDPA; however, according to the Court of Appeal, this did not mean that "loss or damage" under s 32 of the PDPA should *ipso facto* be confined to the "actionable heads of loss or damage under common law".[57] To begin with, the Court of Appeal distinguished between statutory torts (which arise from statute) and the tort of breach of statutory duty (which arises from common law) – where statutory torts are concerned, "the scope of the right of action is to be determined first and foremost by the principles of statutory construction", with common law principles taking only a secondary role (if any).[58]

11.47 As a matter of statutory interpretation, the Court of Appeal found that emotional distress clearly did fall within the meaning of "loss or damage" under s 32 of the PDPA:[59] the text and context of s 32 of the PDPA did not suggest that "loss or damage" should exclude emotional distress,[60] and the general purpose of the PDPA and the specific purpose of s 32 of the PDPA were better achieved by reading "loss or damage" as including emotional distress.[61] However, loss of control over personal data could not constitute such "loss or damage":[62] interpreting "loss or damage" as encompassing the loss of control over personal data would render the requirement of "loss or damage" tautologous, since every breach of a data protection obligation would result in a loss of control over personal data.[63]

11.48 Two aspects of the Court of Appeal's decision in respect of the second issue should be highlighted. First, the Court of Appeal clearly affirmed the view that the PDPA was intended to confer "robust protection for individuals' personal data",[64] and this view supported a wide interpretation of s 32 of the PDPA that was more protective of

57 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [62]. See also Lanx Goh & Jansen Aw, "Data Protection Law and Privacy in Singapore" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018).
58 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [65].
59 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [68].
60 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [70]–[85]
61 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [86]–[107].
62 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [108].
63 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [109]–[111].
64 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [88], [98] and [104].

individuals. As has been suggested elsewhere,[65] such a reading of the PDPA is sound, and it is submitted that it should be generally applicable to the interpretation of other parts of the PDPA as well. Second, the Court of Appeal noted that there are two "control mechanisms" to s 32 of the PDPA that "will keep the scope of the s 32(1) action within reasonable bounds".[66] The first control mechanism is found in the wording of s 32 of the PDPA: the individual must have suffered the relevant loss or damage "*directly* as a result of a contravention" [emphasis added] of a data protection obligation. The second control mechanism, more interestingly, was read into s 32 of the PDPA by the Court of Appeal: the loss or damage must be more than *de minimis*, such that "trivial annoyance or negative emotions which form part of the vicissitudes of life will not be actionable".[67]

11.49 The third issue was whether Reed had suffered emotional distress within the meaning of s 32 of the PDPA.

11.50 The Court of Appeal began by holding that the determination of whether an individual has suffered emotional distress is fundamentally a subjective one.[68] Several factors were regarded as potentially relevant: first, the "nature of the personal data involved in the breach"; second, the "nature of the breach"; third, the "nature of the defendant's conduct"; fourth, the "[r]isks of future breaches of the PDPA causing emotional distress to the claimant"; and fifth, the "[a]ctual impact of the breach on the claimant".[69]

11.51 On the facts, the Court of Appeal found that Reed did suffer emotional distress as a result of Bellingham's breach of the PDPA. Several key facts led the Court of Appeal to this finding: first, Reed was sufficiently disturbed by Bellingham's misuse of his personal data to pursue the matter with some persistence; second, the relevant personal data included information about Reed's private investments, which was regarded as sensitive personal data; third, it was reasonable for Reed to anticipate the future misuse of his personal data, due to Bellingham's refusal to provide an undertaking not to misuse his personal data; and fourth, in response to Reed's expressed concerns, Bellingham had acted evasively and was "dismissive".[70] These facts led the Court of Appeal to find that Reed did face anxiety because of Bellingham's misuse of his personal data.

---

65 See also Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7 *International Data Privacy Law* 287 at 290.
66 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [102].
67 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [93].
68 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [114].
69 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [115].
70 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [117]–[132].

11.52 The end result was that Reed was entitled to bring action under s 32 of the PDPA, and the District Court's injunction and order were both upheld.[71]

B. Re Lovebonito Singapore Pte Ltd – *Meaning of "control" – 2FA/MFA – Individuals outside of Singapore*

11.53 In *Re Lovebonito Singapore Pte Ltd*[72] ("*Lovebonito*"), an organisation was found to have breached the Protection Obligation of the PDPA.

11.54 In this case, the organisation ("Lovebonito") operated an online e-commerce platform ("Website") specialising in selling clothing and accessories. To manage the Website, Lovebonito used an open-source software known as the Magento Content Management System ("Magento CMS"). As for credit card transactions on the Website, Lovebonito used a payment platform offered by Adyen NV ("Adyen"). Whenever a customer elected to pay by credit card, the Adyen payment platform would load as a frame on the checkout page of the Website, and customers could then key in their credit card details ("the Credit Card Data") into that frame. The Credit Card Data would be collected and processed by Adyen, and Adyen would send a partial set of the Credit Card Data ("the Partial Credit Card Data") to Lovebonito. Lovebonito would then compile the Partial Credit Card Data with other personal data relevant to fulfilling the customer's order ("the Order Data"), such as the customer's name and address.

11.55 In 2019, Lovebonito discovered some anomalous behaviour on its Website – in particular, it found that its Website's checkout page had been inexplicably modified so as to replace Adyen's payment platform frame with a different form. After further investigations, it was found that one of Lovebonito's Magento CMS accounts ("the Compromised Account") was likely to have been compromised by a malicious actor. This Compromised Account was likely to have been used to modify the Website's checkout page to cause any Credit Card Data submitted by customers to be transmitted to the malicious actor instead of Adyen. Furthermore, the malicious actor had also used the Compromised Account to extract Order Data from the Website. In total, the personal data of 5,561 Lovebonito customers was exfiltrated by the malicious actor in this data breach incident.

71 *Reed, Michael v Bellingham, Alex* [2022] 2 SLR 1156 at [133].
72 [2022] SGPDPC 3. This decision was issued on 21 February 2022.

11.56 The Personal Data Protection Commission ("PDPC") determined that Lovebonito had breached the Protection Obligation under s 24 of the PDPA for failing to make reasonable security arrangements to secure personal data in its possession or under its control. In particular, Lovebonito did not have a sufficiently robust password policy,[73] and had various exploitable weaknesses in its information technology ("IT") infrastructure.[74]

11.57 There are three points of interest to note in this case.

11.58 The first point of interest relates to the meaning of "control" in the PDPA. In this case, one preliminary issue that arose was whether Lovebonito had "possession" or "control" over the Credit Card Data. It was clear on the facts that Lovebonito did not have possession of the Credit Card Data because it did not collect or store that data; rather, it was Adyen who collected the Credit Card Data. However, the PDPC found that Lovebonito did have control over the Credit Card Data.[75] The PDPC reiterated that "control", within the meaning of the PDPA (including s 24 of the PDPA), is "generally understood 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".[76] On the facts, Lovebonito had exercised control over the collection of the Credit Card Data through its Website, as it had decided to deploy Adyen's code on its Website, and this decision determined the manner in which the Credit Card Data was collected via the Website.[77]

11.59 *Lovebonito* demonstrates that an organisation can be regarded as having "control" over personal data when it incorporates code that facilitates the collection of personal data by others. In this regard, there is a clear analogy between the present decision and that of the Court of Justice of the European Union ("CJEU") in the recent case of *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV*[78] ("*Fashion ID*"). *Fashion ID* involved a website operator who embedded a social media plugin on its website; the social media plugin allowed the associated social media network to collect personal data via the website. The CJEU held that such a website operator was a "controller" of the collection and transmission of personal data by the social media plugin.[79]

73 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [18]–[22].
74 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [23]–[25].
75 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [12].
76 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [13].
77 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [14].
78 Case C-40/17, EU:C:2019:629.
79 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* Case C-40/17, EU:C:2019:629, para 85.

11.60 The second point of interest is about two-factor authentication ("2FA") and multi-factor authentication ("MFA"). In this case, the PDPC found that Lovebonito's failure to implement 2FA/MFA to secure access to its Magento CMS accounts was not an instance of breach of the Protection Obligation.[80] Nevertheless, the PDPC opined that 2FA/MFA should be a "baseline standard" for securing administrative accounts (that is, accounts with administrative privileges) of systems holding sensitive personal data or large volumes of personal data.[81] The PDPC observed that this baseline standard was consistent with domestic and international developments, and had become a "reasonable and industry-standard practice".[82]

11.61 The PDPC set out its "tiered approach" to its expectations on the use of 2FA/MFA, which is included here in full:[83]

> (a) First, 2FA / MFA should be implemented as a baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data … Failure to do so can *ipso facto* amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.
>
> (b) Second, *remote access by privileged accounts* to information systems that host confidential or sensitive personal data, or large volumes of personal data, should *a fortiori* be secured by 2FA / MFA. The risks concerning remote access are higher, thus the expectation to implement 2FA / MFA will correspondingly increase.
>
> (c) Third, organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA / MFA, if this is a feature that is available out-of-the-box. Omission to do so may be considered an aggravating factor.
>
> [emphasis in original]

11.62 A third point of interest in *Lovebonito* relates to how the PDPA protects the personal data of individuals outside of Singapore. In its representations to the PDPC, Lovebonito argued that it should receive a reduction in its financial penalty because, out of the 5,561 individuals whose personal data were affected by the data breach incident, only 4,474 of the affected individuals were in Singapore. This argument was rejected by the PDPC. The PDPC stated that the PDPA "does not draw distinctions between the personal data of individuals in Singapore and outside of Singapore", and organisations therefore must secure all personal data in

80 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [36].
81 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [45]–[48].
82 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [48]–[50].
83 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [51].

their possession or control.[84] Thus, it is clear that the PDPA protects the personal data of individuals even if they are located outside of Singapore.

C. Re Farrer Park Hospital Pte Ltd – *E-mail auto-forwarding – Voluntary acceptance of liability*

11.63 In *Re Farrer Park Hospital Pte Ltd*,[85] an organisation was found to have breached the Protection Obligation of the PDPA.

11.64 The organisation ("Farrer Park Hospital") in this case was a private tertiary healthcare institute. Farrer Park Hospital's marketing department received and processed e-mail requests for medical treatment. These e-mails contained personal data of individuals requesting medical treatment, including the individuals' medical information (such as their medical conditions, medical history, and medical reports). In 2019, it was discovered that the e-mail accounts of two employees in the marketing department had been configured (presumably without authority from Farrer Park Hospital) to automatically forward incoming e-mails to a third party. As a consequence, 9,271 e-mails had been automatically forwarded from the employees' e-mail accounts to the third party's e-mail account, which resulted in the disclosure of the personal data of 3,539 individuals. The PDPC found that Farrer Park Hospital had breached the Protection Obligation. This was because Farrer Park Hospital had failed to implement sufficient security measures to protect the marketing department's e-mail accounts, in light of the large volume of sensitive personal data concerned and the vulnerability of Internet-accessible e-mail accounts.[86]

11.65 There are two issues of interest arising from this case.

11.66 The first issue relates to e-mail auto-forwarding. The PDPC noted that e-mail auto-forwarding is a "known security risk", as malicious actors who gain access to compromised e-mail accounts can set auto-forwarding rules that force the compromised e-mail accounts to forward all received e-mails to the malicious actor's e-mail account.[87] In this case, Farrer Park Hospital had omitted to specifically assess the risks posed by allowing auto-forwarding for its e-mail accounts; however, the PDPC gave Farrer Park Hospital the benefit of doubt in this regard, because at the time of the data breach incident, there were no relevant "guidance, standards

84 *Re Lovebonito Singapore Pte Ltd* [2022] SGPDPC 3 at [39].
85 [2022] SGPDPC 6. This decision was issued on 15 September 2022.
86 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [17].
87 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [22].

or benchmarks" on managing the risks of e-mail auto-forwarding.[88] However, the PDPC emphasised that, in future cases, the failure to make a "reasonable assessment" of the risks of e-mail auto-forwarding would constitute a breach of the Protection Obligation.[89] If, pursuant to its risk assessment, an organisation finds that e-mail auto-forwarding poses an unacceptable risk, one solution would be for the organisation to simply disable email auto-forwarding for some or all of its e-mail accounts.[90]

11.67 The second issue relates to the voluntary acceptance of liability. The voluntary acceptance of liability by an organisation for breaching the PDPA is regarded as a mitigating factor, which can reduce the amount of financial penalty imposed on the organisation. As noted in the PDPC's Guide on Active Enforcement,[91] the "voluntary admission of liability" by an errant organisation is a relevant factor to be considered in adjusting the financial penalty to be imposed.[92] In this case, the PDPC explained that a voluntary acceptance of liability by an organisation "demonstrates its commitment to the Accountability Obligation and shows that it can be responsible for the personal data in its possession or under its control".[93]

11.68 It is important to note that timing matters when it comes to a voluntary acceptance of liability. In this case, the PDPC found that Farrer Park Hospital's late-stage voluntary acceptance of liability merited a "small reduction in the financial penalty"; however, if Farrer Park Hospital had accepted liability at an earlier stage in the investigation of its breach of the PDPA, it may have been given a "larger discount" of its financial penalty.

D. Re Supernova Pte Ltd – *Online platforms – ASEAN model contractual clauses*

11.69 In *Re Supernova Pte Ltd*,[94] two organisations were found to have breached the Transfer Limitation Obligation of the PDPA.

11.70 This case involved the Shopify e-commerce platform. The Shopify platform was operated by Shopify Inc, a company based in Canada. Supernova Pte Ltd ("SNPL") was an online retailer who used the Shopify platform to sell products. Shopify Inc provided certain services

88 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [27].
89 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [27].
90 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [23].
91 Revised 1 October 2022.
92 Personal Data Protection Commission, *Guide on Active Enforcement* (revised 1 October 2022) at p 28.
93 *Re Farrer Park Hospital Pte Ltd* [2022] SGPDPC 6 at [46].
94 [2022] SGPDPC 7. This decision was issued on 6 October 2022.

(including payment processing) to SNPL pursuant to a contract ("the Shopify Plus Agreement").

11.71 The Shopify Plus Agreement included an addendum ("the Shopify Data Processing Addendum"). Under the Shopify Data Processing Addendum, Shopify Commerce Singapore Pte Ltd ("Shopify SG") would collect customer personal data on the Shopify platform and transmit the data out of Singapore to Shopify Inc. Shopify Inc would then process the personal data for two purposes: first, to "facilitate billing, payment and shipping" for retailers on the Shopify platform ("Purchase Processing"); and second, for Shopify Inc's "own commercial and administrative purposes" ("Platform Processing").[95]

11.72 In 2019, the Shopify Plus Agreement (including the Shopify Data Processing Addendum) was assigned to Shopify SG. This assignment did not vary the flow of personal data: Shopify SG continued to transmit personal data to Shopify Inc. However, the assignment did change the relationship between Shopify SG and SNPL. As far as Purchase Processing was concerned, Shopify SG became SNPL's data intermediary as it was processing SNPL's customer personal data on behalf of SNPL. As for Platform Processing, Shopify SG was a data controller in its own right (that is to say, Shopify SG was not a data intermediary) since it was processing personal data for its own purposes.

11.73 In 2020, there was a data breach incident affecting Shopify Inc. Since Shopify SG and SNPL were not responsible for Shopify Inc's data security, neither organisation was directly implicated in the data breach incident. However, since both organisations were involved in the transfer of personal data out of Singapore to Shopify Inc, they were investigated for potential breach of the Transfer Limitation Obligation under s 26 of the PDPA.

11.74 The Transfer Limitation Obligation requires organisations to take certain prescribed measures when transferring personal data out of Singapore, to ensure that the personal data so transferred will receive a comparable level of protection to that provided under the PDPA. In particular, such organisations have to "take appropriate steps 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 that under the PDPA"; such "legally enforceable obligations" may be imposed by contract or by binding corporate rules.[96]

95 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [3].
96 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [8].

11.75 In this case, the PDPC found that both Shopify SG and SNPL had breached the Transfer Limitation Obligation in respect of the transfer of personal data to Shopify Inc for the Purchase Processing and the Platform Processing.

11.76 In respect of the Purchase Processing, Shopify SG did not breach the Transfer Limitation Obligation because it was acting as SNPL's data intermediary. A data intermediary (that is, an organisation that is processing personal data "on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing") is exempt from complying with the data protection obligations under the PDPA.[97] It is instead the data controller (that is, the organisation on whose behalf the data intermediary is processing the personal data) who is responsible for the data intermediary's (non-)compliance.[98] Here, Shopify SG was processing customer personal data for SNPL's purpose of completing purchases on the Shopify platform.[99]

11.77 SNPL, as the data controller of the Purchase Processing, was responsible for ensuring that Shopify SG's transfer of personal data out of Singapore to Shopify Inc was done in compliance with the Transfer Limitation Obligation. In the present case, SNPL did not put in place the necessary contractual provisions to ensure that the transferred customer data would receive a comparable level of protection outside of Singapore.[100] As such, SNPL was found to have breached the Transfer Limitation Obligation.

11.78 In respect of the Platform Processing, Shopify SG was processing personal data for its own purposes (with Shopify Inc as its data intermediary); therefore, Shopify SG had to comply with the Transfer Limitation Obligation.[101] The PDPC found that Shopify SG did breach the Transfer Limitation Obligation in respect of the Platform Processing as there was no contract or binding corporate rule addressing the transfer of personal data from Shopify SG to Shopify Inc.[102]

11.79 This case demonstrates the importance of due diligence on the part of platform users. Online platforms like Shopify often transfer personal data across borders, and it is incumbent on platform users like SNPL to ensure that such transfers are done in compliance with the PDPA by ensuring that there are contractual clauses binding the recipient

97 Personal Data Protection Act 2012 (2020 Rev Ed) s 4(2).
98 Personal Data Protection Act 2012 (2020 Rev Ed) s 4(3).
99 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [14].
100 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [9]–[13].
101 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [15].
102 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [16].

of the personal data. Such contractual clauses may be prudent even when the transfer of personal data is to a destination country that appears to have robust data protection (in this case, Canada). Where platform users do not have the bargaining power to cause the platform owner to change its standard contractual terms, it may be that the only solution for such platform users is to cease to use the platform.

11.80 Another point of interest relates to model contractual clauses ("MCCs") endorsed by the Association of Southeast Asian Nations ("ASEAN"). In its decision, the PDPC highlighted that the ASEAN MCCs had been recognised as satisfying the Transfer Limitation Obligation – as such, organisations may rely on the ASEAN MCCs as a convenient standard.[103]

---

103 *Re Supernova Pte Ltd* [2022] SGPDPC 7 at [21]–[22].