(2020) 21 SAL Ann Rev 291
(Published on e-First 9 April 2021)

11. CONFIDENTIAL INFORMATION AND DATA PROTECTION

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

I. Introduction to the chapter

11.1 This chapter on the law of confidential information and data protection is a new addition to the Ann Rev. Part II[1] of the chapter reviews selected cases on the law of confidential information, while Part III[2] of the chapter reviews selected cases on data protection law. Within each part, the cases are reviewed in chronological order, according to the dates on which they were decided.

II. Confidential information

11.2 Four cases from the Supreme Court have been selected for review in this part.

A. LVM Law Chambers LLC v Wan Hoe Keet – *Solicitor's duty of confidence to counterparty*

11.3 When a law firm has acted against a counterparty in previous proceedings, under what circumstances will the law firm be restrained from acting against the same counterparty in subsequent proceedings? The Court of Appeal had the opportunity to address this question in its decision in *LVM Law Chambers LLC v Wan Hoe Keet*[3] ("*LVM Law Chambers*").

11.4 The facts of *LVM Law Chambers* are as follows. In Suit 315 of 2016 ("Suit 315"), the plaintiff ("Lee") had sued the defendants ("Wan" and "Ho"), claiming that Wan and Ho had made misrepresentations about a scheme known as "SureWin4U". Suit 315 was settled by a settlement

1 See paras 11.2–11.46 below.
2 See paras 11.47–11.80 below.
3 [2020] 1 SLR 1083. This case was decided on 3 April 2020 and arose from an appeal against the High Court's decision in *Wan Hoe Keet v LVM Law Chambers LLC* [2020] 3 SLR 568.

agreement ("the Settlement Agreement") reached through settlement negotiations that were conducted by the parties' solicitors. The Settlement Agreement included a confidentiality clause, obliging the parties to keep confidential certain stipulated information relating to Suit 315. However, Lee's solicitors ("LVM") were not party to the Settlement Agreement, and they were therefore not contractually bound by the confidentiality clause. Subsequently, in Suit 806 of 2018 ("Suit 806"), a different plaintiff ("Chan") similarly sued Wan and Ho, claiming that she was induced to invest in SureWin4U by misrepresentations from Wan and Ho. Notably, Chan was also represented by LVM. This meant that LVM was again acting against Wan and Ho.

11.5 Wan and Ho applied for an injunction to, *inter alia*, restrain LVM from acting for Chan in Suit 806. First, Wan and Ho argued that LVM owed them obligations of confidence arising from its participation in the settlement negotiations in Suit 315. Second, they argued that there was a risk that LVM would, when acting in Suit 806, misuse the confidential information that it had previously learned from the settlement negotiations in Suit 315.

11.6 At first instance, the High Court allowed the application and granted the injunction sought.

11.7 On the issue of LVM's duty of confidence, the court acknowledged that LVM was not bound by the contractual confidentiality clause in the Settlement Agreement.[4] Nevertheless, an equitable duty of confidence could be imposed if a "reasonable solicitor" in the position of LVM "should have known that the information was given in confidence", and on the facts, LVM did know that its client in Suit 315 (Lee) had promised Wan and Ho to not use or disclose the information stipulated in the Settlement Agreement.[5] Therefore, the court held that LVM owed an equitable duty of confidence to Wan and Ho.

11.8 On the issue of threatened misuse of the confidential information, LVM submitted that it would not disclose the settlement sum in Suit 315 to Chan, nor would it even think about the settlement sum. However, the court took the view that the confidential information could nonetheless subconsciously influence LVM's conduct in Suit 806,[6] and if the parties in Suit 806 decided to settle, the confidential information could afford Chan an advantage against Wan and Ho in the settlement negotiations.[7]

4 *Wan Hoe Keet v LVM Law Chambers LLC* [2020] 3 SLR 568 at [9].
5 *Wan Hoe Keet v LVM Law Chambers LLC* [2020] 3 SLR 568 at [9].
6 *Wan Hoe Keet v LVM Law Chambers LLC* [2020] 3 SLR 568 at [10].
7 *Wan Hoe Keet v LVM Law Chambers LLC* [2020] 3 SLR 568 at [11].

Therefore, there was a threat of misuse that was sufficient to justify granting the injunction.

11.9 LVM appealed against the High Court's decision. The Court of Appeal allowed the appeal, permitting LVM to act for Chan in Suit 806, albeit on the condition that LVM would not disclose the terms of the Settlement Agreement from Suit 315.[8]

11.10 In its decision, the Court of Appeal recognised that a law firm can indeed owe an equitable duty of confidence to a counterparty in relation to information obtained from previous proceedings, such that it can be inappropriate for that law firm to act against the same counterparty in subsequent proceedings.[9] To restrain the law firm from acting in the subsequent proceedings, the counterparty must establish that: (a) the information concerned has the "necessary quality of confidence about it"; (b) the information was "received by the lawyer (or law firm) concerned in circumstances importing an obligation of confidence"; and (c) there is a "real and sensible possibility of the information being misused".[10] These elements were derived from the traditional test for breach of confidence as set out in *Coco v AN Clark (Engineers) Ltd*,[11] and modified for the particular issue at hand.

11.11 In the instant case, the Court of Appeal agreed that LVM was obliged to keep confidential the terms of the Settlement Agreement, and ordered LVM not to disclose the terms of the Settlement Agreement.[12] As for the other details about the settlement negotiations, however, the court found that these were not sufficiently proved to be confidential. Therefore, a general restraint on LVM from acting in Suit 806 could not be justified on the basis that LVM might misuse its knowledge of those other details.[13] The court stressed that "mere assertions or vague generalisations will not pass legal muster" and a "granular approach" was demanded,[14] but here Wan and Ho had only made "vague references" to the negotiation process.[15]

11.12 Three points of practical interest from the Court of Appeal's decision in *LVM Law Chambers* should, in particular, be highlighted.

---

8 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [31].
9 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [14].
10 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [15].
11 [1969] RPC 41.
12 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [29]–[31].
13 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [29]–[30].
14 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [29].
15 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [29].

11.13 First, if a counterparty wishes to restrain its opponent's chosen lawyer from acting for the opponent, the counterparty bears the burden of proving that the lawyer should be so restrained. The counterparty's burden of proof is weighty, given the importance of the right of a litigant to choose his own counsel.[16] As a consequence, the counterparty may face evidential difficulties in proving the three elements set out in *LVM Law Chambers* (as the outcome of *LVM Law Chambers* illustrates). Such evidential difficulties can be avoided by the counterparty if it can rely on a *contractual* duty of confidence. It may therefore be useful for counterparties to bind *both* their opponents and their opponents' lawyers to express undertakings of confidence, as these undertakings can then be relied upon in subsequent proceedings.[17]

11.14 Second, the Court of Appeal appeared to have accepted that, in principle, a law firm may be restrained from acting against a counterparty in subsequent proceedings on the basis of potential "unconscious" or "subconscious" misuse of confidential information obtained from previous proceedings.[18] Therefore, the counterparty need not prove that there is a risk that the law firm would actually consciously misuse the confidential information. That said, it bears remembering that the counterparty must still prove that there is a "real and sensible possibility" of unconscious or subconscious misuse: in this regard, two relevant factors are (i) the extent of similarity between the previous proceedings and the subsequent proceedings; and (ii) whether the law firm was "deliberately retained" because of its participation in the previous proceedings.[19]

11.15 Third, and more incidentally, it is interesting to note the Court of Appeal's discussion of the requirement of confidentiality (that is, the requirement that the information concerned has the "necessary quality of confidence"). The court stated in *obiter dicta* that no duty of confidence, "equitable *or otherwise*" [emphasis added], can possibly arise if the information concerned is "common or public knowledge".[20] This statement could be taken as suggesting that the requirement of confidentiality applies even to *contractual* duties of confidence, perhaps as an implied limit to such contractual duties.

16 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [23].
17 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [32].
18 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [19].
19 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [22].
20 *LVM Law Chambers LLC v Wan Hoe Keet* [2020] 1 SLR 1083 at [16].

B. I-Admin (Singapore) Pte Ltd v Hong Ying Ting – *Modified test for breach of confidence*

11.16 Just three days after its decision in *LVM Law Chambers*, the Court of Appeal issued its decision in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting*[21] ("*I-Admin*"). In this decision, the court fundamentally reshaped the law of confidence in Singapore, by modifying the test for breach of confidence.[22]

11.17 In this case, the appellant ("I-Admin") was a company in the business of providing payroll services and human resource services, and it used certain software systems to provide these services. The first respondent ("Hong") and second respondent ("Liu"), were employees of I-Admin and of I-Admin's subsidiary, respectively. In 2009, Hong and Liu began to work on their own payroll software. They eventually incorporated the third respondent ("Nice Payroll") and left their employers to work for Nice Payroll. In 2013, I-Admin discovered Nice Payroll's website, and found out that Nice Payroll was providing payroll and human resource services. I-Admin also found out that Hong and Liu were directors of Nice Payroll. I-Admin commenced proceedings against the respondents, claiming for breaches of copyright, confidence and contract, as well as for conspiracy and inducing breach of contract.

11.18 At first instance, I-Admin was generally unsuccessful in its claims before the High Court.[23] Most of its claims were dismissed, including its claim for breach of confidence. In its assessment of the claim for breach of confidence, the court applied the traditional test for breach of confidence: (a) the information must "possess the necessary quality of confidentiality"; (b) the information must have been "imparted in circumstances importing an obligation of confidence"; and (c) there must have been an "unauthorised use of that information to the detriment of the party communicating it".[24] The main difficulty with I-Admin's claim before the High Court was that element (c) was not made out: I-Admin failed to persuade the court that there was any unauthorised use of its information.

---

21 [2020] 1 SLR 1130. This case was decided on 6 April 2020, and arose from an appeal against the High Court's decision in *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 3 SLR 615.

22 See Benjamin Wong & David Tan, "A Modern Approach to Breach of Confidence Based on an Obligation of Conscience" (2020) 136 LQR 548.

23 For a discussion of the High Court's decision, see also David Tan & Susanna H S Leong, "Intellectual Property Law" (2019) 20 SAL Ann Rev 541 at 545.

24 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 3 SLR 615 at [108], citing *Clearlab SG Pte Ltd v Ting Chong Chai* [2015] 1 SLR 163 at [64].

11.19 First, while some of I-Admin's "source codes, systems, database structures and client information" had been referred to by the respondents, the High Court found that this did not itself amount to "use".[25] Second, I-Admin alleged that the respondents had used its payroll software to generate payroll reports for their own purposes, but there was insufficient evidence of such use.[26] Third, Hong had accessed I-Admin's online product demonstration platform, but it was not proved that the respondents had used any of the information on the platform.[27] Fourth, the respondents had informed two of I-Admin clients that Nice Payroll was in possession of I-Admin's client data, and had reported I-Admin's loss of client data to the police; however, this was not use of the client data itself, but merely use of the knowledge that the client data was in the respondents' possession.[28]

11.20 I-Admin appealed against the High Court's decision, on the issues of copyright infringement and breach of confidence. The Court of Appeal allowed the appeal in part, finding for I-Admin on the issue of breach of confidence.

11.21 In its decision, the Court of Appeal adopted a modified test for breach of confidence. Two main modifications were made. First, the second element of the traditional test for breach of confidence was expressly expanded: whereas the original formulation of the second element stated that the information in question must have been *imparted* in circumstances importing an obligation of confidence, the court made it clear that an obligation of confidence could also arise "where confidential information has been accessed or acquired without a plaintiff's knowledge or consent".[29] Second, the third element of the traditional test for breach of confidence was replaced, so that it is no longer necessary for a plaintiff to prove that there was detrimental unauthorised use of his confidential information; now, once a plaintiff satisfies the first two elements of the test for breach of confidence, "an action for breach of confidence is presumed", and it is for the defendant to displace this presumption by proving that his "conscience was unaffected".[30] In this regard, the court suggested a number of situations where the presumption may be displaced: where "the defendant came across the information by accident or was unaware

25 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 3 SLR 615 at [115]–[125].
26 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 3 SLR 615 at [126]–[129].
27 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 3 SLR 615 at [130]–[134].
28 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 3 SLR 615 at [135]–[138].
29 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61].
30 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61].

of its confidential nature or believed there to be a strong public interest in disclosing it".[31]

11.22 Applying the modified test to the facts before it, the Court of Appeal held that I-Admin's materials were confidential, and the respondents were bound by obligations of confidence.[32] The respondents had committed *prima facie* breaches of their obligations of confidence by "acquiring, circulating and referencing" I-Admin's materials "without permission", and they had "done nothing to displace the presumption that their conscience was negatively affected".[33] Therefore, the respondents were in breach of confidence.

11.23 *I-Admin* is a landmark decision of the Court of Appeal, making a significant impact on the law of confidence. Primarily, *I-Admin* makes it clear that the unauthorised accessing, taking or possession of confidential information can amount to a breach of confidence.[34] A number of other observations should be made about *I-Admin*.

11.24 First, in reforming the law of confidence, it appears that the Court of Appeal's main concern was the need for better protection against the degradation of confidentiality *per se*. The court made it clear at the outset that the traditional action for breach of confidence, as it stood prior to *I-Admin*, did not "adequately safeguard the interests of those who own confidential information".[35] This was because the traditional action for breach of confidence would not assist the plaintiff in the situation where the defendant had wrongfully acquired or accessed confidential information (thereby compromising the confidentiality of said information) but could not be proved to have made unauthorised use of that information.[36] This limitation of the traditional action for breach of confidence is illustrated by the High Court's decision at first instance: although I-Admin's confidential information had been accessed and taken by the respondents, the High Court rejected I-Admin's claim for breach of confidence because there was insufficient proof of unauthorised use by the respondents.

---

31 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [61]. Interestingly, the last-mentioned situation suggests that the defence of iniquity has been subsumed into the third limb of the modified test for breach of confidence: see Benjamin Wong & David Tan, "A Modern Approach to Breach of Confidence Based on an Obligation of Conscience " (2020) 136 LQR 548 at 552.

32 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [63].

33 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [63].

34 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [63] and [66].

35 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [3].

36 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [43].

11.25 Second, the Court of Appeal's reform was grounded on the theoretical foundations of the action for breach of confidence. According to the court, the action for breach of confidence is founded on an obligation of conscience, which binds obligors to not "deal with confidential information in a manner that adversely affects their conscience", and this obligation of conscience "may extend beyond refraining from acts of unauthorised use or disclosure".[37] The purpose of the action for breach of confidence is to protect not only the "wrongful gain interest" (the plaintiff's interest in "preventing wrongful gain or profit from its confidential information"),[38] but also the "wrongful loss interest" (the plaintiff's interest in preventing the "dissipation of the confidential character of the information").[39] The court took the view that the law should now have a "more robust response" against threats to the wrongful loss interest,[40] in view of modern technological advances making it easier to "access, copy and disseminate vast amounts of confidential information",[41] and also in view of the limited alternative remedies available to "plaintiffs who have only suffered a violation of their wrongful loss interest".[42]

11.26 Third, it is an open question whether the plaintiff retains an evidential burden of showing that the defendant had *prima facie* acted in breach of confidence: in other words, after having satisfied the first two requirements in the modified test for breach of confidence, does the plaintiff still need to adduce some evidence that the defendant had *prima facie* acted against his conscience? On one view, the Court of Appeal's analysis in *I-Admin* is arguably consistent with an affirmative answer to this question: the court first made a finding that the respondents had *prima facie* breached their obligations of confidence by their actions, *before* turning to consider the respondents' arguments in defence of their conscience.[43] On the other hand, the High Court's decision in *BAFCO Singapore Pte Ltd v Lee Tze Seng*[44] suggests a negative answer – in that case, the court imposed the presumption on the defendants immediately after the plaintiff satisfied the first and second elements of the modified test for breach of confidence.[45]

37 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [51].
38 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [50].
39 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [57].
40 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [54].
41 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [55].
42 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [56]–[57].
43 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting* [2020] 1 SLR 1130 at [63]–[64]. See also *iVenture Card Ltd v Big Bus Singapore City Sightseeing Pte Ltd* [2020] SGHC 109 at [27].
44 [2020] SGHC 281. Discussed further at paras 11.40–11.46 below.
45 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [21].

11.27 Fourth, the new third element of the modified test for breach of confidence requires a far broader assessment of the defendant's conduct. Previously, under the third element of the traditional test for breach of confidence, it was necessary and sufficient to prove that the defendant had made a detrimental unauthorised misuse of the confidential information. This is no longer the case. Instead, under the new third limb, the question is whether the defendant's conscience was affected by the way in which he had dealt with the confidential information.

11.28 The District Court case of *Tree Art International Pte Ltd v Colour Moon Pte Ltd*[46] offers a good illustration of the broader assessment that may be required by the new third element of the modified test for breach of confidence. In that case, the plaintiff ("Tree Art") provided art education services, and had imparted its customer list to the first and second defendants ("Duan" and "Gou", respectively) in the course of their employment with Tree Art. Duan and Gou subsequently set up the first defendant ("Colour Moon"), which also provided art education services. Subsequent investigations by Tree Art revealed that Colour Moon's students were present or past students of Tree Art. Tree Art sought an interim injunction to restrain the defendants from dealing with Tree Art's confidential customer information. To determine if there was a serious question to be tried, the court applied the *I-Admin* modified test for breach of confidence.[47] When applying the new third limb of the modified test, the court did consider the possible misuse of the confidential customer information by the defendants,[48] but what is notable is that the court also considered that some of the contact numbers in Tree Art's customer data had been changed either to "dummy" numbers or to Duan's own number, and this was held to also be an issue that "potentially impinges on the defendants' conscience".[49]

C. Shanmugam Manohar v Attorney-General – *Public interest exception*

11.29 The law of confidential information admits of a "public interest exception" which recognises that, in exceptional circumstances, the disclosure of confidential information can be justified in the public interest. In cases where the public interest exception applies, the disclosure of confidential information will not be regarded by the court as a breach

46 [2020] SGDC 150.
47 *Tree Art International Pte Ltd v Colour Moon Pte Ltd* [2020] SGDC 150 at [18].
48 *Tree Art International Pte Ltd v Colour Moon Pte Ltd* [2020] SGDC 150 at [37]–[41].
49 *Tree Art International Pte Ltd v Colour Moon Pte Ltd* [2020] SGDC 150 at [42].

of confidence.[50] The High Court applied the public interest exception in *Shanmugam Manohar v Attorney-General*[51] ("*Shanmugam Manohar*"). In this case, the applicant was a partner of a law firm ("the Firm").

11.30 *Shanmugam Manohar* arose out of a police investigation into a motor insurance fraud scheme. The perpetrator of the scheme ("Ng") procured warrants to act from potential insurance claimants. These warrants to act appointed certain law firms to act on the claimants' behalf. If the insurance claims were successful, Ng would receive commissions from the law firms. Ng was investigated by the Commercial Affairs Department ("CAD"), and he was eventually convicted of abetment of cheating. Subsequently, the CAD conducted further investigations into the conduct of the law firms and lawyers involved, at the request of the Attorney-General's Chambers ("AGC"). In the course of its investigations, the CAD recorded a number of statements from various parties ("the CAD statements"). These included statements from Ng, the applicant, and another partner of the Firm.

11.31 Ultimately, the CAD took the view that its further investigations did not disclose any further offence of cheating. The CAD forwarded its findings and the CAD statements to the AGC. The Attorney-General ("AG") then relayed information about the applicant's alleged touting practices to the Law Society, and requested that the Law Society refer the matter to a disciplinary tribunal ("DT"). In response, the Law Society requested certain information, including "copies of the statements of the relevant persons".[52] The CAD informed the AG that it had no objection to the sending of the CAD statements to the Law Society. The AG sent the CAD statements to the Law Society, who then applied to the Chief Justice to appoint a DT to investigate the applicant.

11.32 The applicant filed an Originating Summons ("OS") applying for a number of declarations from the High Court. Broadly speaking, the applicant requested that the High Court declare that the recording, use and disclosure of the CAD statements by the AG and the CAD were unlawful and improper. The applicant argued, *inter alia*, that the CAD statements were "subject to a duty of confidence".[53]

11.33 The High Court dismissed the OS.[54]

50 *Cf AAY v AAZ* [2011] 1 SLR 1093 at [69]–[72], on the distinction between the "public interest exception" and the "public interest defence".
51 [2020] SGHC 120. This case was decided on 16 June 2020.
52 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [8].
53 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [15].
54 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [14].

11.34 On the issue of breach of confidence, it was not disputed that the CAD statements were subject to a duty of confidence; what was contested was whether the public interest exception allowed the AG and the CAD to disclose the CAD statements to the Law Society.[55]

11.35 The High Court began by thoroughly examining the relevant foreign precedents, wherein the public interest exception was applied to the disclosure of police statements to regulatory authorities.[56] The court concluded that "courts in other common law jurisdictions have treated this issue as one where the public interest is better served by disclosure".[57] It went on to hold that:[58]

> … where evidence of disciplinary breaches is presented to the police in the course of investigations, or where such information is then received from the police by the AG, there is a public interest in disclosure being made to the regulatory body in question.

11.36 The court found that the public interest exception applied in the instant case.[59]

11.37 *Shanmugam Manohar* appears to have extended the application of the public interest exception beyond the precedent cases cited from the UK, Australia and New Zealand. Whereas the precedent cases dealt with direct disclosures of confidential information from the police to the regulatory authorities, *Shanmugam Manohar* involved an indirect disclosure *by the AG* of confidential information originally obtained by the police. Nevertheless, it is suggested that this extension is entirely principled. This is because the identity of the discloser – be it the police themselves or some other third party such as the AG – has little relevance to the public interest calculus. What is relevant is that the disclosure be made in the public interest "to one who has a proper interest to receive the information".[60] As has been noted in a recent case from the Court of Appeal of England and Wales, the court's analysis focuses "on whether the disclosure was in the public interest, and on the function of the other public body to which information was to be disclosed".[61]

---

55 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [81].
56 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [85]–[90]. The key cases cited were *Woolgar v Chief Constable of Sussex Police* [2000] 1 WLR 25; *R (Pamplin) v Law Society* [2001] EWHC Admin 300; *McLean v Racing Victoria Ltd* [2019] VSC 690; and *MA v Attorney-General* [2009] NZCA 490.
57 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [85].
58 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [91].
59 *Shanmugam Manohar v Attorney-General* [2020] SGHC 120 at [95].
60 *Initial Services Ltd v Putterill* [1968] 1 QB 396 at 405.
61 *R (on the application of the Centre for Advice on Individual Rights in Europe) v Secretary of State for the Home Department* [2018] EWCA Civ 2837 at [44].

11.38 It should be noted that, for the public interest exception to apply, the disclosure should be limited on the basis of necessity. In *Shanmugam Manohar*, the disclosure of information was correctly limited to the information necessary for the regulatory authority (here, the Law Society) to fulfil its function. This is important because, in other cases, the public interest exception failed due to the defendant's excessive disclosure. For example, in *Saab v Dangate Consulting Ltd*,[62] although the defendants had made disclosures to the relevant financial regulatory authorities, they had made a "broad disclosure of multiplicitous documents going to different aspects", and the court suggested that "it would be vanishingly rare for a situation to arise which justified such a very broad disclosure".[63]

11.39 As a final note, the public interest exception now appears to have been subsumed into the new third element of the modified test for breach of confidence under *I-Admin*.[64] In other words, an assessment of the public interest in the disclosure of the confidential information now forms part of the analysis of whether the discloser's conscience was negatively affected. It remains to be seen what implications this will have on the public interest exception – it may well be that the public interest exception is in substance preserved as a standalone exception, allowing the court to continue taking advantage of the well-developed body of case law on the public interest exception.

D. BAFCO Singapore Pte Ltd v Lee Tze Seng – *Springboard injunctions*

11.40 Springboard injunctions are granted to prevent a defendant from taking unfair advantage of a head-start (the metaphorical "springboard") that he derived from the misuse of the plaintiff's confidential information.[65] In *BAFCO Singapore Pte Ltd v Lee Tze Seng*[66] ("*BAFCO*"), the High Court had to consider whether the plaintiff should be granted an interim springboard injunction.

11.41 The plaintiff ("BAFCO") was a company in the business of selling high-volume, low-speed ("HVLS") fans. The first, second and third defendants ("the Former Employees") were former employees of BAFCO. The fourth defendant ("D&Y") was a company in which the former employees were involved. BAFCO alleged, *inter alia*, that D&Y

62 [2019] EWHC 1558 (Comm) at [159].
63 *Saab v Dangate Consulting Ltd* [2019] EWHC 1558 (Comm) at [159].
64 See paras 11.16–11.28 above.
65 *Roger Bullivant v Ellis* [1987] ICR 464 at 476; *QBE Management Services (UK) Ltd v Dymoke* [2012] IRLR 458 at [240].
66 [2020] SGHC 281. This case was decided on 22 December 2020.

was engaged in the distribution of fans, including HVLS fans produced by the fifth defendant ("Vortikul"). BAFCO claimed that the defendants had misused its confidential information to "divert business opportunities" away from BAFCO, and to "help a competing bidder secure a tender project".[67]

11.42 In the instant proceedings, BAFCO sought various interlocutory reliefs against the defendants. *Inter alia*, BAFCO applied for three injunctions. These are worth setting out fully, below:[68]

> (a) an injunction to restrain the Former Employees from using and/or disclosing any of the plaintiff's confidential information acquired by them during their employment with the plaintiff (until final determination of this action or further order) ('the Disclosure Injunction');
>
> (b) an injunction to restrain the Former Employees and D&Y from relying on the plaintiff's confidential information to procure or do any business with third parties that will enable the defendants to carry out any business which is similar to the plaintiff's business (until final determination of this action or further order or for a period of 12 months, whichever is earlier) ('the Procurement Injunction');
>
> (c) an injunction to restrain the Former Employees and D&Y from continuing communications with the plaintiff's customers whom any of the defendants communicated with during the Former Employees' employment with the plaintiff and up to 3 August 2020, with a view towards procuring or doing business for persons other than the plaintiff (until final determination of this action or further order or for a period of 12 months, whichever is earlier) ('the Communications Injunction') …

11.43 The defendants argued that the injunctions sought by BAFCO amounted to springboard injunctions, such that the stricter requirements for springboard injunctions had to be satisfied by BAFCO.[69] The High Court agreed that the Communications Injunction was a springboard injunction as it was meant to prevent the defendants from exploiting an "unfair competitive advantage".[70] However, the Disclosure Injunction and Procurement Injunction were "conventional injunctions", as they were meant to prevent further breaches of confidence by the defendants.[71]

11.44 For the Disclosure Injunction and Procurement Injunction, the High Court applied the standard *American Cyanamid* principles. First, the

67 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [7].
68 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [6].
69 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [10].
70 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [13].
71 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [13].

court found that there was a serious question to be tried:[72] the court found that the first two elements of the modified test for breach of confidence (as set out in *I-Admin*)[73] were met,[74] and was unconvinced by the defendants' attempts to discharge the presumption that their conscience was not negatively affected.[75] Second, the court found that the balance of convenience lay in favour of granting the injunctions.[76] Accordingly, the court granted the Disclosure Injunction and Procurement Injunction.[77]

11.45 However, the High Court refused to grant the Communications Injunction. According to the court, a springboard injunction must be no wider than reasonably necessary to eliminate the defendant's unfair competitive advantage – that is, to restore the parties' competitive positions to that which they would have obtained but for the defendants' breach.[78] Here, the Communications Injunction was too wide. First, there was no evidence that the defendants intended to "compete with the plaintiff or assist the plaintiff's competitors in any upcoming tender bids".[79] Second, the Disclosure Injunction and the Procurement Injunction appeared to have already eliminated the defendants' unfair competitive advantage.[80] Third, the Communications Injunction went beyond merely eliminating the defendants' unfair competitive advantage, as it precluded contact with any of the plaintiff's customers even if doing so would not involve the use or disclosure of the plaintiff's confidential information.[81]

11.46 *BAFCO* illustrates the point that a plaintiff applying for a springboard injunction should identify clearly the precise unfair competitive advantage that the springboard injunction is intended to address, and frame the springboard injunction no more widely than necessary to remove that advantage (taking into consideration the extent to which the other reliefs sought already remove the said advantage). In framing the terms of springboard relief, the five principles set out by the High Court of England and Wales in *QBE Management Services (UK) Ltd v Dymoke* may be instructive.[82]

72 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [24].
73 See paras 11.16–11.28 above.
74 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [16]–[21].
75 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [21]–[23].
76 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [25]–[26].
77 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [31].
78 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [27].
79 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [27].
80 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [27].
81 *BAFCO Singapore Pte Ltd v Lee Tze Seng* [2020] SGHC 281 at [28].
82 See [2012] IRLR 458 at [285].

III. Data protection

11.47 Four enforcement decisions from the Personal Data Protection Commission ("PDPC") have been selected for review in this part. These decisions are issued pursuant to the Personal Data Protection Act 2012[83] ("PDPA").

A. Re Creative Technology Ltd – *Preservation of evidence*

11.48 The PDPC has previously stated that organisations are under a duty to preserve evidence relating to an investigation by the PDPC.[84] This duty arose as an issue in *Re Creative Technology Ltd*.[85]

11.49 In *Re Creative Technology Ltd*, the organisation ("Creative") operated an online forum, using an internet forum software known as "vBulletin". The vBulletin software had a vulnerability which could allow hackers to extract information from the forum's database using Structured Query Language ("SQL") injection methods. Although the developers of the vBulletin software had released patches to deal with this vulnerability in 2016, Creative did not install these patches. On 28 May 2018, a hacker exploited the vulnerability, using SQL injection methods to extract users' personal data from the forum's database.

11.50 The PDPC found that Creative had breached the Protection Obligation under s 24 of the PDPA, as Creative had failed to put in place reasonable security measures to protect personal data in its possession or under its control.[86] First, it did not patch its vBulletin software.[87] Second, it had used a weak password hashing algorithm known to be insecure (the MD5 algorithm) to hash its passwords.[88]

11.51 Notably, the PDPC went on to discuss the duty to preserve evidence relating to a PDPC investigation.

11.52 In its previous decision of *Re NTUC Income Insurance Co-operative Ltd*,[89] the PDPC had clarified that organisations have a "duty to preserve evidence, including but not limited to documents and records, in relation to an investigation by the PDPC".[90] The PDPC had

83 Act 26 of 2012.
84 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [23].
85 [2020] SGPDPC 1. This decision was issued on 2 January 2020.
86 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [12].
87 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [10].
88 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [11].
89 [2018] SGPDPC 10.
90 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [23].

stated that it would "not look favourably on the destruction of potentially relevant documents and records", and warned that it "may impose tough sanctions on any organisation that is found to have destroyed or deleted such documents or records".[91] The PDPC took the view that an organisation should implement a "detailed litigation hold policy", to "ensure that documents and records relating to an investigation or potential investigation of a breach of its obligations under the PDPA are preserved and not deleted, disposed of or destroyed".[92]

11.53 Further, in *Re NTUC Income Insurance Co-operative Ltd*, the PDPC had identified several factors that it would consider, in determining the appropriate sanctions to be imposed on organisations for their failure to preserve evidence. These include:

> (a) "whether the deletion or destruction of the documents or records was deliberate (which includes negligent or reckless conduct resulting in destruction)";[93]
>
> (b) the extent to which the "deletion or destruction of the records or documents prejudice a fair investigation into a potential breach of the PDPA";[94] and
>
> (c) "whether the litigation or legal proceedings was anticipated or contemplated" by the organisation.[95]

11.54 In the present case, Creative had failed to fulfil its duty to preserve evidence, as it had deleted the user database of its forum shortly after discovering that the forum was hacked. In this regard, two factors were considered by the PDPC: first, in relation to prejudicing the PDPC's investigation, the PDPC found that it was unable to verify how many individuals were affected by the hack due to the deletion of the user database;[96] and second, in relation to anticipating an investigation by the PDPC, Creative ought to have considered that the data breach in question was "not insignificant".[97] As a sanction for Creative's failure to fulfil the duty to preserve evidence, the PDPC regarded the deletion of the user database as an aggravating factor, going towards the remedial directions to be imposed on Creative.[98]

---

91 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [25].
92 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [29].
93 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [26].
94 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [26].
95 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [27].
96 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [16].
97 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [18].
98 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [15].

11.55 Two comments may be made on the issue of the preservation of evidence.

11.56 First, *Re Creative Technology Ltd* makes clear that one mechanism by which the PDPC will impose sanctions for failure to preserve evidence is by regarding such failures as an aggravating factor. However, it should be noted that this mechanism is only available in the event that the organisation under investigation is found to have breached its obligations under the PDPA. Other mechanisms may be available to deter the destruction of evidence. These include the drawing of adverse inferences against the errant organisation,[99] and possibly criminal liability under s 51(3)(*b*) of the PDPA.[100]

11.57 Second, *Re Creative Technology Ltd* confirms that the duty to preserve evidence applies even before the formal commencement of investigations by the PDPC.[101] In the present case, Creative had deleted the user database about two weeks after discovering the data breach. Although the deletion of the user database occurred about five months before the PDPC gave formal notice that it was commencing investigations,[102] the PDPC nonetheless regarded the deletion as a failure of Creative's duty to preserve evidence. Therefore, organisations should take measures to preserve evidence of potential breaches of the PDPA, as soon as those potential breaches are discovered.

B. Re Majestic Debt Recovery Pte Ltd – *Consent and purpose limitation*

11.58 The case of *Re Majestic Debt Recovery Pte Ltd*[103] highlights how consent should and should not be obtained, and demonstrates how even valid consent does not grant a free rein to the organisation.

11.59 In *Re Majestic Debt Recovery Pte Ltd*, the organisation ("Majestic") was in the business of debt collection. Majestic was engaged by a creditor company to recover debts from a debtor company. On one occasion, Majestic's representatives visited the debtor company's premises to collect a debt. During that visit, an argument ensued between

99 *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10 at [26].

100 Section 51(3)(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA") provides that it is an offence for an organisation or person to obstruct or hinder the Personal Data Protection Commission (among other persons) "in the performance of any function or duty, or the exercise of any power" under the PDPA.

101 In the previous case of *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10, the deletion took place after the commencement of investigations.

102 *Re Creative Technology Ltd* [2020] SGPDPC 1 at [15].

103 [2020] SGPDPC 7. This decision was issued on 2 March 2020.

Majestic's representatives and the debtor company's personnel. Majestic's representatives recorded video footage of their exchanges with the debtor company's personnel (including the debtor company's managing director, who was the complainant in this case). The debtor company's personnel could be identified from the video footage. Majestic later uploaded the video footage on its official public Facebook page. Notably, the video footage was recorded and uploaded despite the protests of the complainant.

11.60 The PDPC found that Majestic had, *inter alia*, breached the Consent Obligation under s 13 of the PDPA: by recording and uploading video footage of the complainant despite his protests, Majestic had collected, used and/or disclosed the complainant's personal data without his consent.[104]

11.61 A number of useful observations may be made about the application of the Consent Obligation in *Re Majestic Debt Recovery Pte Ltd*.

11.62 The first observation relates to the issue of implied consent by acquiescence. The PDPA does not stipulate the form in which actual consent must be obtained. This makes it possible to argue that implied consent, obtained through the individual's acquiescence or failure to object, can constitute actual consent. This argument was made by Majestic in *Re Majestic Debt Recovery Pte Ltd* as it claimed that it had obtained implied consent for the collection, use and disclosure of the video footage; specifically, Majestic claimed that there was implied consent as the debtor company did not object to similar video recordings on previous visits by Majestic's representatives.[105] The PDPC found, however, that Majestic was unable to provide evidence for the implied consent which they claimed to have obtained.[106] This demonstrates the evidential difficulties that may arise in any attempt to rely on implied consent by acquiescence. In this case, it is difficult to see how it would be possible for Majestic to prove that it had *never* received any objections to its recording of video footage.

11.63 The second observation relates to the withdrawal of consent. Section 16 of the PDPA provides that an individual may withdraw his consent by giving reasonable notice to the organisation. While s 16 of the PDPA does not elaborate on what constitutes "reasonable notice", *Re Majestic Debt Recovery Pte Ltd* suggests that the requirement to give reasonable notice may be easily met. Here, the PDPC found that even if

104 *Re Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [6].
105 *Re Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [12].
106 *Re Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [13].

Majestic had obtained consent from the complainant, this consent had been withdrawn simply by the complainant's verbal objections to the recording and uploading of the video footage.[107]

11.64 The third observation relates to the Purpose Limitation Obligation under s 18 of the PDPA, which limits the collection, use and disclosure of personal data to purposes that a reasonable person would consider appropriate in the circumstances. In *Re Majestic Debt Recovery Pte Ltd*, the PDPC found that, if the purpose of uploading the video footage was to "shame the debtor", such a purpose was unlikely to be one that a reasonable person would consider appropriate; therefore, even if Majestic had obtained consent, it would not have been at liberty to upload the video footage.[108] The PDPC appears here to have drawn a fairly clear line against the uploading of video footage for the purpose of shaming debtors,[109] and it remains to be seen whether this attitude against public shaming will extend to other situations unrelated to debt collection.[110]

C. Re Times Software Pte Ltd – *Subsidiary data intermediaries*

11.65 There may be situations where an organisation ("the data controller") outsources data processing operations to a data intermediary ("the primary data intermediary") who in turn further outsources data processing operations to another data intermediary ("the subsidiary data intermediary"). The concept of subsidiary data intermediary was developed and discussed by the PDPC in *Re Times Software Pte Ltd*.[111]

11.66 *Re Times Software Pte Ltd* involved three data controllers, namely "Dentons", "Red Hat" and "LIU". Each of these data controllers had, directly or indirectly, engaged the services of an IT services vendor ("Times"). The relationships among the parties are as follows: First, Times was directly engaged by Dentons to develop new functionality on payroll software used by Dentons. Dentons provided its employees' personal data to Times for this purpose. Second, Times was indirectly engaged by Red Hat and LIU: Red Hat and LIU had engaged a professional services

107 *Re Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [13].
108 *Re Majestic Debt Recovery Pte Ltd* [2020] SGPDPC 7 at [7] and [13].
109 This is similar to what the Office of the Privacy Commissioner has done in setting out certain "No-Go Zones": Office of the Privacy Commissioner of Canada, *Guidance on Inappropriate Data Practices: Interpretation and Application of subsection 5(3)* (May 2018). See also Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25 at 31–32.
110 The Personal Data Protection Commission appears to have taken a negative view towards shaming in previous cases: see *Club the Chambers* [2018] SGPDPC 24 at [22]; and *Jump Rope (Singapore)* [2016] SGPDPC 21 at [12].
111 [2020] SGPDPC 18. This decision was issued on 18 June 2020.

company ("TMF"), and TMF had in turn engaged Times in order to use its payroll software. TMF provided Times with the personal data of the employees of Red Hat and LIU, albeit only for a "one-time data migration exercise".[112]

11.67 As a result of certain failures on the part of Times, the personal data of some of the employees of the three data controllers were exposed online. The PDPC found that Times had breached the Protection Obligation under s 24 of the PDPA and the Retention Limitation Obligation under s 25 of the PDPA,[113] while Dentons and TMF had breached the Protection Obligation under s 24 of the PDPA.[114]

11.68 What is notable about *Re Times Software Pte Ltd* is the PDPC's conceptualisation and development of the concept of subsidiary data intermediary, although it was not directly applicable in this case. This appears to be the first PDPC decision in which the concept of subsidiary data intermediary was expressly discussed.

11.69 According to the PDPC, a subsidiary data intermediary is:[115]

> … an organisation who is a sub-contractor to a data intermediary, and who is sub-contracted to carry out data processing activities that are *directly related and necessary* to what the said data intermediary is supposed to undertake for an organisation (analogous to a data controller). [emphasis in original]

11.70 The facts of the present case may be used to illustrate the concept of subsidiary data intermediary: if, hypothetically, TMF had not merely used Times' payroll software, but outsourced its payroll processing operations to Times, then Times would have been a subsidiary data intermediary of Red Hat and LIU, since Times would be processing Red Hat's and LIU's employee personal data to provide the very payroll services that TMF was supposed to undertake for Red Hat and LIU.[116]

11.71 The PDPC set out the practical implications of the concept of "subsidiary data intermediary". It explained that "in situations where there are multiple layers of sub-contracting and sub-processing of personal data, there is a separate data controller and data intermediary relationship

112 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [30].
113 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [11] and [14].
114 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [26] and [37].
115 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [29].
116 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [28]–[30]. On the facts, Times was not a subsidiary data intermediary of Red Hat and LIU, since it was TMF itself who carried out the payroll processing, and TMF had only engaged Times in order to use Times' payroll software.

in each layer".[117] Accordingly, a data controller is not "responsible for its subsidiary data intermediary in the same way as it does for its primary data intermediaries"; instead, it is only the primary data intermediary who is responsible for the subsidiary data intermediary.[118]

11.72 Why is a data controller not responsible for its subsidiary data intermediary? An explanation is that the subsidiary data intermediary is not truly a data intermediary of the data controller.[119] Turning to the relevant provisions, s 2(1) of the PDPA defines "data intermediary" as "an organisation which processes personal data *on behalf of* another organisation", while s 4(3) of the PDPA provides that an "organisation shall have the same obligation under [the PDPA] in respect of personal data processed *on its behalf* and for its purposes by a data intermediary as if the personal data were processed by the organisation itself" [emphasis added]. On one reading of these provisions, it may be argued that a subsidiary data intermediary processes personal data not on behalf of the data controller, but only on behalf of the primary data intermediary by whom it was engaged. Even if the subsidiary data intermediary is processing personal data that originated from the data controller, this does not mean that the subsidiary data intermediary is in a data intermediary relationship with the data controller, because the subsidiary data intermediary is not processing that personal data *on behalf of* the data controller [emphasis added].

11.73 From a policy standpoint, it might also be argued that a data controller should not be made responsible for the failures of a subsidiary data intermediary, as it is the primary data intermediary (and not the data controller) who has effective control over the subsidiary data intermediary. As the PDPC noted, there are many outsourcing scenarios in which "the data controller may not even be aware that its primary data intermediary had engaged a sub-contractor, and hence it is in no position to influence its subsidiary data intermediary".[120] As such, making data controllers responsible for subsidiary data intermediaries could result in unexpected liability on data controllers. Further, insisting that data controllers monitor their subsidiary data intermediaries would raise the compliance costs of outsourcing data processing operations. This increase in cost would be quite unnecessary, since it would suffice for the primary data intermediaries to monitor the subsidiary data intermediaries. Therefore, it is submitted that it is justifiable to interpret ss 2(1) and 4(3)

117 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [31].
118 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [31]–[32].
119 This is consistent with the language used by the Personal Data Protection Commission in *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [31].
120 *Re Times Software Pte Ltd* [2020] SGPDPC 18 at [31].

of the PDPA as not making data controllers responsible for subsidiary data intermediaries, even though a stricter reading is possible.

D. Re Everlast Projects Pte Ltd – *Data protection in corporate groups*

11.74 For the sake of efficiency or for other reasons, a corporate group may decide to centralise certain personal data processing functions (for example, human resources), by assigning those functions to particular members within the corporate group. In *Re Everlast Projects Pte Ltd*,[121] the PDPC discussed how corporate groups engaging in such "internal outsourcing" of personal data processing can comply with their data protection obligations.

11.75 *Re Everlast Projects Pte Ltd* involved three organisations (namely "EPPL", "EIPL" and "ESPL") who were part of the same corporate group – they shared the same owner, directors and business premises. The three organisations centralised their payroll processing, putting the human resource department of EPPL in charge of payroll processing for all three organisations. Subsequently, EPPL suffered a ransomware attack, which affected a server on which the personal data of employees of all three organisations was stored.

11.76 In determining whether the organisations had breached their obligations under the PDPA, the PDPC took the opportunity to suggest how corporate groups in situations similar to that of the three organisations in question can fulfil their data protection obligations.

11.77 First, the PDPC found that the three organisations had breached the Accountability Obligation under s 12 of the PDPA.[122] On the facts, none of the organisations had any written data protection policies in place.[123] The PDPC suggested that within a corporate group, the Accountability Obligation could be met by having "binding group-level written policies or intra-group agreements that set out a common and binding standard for the protection of personal data across all organisations in the same corporate group".[124]

11.78 Second, the PDPC found that the three organisations had also breached the Protection Obligation under s 24 of the PDPA.[125] EPPL had

121 [2020] SGPDPC 20. This decision was issued on 30 October 2020.
122 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [14].
123 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [12].
124 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [13].
125 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [20] and [22].

failed to implement written IT security policies, did not install a firewall on the affected server, and did not conduct "periodic security reviews of its IT systems".[126] As for EIPL and ESPL, they were the data controllers of EPPL, who was their data intermediary for payroll processing; on the facts, EIPL and ESPL did not have any written contract with EPPL setting out EPPL's data protection responsibilities, nor did they supervise EPPL's personal data processing.[127]

11.79 In cases involving "internal outsourcing" of personal data processing within a corporate group, the PDPC suggested that the requirement for the data controller to have a written agreement with its data intermediary could be met by "binding group-level written policies, intra-group agreements" or binding corporate rules.[128] It also suggested that the requirement for the data controller to supervise its data intermediary could be met by having a "robust audit framework" (more suited for multi-national corporations), or by having the data intermediary explain its security measures with "appropriate documentation to evidence this process" and with "regular reports showing that it has put these processes in place" (more suited for small and medium-sized enterprises).[129]

11.80 Through its decision in *Re Everlast Projects Pte Ltd*, the PDPC provided useful guidance to corporate groups on ways by which they may fulfil their data protection obligations, and it provided some assurance that corporate groups can rely on group-level data protection policies, rather than maintaining separate data protection policies for each member of the corporate group.

126 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [21].
127 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [20].
128 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [18].
129 *Re Everlast Projects Pte Ltd* [2020] SGPDPC 20 at [19].