Published on e-First 7 July 2026

11. CONFIDENTIAL INFORMATION AND DATA PROTECTION

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

CONFIDENTIAL INFORMATION

I. Interplay between contract and equity

11.1 The General Division of the High Court ("General Division") delivered its decision in the case of *Hayate Partners Pte Ltd v Rajan Sunil Kumar*[1] ("*Hayate Partners*") on 14 March 2025.

11.2 The claimant was a financial institution in Singapore, while the defendant was the head of investor relations employed by the claimant. Clause 6 of the employment contract between the claimant and the defendant required the defendant to not retain material belonging to the claimant after the termination of their employment relationship.

11.3 On 8 December 2021, the defendant tendered his resignation. The claimant subsequently discovered that, prior to the resignation, the defendant had downloaded a large number of files from the claimant's information technology systems. The claimant alleged that the defendant had accessed and downloaded the files for purposes not related to his work, and had subsequently retained the files after the termination of his employment. These actions were, according to the claimant, in breach of the defendant's contractual and equitable obligations of confidence to the claimant.

11.4 The court found that, in relation to some of the downloaded files, the defendant had breached his contractual obligation of confidence (as set out in cl 6) by retaining the files after the termination of his employment. In addition, although cl 6 did not regulate the access and downloading of files, the court found that the defendant had also breached his equitable obligation of confidence by accessing and

1 [2026] 3 SLR 1.

downloading the files for non-work purposes and retaining them after the termination of his employment.[2]

11.5 The key point of interest in *Hayate Partners* arose from the defendant's argument that equity should not intervene in the face of a pre-existing express contractual obligation of confidence between the parties.[3] The court disagreed with this argument, holding that even if there was already an express contractual obligation of confidence owed by the defendant to the claimant, equity could still intervene to impose an equitable obligation of confidence that extended beyond the contractual obligation of confidence.[4] To determine whether the court should impose "additional or more extensive obligations of confidentiality in equity",[5] the court will adopt a "two-step inquiry":[6]

(a) It will first consider whether the contract specifies the "information to be treated as confidential and/or the extent and/or the duration of the obligations in respect of the information"[7] – if yes, then the court will ordinarily not impose "additional or more extensive obligations" in equity.

(b) However, the court may depart from this starting point if it would "plainly excite and offend a reasonable man's conscience that additional or more extensive obligations in equity are not so imposed".[8]

11.6 In this regard, the more "definite" the contractual obligation of confidence, the less likely it is that there will be imposed "additional or more extensive obligations" in equity; this is because, where the parties have made clear their intentions as to the scope of the contractual obligation of confidence, it will be more difficult for the claimant to argue that the defendant's conscience ought to be bound to a wider obligation of confidence in equity.[9]

11.7 The court applied its two-step inquiry as follows:[10]

(a) First, the employment contract failed to clearly define the scope of the information to be protected. Presumably, this meant that the starting point (*ie,* that the court would ordinarily

2 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [161]–[162].
3 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [43].
4 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [50].
5 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [52].
6 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [52].
7 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [52(a)].
8 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [52(b)].
9 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [53].
10 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [54]–[57].

not impose additional or more extensive obligations in equity) was inapplicable.

(b) Second, although the employment contract did not restrict the access and download of confidential information, equity imposed obligations to that effect. Such obligations were, in fact, not "additional or more extensive obligations", but were regarded as "pre-cursors to using, disclosing and/or retaining"[11] of the confidential information. Furthermore, even if they were "additional or more extensive obligations", it would "plainly excite a reasonable man's conscience"[12] if these obligations were not imposed on the defendant, who was only authorised to access and download the files for work purposes.

11.8 Accordingly, an equitable obligation of confidence was imposed on the defendant.

11.9 The two-step inquiry presented by the court in *Hayate Partners* provides useful guidance on the interplay between contract and equity in the law of confidence. Certainly, it serves as a reminder to contracting parties to ensure that the obligations of confidence contained in their contracts are set out in a clear and comprehensive manner, to avoid the unexpected imposition of additional equitable obligations of confidence. On a theoretical level, the two-step inquiry strives to align distinct goals in contract law and in equity, which are, respectively, (a) to give effect to the objective intentions of contracting parties; and (b) to intervene against unconscionable conduct.

DATA PROTECTION

I. Implied consent and concept of "disclosure"

11.10 The Personal Data Protection Commission ("PDPC") delivered its decision in the case of *Re Institute of Mental Health*[13] ("*Re IMH*") on 21 May 2025.

11.11 In this case, the organisation was a mental health institute, and the complainant was a patient of the organisation.

11 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [56].
12 *Hayate Partners Pte Ltd v Rajan Sunil Kumar* [2026] 3 SLR 1 at [57].
13 [2025] SGPDPC 1.

11.12 The organisation was involved in a research study about certain medical conditions. A research officer of the organisation was engaged in that research study. To obtain suitable research subjects for the research study, the research officer went to one of the organisation's doctors and asked for the names of patients who fit a certain "age group and medical profile".[14] The doctor gave the research officer some names, including the name of the complainant.

11.13 On 20 March 2024, the complainant visited the organisation. While he was waiting in a waiting area, the research officer approached him, identified him by his full name, and sought his participation in the research study.

11.14 The complainant was aggrieved that the doctor had disclosed his personal data, including his "name and health condition and/or history",[15] without having obtained his consent. He proceeded to submit a complaint to the PDPC about the organisation.

11.15 In this case, the relevant data protection obligation was the Consent Obligation. The Consent Obligation requires organisations to obtain consent from an individual before collecting, using, or disclosing his personal data.[16] This consent may be actually given by the individual ("actual consent") or may in some circumstances be deemed to be given by the individual ("deemed consent").

11.16 The PDPC found that the organisation had obtained actual consent from the complainant to use his personal data for the purpose of recruiting him as a research subject for the research study.[17] Under s 14(1) of the Personal Data Protection Act 2012[18] ("PDPA"), for actual consent to be valid, the individual must (a) be notified of the purpose for the collection, use, or disclosure of his personal data; and (b) have provided his consent for that purpose. In this case, although the complainant did not provide *express* actual consent, he had provided *implied* actual consent. The actual consent was implied from the facts that (a) the organisation had, in its premises, prominently displayed a notification which stated that the organisation would use its patients' personal data for the purposes of research study recruitment;[19] (b) the complainant had "ample reasonable opportunities"[20] to read the

14 *Re Institute of Mental Health* [2025] SGPDPC 1 at [4].
15 *Re Institute of Mental Health* [2025] SGPDPC 1 at [2].
16 Personal Data Protection Act 2012 (2020 Rev Ed) s 13.
17 *Re Institute of Mental Health* [2025] SGPDPC 1 at [27].
18 2020 Rev Ed.
19 *Re Institute of Mental Health* [2025] SGPDPC 1 at [5] and [14].
20 *Re Institute of Mental Health* [2025] SGPDPC 1 at [15].

notification during his visits to the organisation;[21] and (c) despite having notice of the organisation's use of his personal data for the purposes of research study recruitment, the complainant continued to visit the organisation, continued to provide his personal data, and "never objected to the use of his personal data"[22] for the purposes of research study recruitment.[23]

11.17 As such, the PDPC found that the organisation was not in breach of the Consent Obligation.

11.18 In addition, the PDPC also found that the organisation could not rely on deemed consent by notification. Under s 15A of the PDPA, an individual is deemed to have given consent if the following conditions are met:

(a) The organisation conducted an assessment to determine that the collection, use, or disclosure is "not likely to have an adverse effect on the individual".[24]

(b) The organisation took reasonable steps to inform the individual about the purposes of the collection, use, or disclosure.

(c) The organisation gives the individual a reasonable period and reasonable means to object to the collection, use, or disclosure, and takes reasonable steps to inform the individual about that period and means.

(d) The individual does not object to the collection, use, or disclosure.

11.19 In this case, it was plain that the organisation did not take reasonable steps to inform the complainant about the means by which he could object to the use of his personal data for research study recruitment, and the period within which he could so object.[25] In this regard, although the organisation did create channels of communication through which the complainant could have raised an objection (namely, through their data protection officer or their customer service staff), the mere provision of such channels was "insufficient as they place the onus on the individual to navigate the Organisation's bureaucracy to find out how he may opt out".[26]

21 *Re Institute of Mental Health* [2025] SGPDPC 1 at [15].
22 *Re Institute of Mental Health* [2025] SGPDPC 1 at [16(a)].
23 *Re Institute of Mental Health* [2025] SGPDPC 1 at [16].
24 Personal Data Protection Act 2012 (2020 Rev Ed) s 15A(4)(*a*).
25 *Re Institute of Mental Health* [2025] SGPDPC 1 at [23].
26 *Re Institute of Mental Health* [2025] SGPDPC 1 at [24]–[25].

11.20 There are two notable points about *Re IMH*.

11.21 First, in this case, the PDPC clarified that the internal sharing of personal data within an organisation (*eg*, between one employee and another employee, or between one department and another department) does not constitute a "disclosure" of that personal data.[27] In other words, personal data is disclosed by an organisation only if the personal data was shared with a third party. Thus, there was no "disclosure" of the complainant's personal data by the organisation, since the personal data was shared between members of the organisation.

11.22 This clarification has practical significance. It is true that, in *Re IMH*, it was of no practical significance whether the organisation's conduct could be characterised as "disclosure" (because the Consent Obligation applies to both "disclosure" and "use" of personal data).[28] However, in cases where the applicable PDPA provision pertains specifically to the disclosure of personal data, clarity about the meaning of "disclosure" will be important. One example of such a provision is s 48D of the PDPA, which criminalises the unauthorised disclosure of personal data.

11.23 Second, *Re IMH* illustrates the interaction between (a) implied actual consent; and (b) deemed consent by notification. Deemed consent by notification is the prescribed method through which "opt-out" consent (*ie*, consent that is assumed from the lack of an objection from the individual) may be obtained under the PDPA, subject to the safeguards discussed above. However, at first glance, it appears from this case that opt-out consent may also be obtained as implied actual consent, and without the same safeguards. This raises the question of whether implied actual consent renders deemed consent by notification otiose. It is submitted that the answer is no, because the better view of implied actual consent is that it only encompasses "opt-in" consent (*ie,* consent that is given through some positive action by the individual). In this case, the implied actual consent given by the complainant was really opt-in consent, because the consent was implied not only from his omission to object to the organisation's use of his personal data, but also from his continued visitation of the organisation and his continued provision of his personal data – both positive actions by the complainant.

27 *Re Institute of Mental Health* [2025] SGPDPC 1 at [6].
28 *Re Institute of Mental Health* [2025] SGPDPC 1 at [8].

II. Preservation of personal data subject to access request

11.24 The PDPC delivered its decision in the case of *Re The Management Corporation – Strata Title Plan No 4599*[29] ("*Re MCST 4599*") on 19 May 2025.

11.25 In this case, the organisation was the management corporation of a condominium. At the material time, the organisation had appointed a managing agent and a security company (which controlled closed-circuit television ("CCTV") cameras around the condominium). The complainant was an individual who was involved in a traffic accident along a road next to the condominium. On 25 April 2024, the complainant wrote to the managing agent to request access to the video footage of the accident recorded on the condominium's CCTV cameras. However, the managing agent and the security company were unable to download the video footage, and by 30 April 2024 the video footage had been automatically overwritten. On 2 May 2024, the managing agent informed the complainant of the organisation's refusal of his access request. Subsequently, the complainant complained to the PDPC that the organisation had wrongfully refused his access request and had failed to preserve the relevant personal data sought by the complainant.

11.26 The key obligation the PDPC considered was the Access Obligation under s 21 of the PDPA, which requires an organisation to provide an individual with access to his personal data that is in the possession or under the control of the organisation. Here, the PDPC took the view that it was unable to determine whether the organisation was required to provide the complainant with access to the video footage, because the video footage had already been deleted.[30]

11.27 There is an ancillary obligation to the Access Obligation, set out under s 22A of the PDPA, which provides that if an organisation refuses an access request, then the organisation must preserve a copy of that personal data for 30 days after the date of refusal. However, this ancillary obligation was also not breached by the organisation in *Re MCST 4599* because the organisation deleted the video footage *before*, not *after*, refusing access.[31]

29 [2025] SGPDPC 3.

30 *Re The Management Corporation – Strata Title Plan No 4599* [2025] SGPDPC 3 at [11].

31 *Re The Management Corporation – Strata Title Plan No 4599* [2025] SGPDPC 3 at [18].

11.28 Another obligation the PDPC considered was the Accountability Obligation. The Accountability Obligation requires organisations to implement data protection policies and appoint data protection officers. In this case, the Accountability Obligation was breached because the organisation had failed to implement a data protection policy (including procedures on handling access requests) and did not appoint a data protection officer.[32]

11.29 *Re MCST 4599* is of interest because it illustrates an apparent lacuna in the Access Obligation, and how this apparent lacuna is addressed (at least in part) by the Accountability Obligation. The apparent lacuna arises because it seems that an organisation that wishes to avoid complying with the Access Obligation may simply delete the personal data before refusing the access request. However, an organisation that does so may well be found to have breached the Accountability Obligation for failing to implement a data protection policy that governs how the organisation ought to deal with access requests. An open question nevertheless remains as to the position of an organisation that (a) does have a data protection policy addressing access requests; but (b) deletes the personal data requested, in breach of its own policy. In such a case, there are at least two potential results:

(a) If the deletion was done inadvertently by the organisation (*ie,* by a staff member who failed to follow the organisation's policy), then it is possible that the organisation will be found to have breached the Accountability Obligation because it failed to effectively communicate its data protection policy to its staff.

(b) If the deletion was done deliberately by the organisation (*ie*, the organisation instructed its staff to delete the personal data), then perhaps an adverse inference may be drawn on the basis that the organisation was clearly attempting to evade having to provide access (the inference being that the deleted personal data was data that the individual was entitled to access), thereby permitting a finding of breach of the Access Obligation.

III. Financial penalty

11.30 The PDPC delivered its decision in the case of *Re Marina Bay Sands Pte Ltd*[33] on 28 October 2025.

32 *Re The Management Corporation – Strata Title Plan No 4599* [2025] SGPDPC 3 at [22]–[25].
33 [2025] SGPDPC 6.

11.31 The organisation in this case was an integrated resort. It suffered a data breach resulting in the exfiltration of the personal data of about 665,495 members of the organisation's membership programme. The threat actor was able to execute the exfiltration because the organisation's employee had made a configuration error while migrating to a new software platform, thereby creating a vulnerability that the threat actor was able to exploit.

11.32 The PDPC found that the organisation had breached the Protection Obligation. The Protection Obligation is set out in s 24 of the PDPA, which provides that organisations must make reasonable security arrangements to prevent the unauthorised processing of personal data in the possession or under the control of the organisation. Here, the organisation failed to implement security arrangements for the software migration exercise, and instead relied entirely on the employee to protect personal data.[34]

11.33 In its preliminary decision, the PDPC imposed a financial penalty of $450,000 on the organisation.[35] However, this was reduced to $315,000 in the final decision, in consideration of some of the representations made by the organisation.[36]

11.34 The key point of interest in this case is that, to refute a representation made by the organisation that the PDPC "had determined the preliminary financial penalty arbitrarily and without reference to any objective computational framework",[37] the PDPC set out a comprehensive framework for its assessment of financial penalties.[38] This framework is summarised below:[39]

(a) Preliminary step: The PDPC will determine the maximum financial penalty imposable in the case at hand. This is derived from the statutory maximum financial penalty, to which a modifier is applied based on the nature of the organisation's breach.

(b) Step 1: The PDPC will determine the level of culpability and level of harm.

(c) Step 2: Based on the level of culpability and level of harm, the PDPC will determine the starting financial penalty.

34 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [18]–[24].
35 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [37].
36 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [122].
37 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [87].
38 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [87].
39 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [95]–[108].

(d) Step 3: The PDPC will adjust the starting financial penalty based on relevant mitigating and aggravating factors.

(e) Step 4: The PDPC may adjust the financial penalty to ensure that it does not "adversely affect the organisation's ability to continue its usual activities".[40]

(f) Step 5: The PDPC will make final adjustments to the financial penalty to "ensure that the proposed financial penalty is effective and proportionate".[41]

11.35 This was the framework that the PDPC applied to determine the organisation's financial penalty in its final decision.[42] First, at the preliminary step, the PDPC identified the maximum financial penalty imposable, which was 10% of the organisation's annual turnover multiplied by an unstated percentage rate (the percentage rate being based on the fact that the breach was negligent in nature). Second, at Step 1, the PDPC determined that the organisation's culpability was low, while the level of harm was moderate. Third, at Step 2, the PDPC determined the starting financial penalty within the low-moderate band. Fourth, at Step 3, to account for certain mitigating factors (including the organisation's voluntary notification of the breach, the organisation's prompt remedial actions, and the organisation's co-operation with the PDPC's investigations), the PDPC reduced the financial penalty to $315,000. Fifth, at Step 4, the PDPC considered that the financial penalty would not adversely affect the organisation's ability to continue its usual activities, and so no adjustment was made. Sixth, at Step 5, the PDPC considered that no final adjustments were necessary. Accordingly, the organisation was issued a financial penalty of $315,000.

11.36 It goes without saying that the elaboration of this financial penalty framework by the PDPC is significant. It should, however, be observed that the framework does represent a partial departure from the PDPC's decision-making process in previous decisions. For example, the culpability of the organisation was previously regarded as an aggravating factor,[43] but is now elevated to a primary determinant of the financial penalty to be considered in Step 2. Nevertheless, it is submitted that this is a salutary departure that provides greater clarity to organisations about how financial penalties for breaches of the PDPA are calculated.

40 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [107].
41 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [108].
42 *Re Marina Bay Sands Pte Ltd* [2025] SGPDPC 6 at [109]–[121].
43 See, *eg*, *Eatigo International Pte Ltd* [2022] SGPDPC 9 at [27].

IV. Deemed consent

11.37 The General Division delivered its decision in the case of *Piper, Martin v Singapore Kindness Movement*[44] on 29 August 2025.

11.38 The appellant was an individual who had sent e-mails to the respondent, complaining about the conduct of a third party, Carol Loi Pui Wan ("Loi"), who was affiliated with the respondent. In the course of dealing with the appellant's complaint, the respondent disclosed the appellant's identity to Loi. Loi proceeded to commence proceedings against the appellant for harassment and publicised her claim on Facebook. The appellant later received threatening messages.

11.39 The appellant brought private action under s 48O of the PDPA against the respondent, in the District Court. The appellant alleged that the respondent had disclosed his personal data without his consent. The District Court dismissed the appellant's claim, because the appellant had disclosed his personal data to the respondent when making his complaint against Loi, and was therefore deemed to have consented to the disclosure of his identity by the respondent for the purpose of acting on his complaint. In addition, the District Court found that there was no direct causal connection between the respondent's alleged breach of the PDPA and any alleged harm suffered by the appellant, and that the appellant had not proved the emotional distress that he claimed to have suffered, which meant that the appellant did not have standing to sue under s 48O of the PDPA.

11.40 The District Court accordingly dismissed the appellant's claim. The appellant then appealed to the General Division, which ultimately dismissed the appeal because it agreed with the District Court's finding that the appellant had no standing to sue.

11.41 However, it is interesting to note the General Division's disagreement with the District Court on the issue of deemed consent. Here, the General Division found that the appellant could not in fact be deemed to have consented to the disclosure of his personal data by the respondent. The relevant provision here is s 15(1) of the PDPA, which provides that an individual may be deemed to consent to the collection, use, or disclosure of his personal data for a purpose if (a) he voluntarily provided the personal data to the organisation for that purpose; and (b) it was reasonable that he would voluntarily provide that personal data. Here, it was clear that both requirements were met: the appellant voluntarily provided his name and e-mail address to the respondent for the purpose

44 [2025] 5 SLR 293.

of investigating his complaint against Loi, and it was reasonable for him to have done so.[45] However, the respondent had nevertheless exceeded the scope of the consent given by the appellant when it disclosed his personal data to Loi, because the scope of consent deemed pursuant to s 15(1) of the PDPA is limited to that which is reasonable for the purpose, and in this case it was "completely unnecessary, and hence unreasonable"[46] for the respondent to disclose the appellant's personal data to Loi when conducting its investigations.[47] As such, the respondent was in breach of the Consent Obligation under the PDPA when it disclosed the appellant's personal data to Loi.

11.42 Thus, what this case clarifies is that an individual's deemed consent for a particular purpose does not *confer* upon the organisation a blank cheque to use or disclose the individual's personal data in any way it likes in relation to that purpose – the organisation is held to "an objective standard of reasonableness".[48] It is submitted that this is a necessary limitation that was left unstated in s 15(1) of the PDPA. This is in line with the "overarching standard of reasonableness" that is imposed on organisations under ss 11(1) and 18(*a*) of the PDPA.[49]

---

45 *Piper, Martin v Singapore Kindness Movement* [2025] 5 SLR 293 at [54]–[60].
46 *Piper, Martin v Singapore Kindness Movement* [2025] 5 SLR 293 at [65].
47 *Piper, Martin v Singapore Kindness Movement* [2025] 5 SLR 293 at [63]–[65].
48 *Piper, Martin v Singapore Kindness Movement* [2025] 5 SLR 293 at [63].
49 *Piper, Martin v Singapore Kindness Movement* [2025] 5 SLR 293 at [50]–[53].