The purpose of publishing AAB's decisions in PCPD's website is primarily to promote awareness and understanding of, and compliance with, the Personal Data (Privacy) Ordinance. The general practice of PCPD is to upload AAB's decisions on an "as is" basis. Use of any personal data contained in AAB's decisions for any other purpose may constitute a breach of the Personal Data (Privacy) Ordinance.

(Please read the FULL VERSION of the above on the webpage of AAB Decisions)

ADMINISTRATIVE APPEALS BOARD
ADMINISTRATIVE APPEAL NO. 46/2022

BETWEEN

EC HEALTHCARE Appellant

and

PRIVACY COMMISSIONER FOR PERSONAL DATA Respondent

Coram: Administrative Appeals Board

- Mr Jenkin Suen, SC (Deputy Chairman)
- Mr Ernest Chan Ho-sing (Member)
- Ms Christine Yung Wai-chi (Member)

Date of Hearing: 27 September 2023

Date of Handing down Written Decision with Reasons: 26 February 2025

DECISION

A. INTRODUCTION

1. This is an appeal ("the Appeal") by EC Healthcare ("the Appellant") against the decision of the Privacy Commissioner for Personal Data ("the Commissioner" or "the Respondent") to serve on the Appellant an Enforcement

Notice (as contained in the Investigation Report scheduled to be published on 14 November 2022 (No. R22-13928) ("the Investigation Report")) on 11 November 2022 ("the Decision").

2. In gist, the Decision is premised on findings of cross-brand access to and use of clients' personal data in the Appellant's information system ("System") in breach of Data Protection Principle 3(1) ("DPP3(1)") under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO").

3. The Appellant's stance and arguments are set out in (i) Notice of Appeal dated 25 November 2022 ("NOA"), (ii) Appellant's Reply dated 2 March 2023 ("Reply") and (iii) Appellant's Skeleton Submissions dated 12 September 2023 ("A's Skel").

4. Further, on behalf of the Appellant, Mr Lu Lyn Wade Leslie ("Mr Lu"), Co-Chief Executive Director of the Appellant, made a witness statement together with (i) a one-page slide as Annex 1 to explain the operation of the Appellant's System with regard to those personal data which may be used across various brands and (ii) the meeting minutes prepared by the Appellant for the site visit on 14 June 2022 ("the Site Visit") as Annex 2 to facilitate explanation of the points discussed and raised in the Site Visit.

5. On the other hand, the Commissioner's stance and arguments are set out in (i) Commissioner's Statement dated 28 December 2022 ("Defence") and (ii) Commissioner's Skeleton Submissions dated 19 September 2023 ("R's Skel").

6. Further, on behalf of the Commissioner, Ms Natalie Yung (容潔瑩) ("Ms Yung"), Personal Data Officer of the Office of the Privacy Commissioner for Personal Data ("PCPD"), made a witness statement in response to Mr Lu.

7. The substantive hearing for the Appeal took place on 27 September 2023.

8. During the hearing, Mr Lu testified on behalf of the Appellant. Exhibits 1 to 4 were also produced to the Administrative Appeals Board ("the Board") in the course of Mr Lu's oral testimony. Thereafter, Ms Yung testified on behalf of the Commissioner.

9. After the close of evidence, the parties have made oral closing submissions. Although leading Counsel for the Appellant indicated he had prepared written closing submissions in advance, he confirmed upon completing his oral submissions that he did not consider it necessary to produce the same.

B. THE DECISION

10. The factual premises and reasonings of the Decision are set out in the Investigation Report.

11. First of all, the Commissioner primarily relied on the investigations of two complaints (respectively "Case (1)" and "Case (2)"), the Site Visit on 14 June 2022, visits to two branches of the Appellant's brands (namely New York Medical Group ("NYMG") and re:HEALTH) and written replies from the Appellant for her findings. These are summarised in the Executive Summary of the Investigation Report ("Executive Summary") as follows:

"Background

1. The Office of the Privacy Commissioner for Personal Data ("PCPD") received two complaints lodged by citizens on 10 June and 26 August 2021 respectively. Both complaints were made against the brands under EC Healthcare, namely, Primecare Paediatric Wellness Centre ("Primecare"), Dr Reborn, New York Medical Group ("NYMG") and re:HEALTH.

Investigation Case (1)

2. In the first case, which took place in June 2018, Complainant A took her daughter (the "Daughter") to a Primecare clinic at Ocean Centre in Tsim Sha Tsui to consult a doctor (the "Doctor"). Upon registration, Complainant A provided the personal data of herself and the Daughter, and the phone number of the grandmother of the Daughter (the "Grandmother") for contact purpose.

3. In 2020, the Grandmother, who had been using the services provided by Dr Reborn, received a text message from Dr Reborn. The Grandmother noted that the message included the Daughter's name, and hence made inquiries with Dr Reborn. The Grandmother was told that since the Doctor joined Dr Reborn, the personal data of his clients had also been transferred to Dr Reborn.

4. Having learnt about the incident from the Grandmother in 2021, Complainant A lodged a complaint to the PCPD in June.

Investigation Case (2)

5. In another case, in March 2016, Complainant B received chiropractic treatments at an NYMG centre, which was located at Humphreys Avenue in Tsim Sha Tsui at the material time, and he provided his personal data to NYMG.

6. In July 2021, Complainant B contacted a staff of re:HEALTH (the "Staff") by phone to follow up a complaint lodged by a member of his family against re:HEALTH, during which he provided his surname and phone number. Thereafter, the Staff called back Complainant B and addressed him by his full name.

7. Since Complainant B had never been in touch with the Staff, he questioned how the Staff had known his full name. The staff explained that since the complainant had previously used the service of NYMG, which was also under EC Healthcare, and the Staff was able to access the database of all clients of EC Healthcare, the Staff can thus access Complainant B's full name in the computer system. In addition to that, the Staff could tell the date when Complainant B visited NYMG.

8. Dissatisfied with such access by re:HEALTH to his record of medical visit(s) with NYMG, Complainant B lodged a complaint with the PCPD.

Investigation

9. Given that the four organisations involved in the matters complained of are all brands under EC Healthcare, and that replies to the preliminary inquiry made with Primecare by the PCPD were provided by EC Healthcare, the PCPD commenced investigations in respect of the two subject complaints against EC Healthcare on 6 August and 11 November 2021 respectively, in accordance with section 38(a)(i) of the Personal Data (Privacy) Ordinance (the "Ordinance").

10. During the investigation, the PCPD received several written replies from EC Healthcare. The PCPD also visited the office of EC Healthcare at Langham Place in Mong Kok to make inquiries with the representatives of EC Healthcare and obtain from them information pertinent to the cases. Additionally, the PCPD conducted site inspections at branches of two of the brands under EC Healthcare."

12. Secondly, the Investigation Report acknowledged that records of the two complaints may not be available but stressed that the totality of evidence points to the sharing, disclosure and use of clients' personal data across the brands of the Appellant (at §§84-86). As summarised in the Executive Summary:

"*Sharing, Disclosure and Use of Clients' Personal Data by The System*

22. In both complaints, the personal data in question was collected years ago, and records of how such collection took place may not be available. Besides, there is no actual record in Case (1) to prove whether the Daughter's name was included in the text message.

Notwithstanding the above, it is revealed from the information obtained during the investigations of both cases, the inquiries and the site visits conducted by the PCPD that the frontline staff of the 28 brands are able to make cross-brand access to and use of clients' personal data in the System. It did not involve unauthorised or accidental access to personal data, as it was indeed an intended arrangement of EC Healthcare for its business operation purposes.

23. As far as Case (1) is concerned, EC Healthcare confirmed that after the staff of Dr Reborn enter the Grandmother's phone number into the System, the information of both the Daughter and the Grandmother returned. According to the screen captures provided by EC Healthcare, the membership number, name and medical records of the Daughter would also be displayed. As regards Case (2), after the staff of re:HEALTH input Complainant B's phone number, the staff would know that Complainant B was also a member of EC Healthcare and could tell his full name, his consultation records at NYMG, as well as the name and insurance policy information of his mother. However, Complainant B had never provided the aforementioned information to re:HEALTH.

24. Thus, when a frontline staff of the 28 brands adopting the System checks the records of a particular client of its own brand, he/she could also read that client's records of using the services of other brands of EC Healthcare, including the personal data collected by those other brands. In other words, the System is featured with the sharing and transfer of clients' personal data, with the clients'

personal data of one brand being disclosed to the staff of other brands for their access and use."

13. Thirdly, the Commissioner relies on various written replies from the Appellant, including a table setting out the access rights of different types of staff of the Appellant (i.e. Table 13 at §50 of the Investigation Report). Such table originates from the table contained in Appendix I to the Appellant's letter dated 8 August 2022 (under Answer (13) in response to the Commissioner's letter dated 8 July 2022).

14. Fourthly, the Commissioner relies on visits paid to two branches of the Appellant's brands, including a branch of NYMG and a branch of re:HEALTH. During such visits, the staff confirmed that they are able to gain access to cross-brand personal data although, to be fair, the staff at the branch of NYMG asked for the consent of the Commissioner's staff before obtaining access to his personal data at another brand (see §§63-74 of the Investigation Report).

15. Fifthly, the Commissioner proceeded to find the Appellant in contravention of DPP3(1). As summarised in the Executive Summary:

"*EC Healthcare Failed to Inform Existing Clients Before Acquisitions of the Possible Use of Their Personal Data*

25. The Daughter and Complainant B were the Existing Clients Before Acquisitions of Primecare and NYMG respectively prior to their acquisitions by EC Healthcare.

26. After the acquisitions, EC Healthcare stored the personal data of Existing Clients Before Acquisitions (including that of the Daughter and Complainant B) in the System. Hence, frontline staff of other brands under EC Healthcare using the System could access personal data of the relevant clients as well. However, since the acquisitions took place and over the course of the present investigations, EC Healthcare had never informed the Existing Clients Before Acquisitions of the relevant acquisitions by any means, nor provided them with the Privacy Policy of EC Healthcare. As such, Existing Clients Before Acquisitions were not informed that their personal data had been stored in the System and were accessible by the staff of other brands under EC Healthcare, and EC Healthcare had never sought any consent from the Existing Clients Before Acquisitions in respect of such arrangement.

EC Healthcare Contravened Data Protection Principle 3(1)

27. Data Protection Principles 3(1) and (4) of Schedule 1 to the Ordinance stipulates that personal data, without the express and voluntary consent of the data subject, shall only be used (including disclosure and transfer) for the purpose for which the data was to be used at the time of the collection of the data, or a purpose directly related to that purpose.

28. Based on the information provided by EC Healthcare, Primecare at first collected the Daughter's personal data for the purpose of providing medical services, without explicitly stating the purpose of such collection of the data and the classes of persons to whom the

data may be transferred. Meanwhile, upon the collection of Complainant B's personal data, NYMG had only informed Complainant B that the personal data collected would be used in the provision of treatment and dissemination of healthcare newsletters, without mentioning the classes of persons to whom the data may be transferred.

29. Subsequently, after acquiring Primecare and NYMG, EC Healthcare stored the personal data of the clients of these two brands (including those of the two complainants) in the System, and shared parts of their personal data among the 28 brands of EC Healthcare using the System, so that the relevant personal data were accessible by the frontline staff of various brands. As a result, the personal data originally provided by them to a single brand was disclosed and transferred, without their knowledge, to the staff of some other brands. The Privacy Commissioner for Personal Data (the "Commissioner") finds that the above arrangement was plainly inconsistent with the original purpose of collection of the complainants' personal data, and also fell short of their reasonable expectation for personal data privacy.

30. In addition, after acquiring Primecare and NYMG, EC Healthcare failed to obtain consents from the two complainants to the use, disclosure and transfer of their personal data among the various brands within the group, and never informed them by any means that their personal data would be stored in the System. Such practices are disappointing both from the perspective of compliance with legal requirements or that of respecting clients' wills.

31. In the circumstances, the Commissioner is of the opinion that EC Healthcare has contravened the requirements of Data Protection Principle 3(1) on the use (including disclosure and transfer) of personal data.

32. The Commissioner considers that, as an established listed company, EC Healthcare should possess adequate resources and capabilities to formulate comprehensive policies and operation plans (such as carrying out a Privacy Impact Assessment for the System), so as to ensure that the design of the System, and the policies and practices of sharing clients' personal data are in compliance with the requirements under the Ordinance. However, the two complaints reveal that in undertaking mergers and acquisitions for market consolidation, and in collating clients' personal data of its various brands through the System, EC Healthcare disregarded the requirements under the Ordinance on the use (including disclosure and transfer) of personal data and failed to duly consider how the operation of the System may impact clients' personal data privacy. The Commissioner expresses regret at the above shortcomings."

16. Sixthly, the Commissioner then directed enforcement actions and made recommendations as more particularly set out in the Investigation Report.

C. GROUNDS OF APPEAL

17. It is common ground between the parties that the nature of the Appeal is a *de novo* hearing by way of rehearing on the merits, and the appellant has to say

why the decision below is wrong and the tribunal/board will address these grounds of appeal: see *Li Wai Hung Cesario v Administrative Appeals Board* (CACV 250/2015, 15 June 2016) per Cheung JA at §§6.1, 6.2, 7.6; *Ko Siu Luen v Appeal Tribunal (Buildings)* [2012] 1 HKLRD 149 per Au J (as he then was) at §§52-55; *Happy Pacific Ltd v Commissioner of Police* (HCAL 115/1999, 11 November 1999) per Stock J (as he then was) at p.14.

18. In gist, the Appellant relies on 3 grounds of appeal:

(1) The Commissioner erred in finding that frontline staff of the Appellant's brands are able to make cross-brand access to and use of clients' personal data in the Appellant's System ("Ground 1");

(2) The Commissioner erred in finding there was contravention of DPP3(1) ("Ground 2"); and

(3) Procedural irregularities leading to the Decision ("Ground 3").

19. At the hearing of the Appeal, Mr Lu also testified in support of the above.

D. ANALYSIS – GROUND 1

20. In respect of Ground l, the Appellant's contentions are set out in §§1-3 of the NOA, §§19-47 of the Reply, and Section E1 of A's Skel. Specifically, in §2 of the NOA, the Appellant contends that the Commissioner's findings are contradicted by various matters including *inter alia* the following:

(1) The Appellant and its brands/ subsidiaries, including Primecare and NYMG, were operationally separate and independent, and the customer data of the brands/subsidiaries were limited to be used by each brand/subsidiary and partitioned, unless specified types of staff had specific legitimate needs to use the personal data of the customers in order to provide service or due to operational needs;

(2) Primecare Paediatric Wellness Centre ("Primecare") operated under the business model of "Customer Service & Proposition Integration", whereby it adopted the Appellant's membership approach following the customers' proper acceptance of the Appellant's privacy policy;

(3) NYMG was operating under the business model of "Back-Office Integration", whereby customer data from different businesses were separately stored in partition and are not integrated under a single user profile;

(4) The screenshots and demonstration of the usage of the portal of the System were solely for the purpose of allowing the Commissioner's office to understand the full operation of the System during their investigation;

(5) Under the System, staff members could only view the specific information on a need-to-know basis, all personal data held in the portal were redacted and partitioned, and no access rights were granted to unrelated members;

(6) Clients and potential clients might have provided the Appellant with the same telephone number as contact for multiple customers, which might have caused confusion for customer service staff;

(7) In Case (1), there is no actual record to prove whether the name of the daughter of Complainant A was in fact included in the text message;

(8) In Case (2), during the visit of an officer of the Commissioner to NYMG in July 2022, only when the said officer gave consent to check the officer's information with another brand, that the staff would proceed.

21. Mr Lu also made a witness statement and testified to the following effect:

(1) An operating system is set up for the Appellant which works at different layers, the personal data of the customers of each brand is not necessarily shared across different brands;

(2) Where a brand is acquired by the Appellant following mergers and acquisitions ("M&A"), cross-brand access of its customers' personal data would be allowed only after the customers agreed and consented to the Appellant's privacy policy and depending on the business operation model where the Appellant may or may not be appointed as the service provider to carry certain back-office functions;

(3) For those customers who did not agree to the Appellant's privacy policy, only the staff of the relevant brands could access their

personal data. Their personal data would not be accessible by the staff of other brands, or the back-office staff managing the cross-brand data who did not need to know such data;

(4) Further, even where the customers had consented to the Appellant's privacy policy and therefore allowed cross-brand access, not all staff of the Appellant would be given free access to the personal data of the clients of all brands. Instead, a multi-level operation system was put in place to regulate how the personal data stored under the cross-brand database could be accessed and used, as explained under paragraph 23 of the Reply; and

(5) For illustration purposes, Mr Lu has prepared a one-page slide as Annex 1 to his statement. Among others, insofar as front-line staff are concerned: (i) modules and functions are controlled by access right based on staff's functional roles, (ii) staff's access to customer data is restricted to need-to-know basis, governed by the Appellant's data governance policies, and (iii) staff's access to any brand's customer data requires explicit consent to the Appellant's personal information collection statement ("PICS").

22. Further, Mr Lu testified that the officers of the Commissioner were unable to correctly understand the operation of the Appellant's System during the Site Visit. Among others, he said that:

(1) During the Site Visit, they were asked by officers of the Commissioner for a demonstration of the frontline portal accessible by their frontline staff;

(2) For illustration purposes, they shared multiple screenshots to demonstrate how they conducted data management across customers who had or had not accepted their group's privacy policy under various scenario;

(3) One of the shared screenshots involved a customer profile which belonged to their IT staff with full access rights and who had accepted the Appellant's privacy policy. As such, her data could be accessed across the brands;

(4) It was emphasized that the demonstration was not representative in respect of all customers under the Appellant. Where the relevant customer had not consented to the Appellant's privacy policy, their personal data would be stored separately and could not be accessed by the staff of other brands. Further, even where cross-brand access was permitted following the customer's consent, it would be on a need-to-know basis based on operation needs.

23. Moreover, whilst the screenshots previously provided by the Appellant (e.g. Exhibit 1 which is a screenshot of a search conducted in 2021 by a staff with user ID "UH0028") suggest that frontline staff could have access to the personal data of both Complainant A's daughter and mother, Mr Lu has produced in Exhibit 4 various screenshots of searches conducted on the day of the hearing of the Appeal (i.e. 27 September 2023) to the following effect:

(1) The Appellant's System has records of the accounts of both Complainant A's mother and daughter (respectively "Grandmother" and "Daughter") under the same phone number;

(2) If the System is logged in by "IT Admin", one can search and view the accounts of both the Grandmother and the Daughter, including their personal profile and transactions;

(3) If the System is logged in by a Dr Reborn frontline staff, one can only search and view the account of the Grandmother but not the Daughter who did not give consent to Dr Reborn to access her data;

(4) If the System is logged in by a Primecare frontline staff, given that the Grandmother had given explicit consent to the Appellant's PICS on 8 February 2023, such staff could search the accounts of both the Grandmother and Daughter, but whilst the staff can view the profile of the Daughter and her transaction with Primecare, such staff can only view the profile but not the transaction of the Grandmother with Dr Reborn which is not relevant for servicing needs at Primecare;

(5) If the System is logged in by a re:HEALTH frontline staff, such staff can search the account of the Grandmother as she had given explicit consent to the Appellant's PICS on 8 February 2023, but the staff can only view her profile but not her transactions as they are not relevant for servicing needs at re:HEALTH.

24. On the face of it, the new evidence at Exhibit 4 supports Mr Lu's evidence, although it is fair to note that the searches were conducted on the day of the

hearing of the Appeal. This begs the question whether the System already had such access rights restrictions prior to the date of the Decision in 2022.

25. Of course, it has to be borne in mind that the Appeal is in the nature of a *de novo* hearing and the Board should take into account new evidence including Exhibit 4. That said, the crux remains whether the access rights restrictions as demonstrated in Exhibit 4 already existed prior to 2022. If the restrictions were only introduced subsequently following the receipt of the enforcement notice, this plainly could not be a basis for quashing the Decision on Ground 1. In this regard, it is pertinent to consider the oral evidence of Mr Lu. During cross-examination, it was suggested to Mr Lu that after the enforcement notice was sent to the Appellant, there is change and update in the Appellant's System to address the same. In response, Mr Lu said that the System is always there, but there is constant change of the System in terms of new product and services. However, he is adamant that what is required to be done in the enforcement notice has already been done previously; and that the relevant design, access right, function and features of the System were already present well before the Site Visit in 2022.

26. Moreover, when it was suggested to Mr Lu during cross-examination that the screenshot in 2021 with user ID "UH0028" in Exhibit 1 belonged to a frontline staff, Mr Lu disagreed and said it should be "IT Admin" (which, if true, could help explain why there was full access as shown by such screenshot).

27. Plainly, it would be a rather serious allegation to suggest that Mr Lu falsely testified that the features as demonstrated in the searches conducted on the day of the hearing of the Appeal in 2023 in Exhibit 4 already existed before the Site Visit in 2022. The Board could not lightly reach such conclusion in the absence of cogent evidence substantiating the same. For such reason, there is force in the

Appellant's stance that, taking into account such new evidence, one should be slow to conclude that there is sufficient evidence to substantiate the factual basis of contravention of DPP3(1). Having said that, the new evidence alone is not conclusive, as the Board must consider its veracity against other evidence, including in particular contemporaneous documentary evidence. With that in mind, the Board will examine such other evidence in turn. For the avoidance of doubt, the Board has considered all relevant evidence and arguments but will focus on the more salient ones in articulating its analysis.

28. To begin with, the gist of other evidence relied on by the Commissioner in response has been set out in §§26-45 of the Defence. It is not necessary to repeat all of them here, save to stress that the Board has had these (and other relevant) documents in mind in evaluating the evidence.

29. *First of all*, in relation to the sharing of information as between Primecare and Dr Reborn (as illustrated by Case (1)), there are *contemporaneous* written replies from the Appellant, particularly letters dated 2 August 2021, 5 October 2021, 21 December 2021 and 8 August 2022 (as referred to in Defence §§28.1, 28.2, 28.4, 28.5.5). These letters accept that, upon entering the phone number of the Grandmother in Dr Reborn's interface, the System would show the name and records of both the Grandmother and the Daughter. Given that the Appellant was specifically informed of the nature and particulars of the complaint in Case (1), it seems clear that in those letters, the Appellant accepted on an informed basis that the staff of Dr Reborn could in fact gain access to the personal data of both the Grandmother and the Daughter.

30. The suggestion that the staff of Dr Reborn could not in fact access the Daughter's information and the Appellant merely provided a screenshot in the

letter of 21 December 2021 (i.e. Exhibit 1) to demonstrate the full functionality of the System does not sit comfortably with the context of the investigation, or indeed the clear wordings of the letters. For instance, the letter dated 2 August 2021 from the Appellant accepts that a Dr Reborn staff could access the information of the Daughter via the System as follows:

"… 經過內部調查本集團發現，有 Dr Reborn 的員工在聯絡投訴人母親時嘗試在系統裏用電話號碼搜尋其名字。但因投訴人女兒和投訴人母親共用一個聯絡號碼，員工搜尋到投訴人女兒的名字，誤以為是投訴人的母親。所以，在發訊息的時候員工便用了投訴人女兒的名字，造成了今次的誤會。" [Emphasis added]

31. Similarly, the letter dated 5 October 2021 stated the position unequivocally as follows (and also included a screenshot in support of the same):

"… 匯兒及 Dr Reborn 均是醫思健康 (2138.HK) 屬下子公司，醫思健康則採用統一的內部管理系統。根據匯兒及 Dr Reborn 職員職能的權限及工作上的需要，職員可在該系統有限度地查閱其工作上需要的資料。但如附錄一所顯示，職員在該系統能查閱資料只包括姓名，已遮蔽的電話號碼及過去消費記錄，並不包括身分證號碼，地址，性別，出生日期等個人資料。

…

投訴人女兒和投訴人母親分別為匯兒及 Dr Reborn 的客戶，而投訴人女兒及投訴人母親的聯絡電話均以投訴人母親的聯絡電話號碼作為登記，故此當 Dr Reborn 職員在系統內以投訴人母親 (Dr Reborn 客戶)

的已登記聯絡電話查閱時，會一併顯示投訴人女兒及投訴人母親的記錄…” [Emphasis added]

32. Further, in the letter dated 21 December 2021, there was no mention that the screenshot enclosed as Annexure 3 thereto (i.e. Exhibit 1 which is a clearer version) was intended to demonstrate the full functionality of the System. This does not tally with Mr Lu's statement and his oral evidence during cross-examination that the screenshot was generated with "IT director" log-in, etc. Instead, the letter refers produces such screenshot in the following context (at §(6)(c)):

> "關於醫思健康旗下所有公司的職員可否閱覽客戶的個人資料，本集團需釐清所謂可閱覽的客戶個人資料是不完整的，只會顯示該會員之姓名、電話號碼首四位數字，並不包括其身分證號碼，地址，性別或出生日期等，…（以下稱不完整的客戶資料為「會員資料」），詳見附件三。
>
> 一般而言，職員僅能在其職能範圍閱覽會員資料…” [Emphasis added]

33. Both from the context of the query as well as the wordings of the letter, it seems plain and obvious that the Appellant was producing Annexure 3 (i.e. Exhibit 1) to illustrate the personal data which could be accessed by the staff in general via the System.

34. Importantly, in the Appellant's letter dated 8 August 2022, the Appellant has included an Appendix I to provide answers to various queries raised by the

Commissioner. Of particular significance is a table provided by the Appellant in Appendix I (under Answer (13) in response to the Commissioner's letter dated 8 July 2022), which unequivocaly particularizes the access rights of different types of staff across the brands of the Appellant under the System.

35. As admitted in such table, among the five different types of staff of the Appellant, namely sales (銷售), customer service (顧客服務), reception (接待), treatment staff (治療師), and managers (中心經理), they all have access rights or access to the information of 1.08 million customers in the System in terms of (i) customer information (客戶資料), (ii) customer payment and purchase records (客戶付款及購買紀錄), (iii) customer appointment records (客戶預約紀錄), (iv) appointment management (預約管理), and (v) making phone calls to customers via the System (於系統功能致電客戶). In addition, as accepted by the Appellant under Answer (14), the System contains information of 1.08 million customers and these include information of existing customers prior to acquisition by the Appellant.

36. All in all, these letters contradict the Appellant's latest stance that, as demonstrated in Exhibit 4, a frontline staff of Dr Reborn could not search and view the profile and transactions of the Daughter at all (see also Defence §§33-36). They suggest that, at least at the time of those letters, the System did not have such access rights restrictions – otherwise the Appellant should have no difficulty producing screenshots similar to those in Exhibit 4 then.

37. *Secondly*, in relation to the sharing of information as between NYMG and re:HEALTH (as illustrated by Case (2)), there are also *contemporaneous* written replies from the Appellant on 18 October 2021 (as set out in Defence §28.3) and 21 December 2021. For instance, the letter dated 18 October 2021 from the

Appellant accepts that staff of NYMG and re:HEALTH could access information via the System as follows:

> "… 仁和體檢及紐約醫療集團均是醫思健康(2138.HK)（"本公司"）屬下子公司，本公司採用統一的內部管理系統（"統一系統"）。根據仁和體檢及紐約醫療集團職員職能的權限及工作上的需要，職員可在統一系統裡有限度地查閱其工作上需要的資料。如附錄二所顯示，職員在統一系統能查閱資料只包括姓名，已遮蔽的電話號碼及過去消費記錄，並不包括身分證號碼，地址，性別，出生日期等個人資料（附錄二）。" [Emphasis added]

38. This is borne out by Annexure 2 enclosed thereto (i.e. Exhibit 2 which is a clearer version). Again, this contradicts the Appellant's latest stance that a frontline staff of NYMG and re:HEALTH could not search and view the profile and transactions of other brands via the System unless the relevant person has signed and consented to the PICS because, in the case of Complainant B in Case (2), he did not sign and consent to the PICS and yet Annexure 2 (i.e. Exhibit 2) still shows his personal profile and transaction at NYMG.

39. Accordingly, the Board accepts the Commissioner's submissions at §17 of R's Skel that the circumstances of Case (1) and Case (2) both indicate that the personal data of the Daughter and Complainant B, who were clients of Primecare and NYMG respectively before the brands were acquired by the Appellant, were accessed and used by the frontline staff of other brands under the Appellant that also use the System, namely, Dr Reborn and re:HEALTH respectively.

40. *Thirdly*, whilst the Appellant emphasizes there is no actual record to prove whether the name of the Daughter was in fact included in the text message, this

does not detract from the position as stated and demonstrated by the letters and screenshots provided by the Appellant. Moreover, the Commissioner already took this into account and did not rely on such text message itself as evidence (see Investigation Report §22 and Defence §42).

41. *Fourthly*, the Commissioner relies on the Site Visit (see Defence §§28.5.1, 28.5.2). The Commissioner has also disclosed a written minutes of the Site Visit which was prepared contemporaneously on the same day as the Site Visit (i.e. 14 June 2022). Such minutes were disclosed as item 52 of the Commissioner's list of documents dated 28 December 2022. As recorded in the minutes of the Site Visit prepared by the Commissioner:

> "醫思健康的統一系統
>
> 醫思健康以某一品牌**前線員工**的身份登入其統一系統，以向公署展示透過該系統其前線職員在日常工作中可看到儲存於系統內的客戶的哪些資訊，及如何運作有關系統。" [Emphasis added]

42. The minutes then went on to set out the results of the demonstration.

43. In this regard, if the Appellant has prepared its own minutes of the Site Visit contemporaneously and disagrees with the contents of the version of the Commissioner, the Appellant ought to have disclosed its version at or around the same time. Yet, no such minutes were disclosed in the Appellant's List of Documents/Authorities dated 2 March 2023. It was not until 31 August 2023 that the Appellant belatedly disclosed its version of the minutes as Annex 2 to Mr Lu's witness statement. Mr Lu has not stated in his statement as to the time when such version was prepared. Moreover, he has not given any satisfactory

explanation as to why such version was not produced earlier, if it were prepared contemporaneously. As such, the Board prefers the version of the Commissioner to that of the Appellant in case of any discrepancy.

44. Based on the minutes prepared by the Commissioner, there is force in the Commissioner's submissions at §17 of R's Skel that the information obtained during the Site Visit showed that the personal data of clients of a brand of the Appellant could be shared amongst other brands under the Appellant that also use the System, enabling the relevant information to be accessible to the frontline staff of other various brands.

45. Moreover, there are little merits in the Appellant's complaint that the Commissioner erroneously found that the demonstration during the Site Visit was representative of *all* customers under the Appellant. With respect, this is not the Commissioner's stance (see R's Skel §18), and it is also not strictly necessary for the Commissioner to go so far, as the focus is on the access of information of customers of Primecare and NYMG by other brands under the Appellant.

46. Indeed, the Appellant should be left with little doubt as to the purpose of the Site Visit. Given the context of the Commissioner's investigations of Cases (1) and (2) and the correspondences exchanged between the Appellant and the Commissioner (e.g. the Commissioner's letter dated 15 November 2021 as relied upon in R's Skel §22), the Appellant should have realised that the focus of the investigations has always been the access to personal data by frontline staff of other brands under the Appellant via the System. Even Mr Lu had to accept at §13(1) of his statement that, during the Site Visit, the Appellant was asked by officers of the Commissioner for "a demonstration of the *frontline portal*

accessible by [its] frontline staff" (even though such wording was absent in the version of the minutes produced by Mr Lu as Annex 2 to his statement).

47. In this regard, there is force in the Commissioner's submissions at §24 of R's Skel that the Appellant only changed its stance after the Site Visit and even went so far to claim that the System demonstration provided by the Appellant were simply a demonstration to the Commissioner and did not reflect the real situation, and yet the Appellant did not offer any reasonable explanation for this inconsistency in its stance.

48. All in all, the above militate against the belated suggestion by the Appellant that the demonstration was done with full access rights of the IT director, which would otherwise defeat the very purpose of the investigation and the Site Visit to demonstrate the frontline portal accessible by the frontline staff of the Appellant's brands (see also Defence §§37, 39).

49. *Fifthly*, the Commissioner relies on the two visits to the branches of NYMG and re:HEALTH respectively (see Defence §§28.5.3, 28.5.4). In respect of both visits, what is significant is the confirmation by NYMG and re:HEALTH staff that they can search and view whether the staff of the Commissioner is the customer of other brands of the Appellant (see Defence §39). This tallies with other documentary evidence that a frontline staff of a brand of the Appellant could search and access the personal information of a customer across different brands of the Appellant via the System. Whilst the Applicant emphasizes that the NYMG staff would do so only with the consent of the staff of the Commissioner and the re:HEALTH staff did not proceed further as the registration process was not complete, this is beside the point as the focus is whether such staff can access

information across different brands, to which the answer is in the affirmative (see similarly Defence §44).

50. Further, it is significant that in both Cases (1) and (2), and as demonstrated by the screenshots provided by the Appellant, the System would show the personal data of the Daughter or Complainant B by the frontline portal, even though neither of them has signed and consented to the PICS. In a similar vein, although the NYMG staff mentioned that searches could be done with the consent of the staff of the Commissioner, there is no mention that the NYMG could only do so if the staff of the Commissioner has already signed and consented to the PICS. This tends to suggest that, irrespective of whether a customer has already signed and consented to the PICS (which would be most relevant in the scenario of M&A in which a brand is subsequently acquired by the Appellant such as Primecare or NYMG), the customer's information could still be accessed across the brands via the System.

51. *Sixthly*, whilst the Appellant contends that the various brands under the Appellant operated in three different models and layers, the Appellant has not explained how this would assist its case. In this regard, we agree with the Commissioner's stance that such contention is irrelevant for the purpose of her investigation (R's Skel §18) and it does not detract from the fact that the System was used by all such brands to store and access personal data of clients (see Defence §31).

52. Importantly, irrespective of the characterization of such different models and layers, this does not detract from the fact that, as demonstrated from the investigations (including the Appellant's replies, screenshots and site visits etc),

personal data of clients of Primecare and NYMG could be accessed by frontline staff of other brands under the Appellant.

53. *Seventhly*, whilst the Appellant emphasizes that access and use of clients' personal data in the System was permitted only on a need-to-know basis, for specified purposes which were the same or directly related to the purposes for which the data was originally collected, and that the staff of the Appellant's brands would only have limited access depending on their scope of duty (職能) and the relevant information would not be accessed by unrelated person etc, the Appellant has not provided much particulars or concrete evidence to substantiate such contentions (see also Defence §40). As such, there is no proper basis for the Appellant to challenge the Commissioner's evaluation based on documentary evidence, site visits and replies from the Appellant (see also Defence §32).

54. *Eighthly*, we also agree with the Commissioner's view that it does not assist the Appellant to suggest that confusion results due to a single phone number being used for multiple customers. As submitted by the Commissioner with reference to Case (1), if a frontline staff could not gain access of personal information of other brands of the Appellant, then regardless of whether the System is logged in using the account of a Primecare staff or a Dr Reborn staff, the System should only show the personal data of either the Grandmother or the Daughter, but not both of them. This is particularly the case bearing in mind that the Appellant could not locate any PICS signed by (or on behalf of) the Daughter, whilst the Grandmother only signed the PICS on 8 February 2023 (i.e. after the date of the Decision) (see similarly Defence §41).

55. *Ninthly*, the Appellant contends that, where the then existing customers of acquired brands had not consented to the Appellant's privacy policy or PICS,

their personal data would be stored under the separate brands, and would not be accessible by the staff of other brands. However, whilst this is supported by the screenshots of Exhibit 4, they are contradicted by other *contemporaneous* evidence analysed above (including the Appellant's then replies, screenshots and site visits).

56. For all these reasons, and notwithstanding the new evidence (including Exhibit 4) and the Appellant's arguments, we do not consider that the Appellant has made out its case on Ground 1. For the avoidance of doubt, it is not strictly necessary for us to come to any specific view or finding as to whether Mr Lu has intentionally misled the Board in the course of his evidence. There could be other possibilities including incorrect understanding on his part, but (among others) the key is that we are not satisfied that the access rights restrictions as demonstrated in Exhibit 4 already existed prior to the date of the Decision in 2022.

E. ANALYSIS – GROUND 2

57. In relation to Ground 2, the Appellant's contentions are set out in §§4-6 of the NOA, §§48-78 of the Reply and Section E2 of A's Skel.

58. In gist, the Appellant contends that even if the factual findings of the Commissioner in relation to the operation of the System are adopted, there would have been no contravention of DPP3(1) as there was no use of personal data for a new purpose.

59. Relevantly, DPP3(1) and 3(4) provide as follows:

> **"3. Principle 3—use of personal data**

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

...

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or
(b) a purpose directly related to the purpose referred to in paragraph (a)."

60. In this regard, the Commissioner says that in considering whether there is a breach of DPP3(1), the issue is whether the disclosure of the relevant personal data is for the purpose or directly related purposes for which the relevant data was to be used at the time of the collection of the data, i.e. the purposes in DPP3(4)(a) and (b) (R's Skel §33). If the answer is in the negative, the relevant personal data would have been used for a new purpose, thereby resulting in a breach.

61. On the facts of the present case, the Commissioner says the key question is whether it constituted a breach of DPP3 for the Appellant, as a data user, after acquiring Primecare and NYMG, to have stored in the System of the Appellant the personal data of existing clients before acquisition (including the Daughter in Case (1) and Complainant B in Case (2)) and shared parts of their personal data amongst the 28 brands under the Appellant that also used the System so that the

relevant personal data were accessible to the frontline staff of various brands, as a result of which personal data originally provided by them to a single brand was disclosed and transferred, without their knowledge, to the staff of other brands (R's Skel §16). Ultimately, it boils down to the question whether the Appellant's use (including disclosure or transfer) of such personal data is for a "new purpose".

62. Broadly speaking, the Appellant's arguments are threefolds.

(1) First of all, the Appellant contends that access to cross-brand personal data under the Appellant does not constitute a "new purpose". Accordingly, there is no contravention of DPP3(1).

(2) Secondly, the Appellant relies on the exemption provision in section 63B of the PDPO concerning personal data transferred or disclosed by a data user for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction that involves acquisition or merger.

(3) Thirdly, the Appellant relies on the statutory defence under section 65(3) of the PDPO on the ground that the Appellant had taken such steps as were practicable to prevent the employees from doing the act or engaging in that practice in the course of their employment, act or practice.

63. The above arguments are developed in §27 of A's Skel as follows:

(1) In ascertaining the "original purpose" of personal data collection, the Board is urged to consider, *inter alia*, (a) the explicit purposes, (b)

the function or activity of the data user, and (c) the restrictions of use imposed by the data subject or the transferor (if any);

(2) Use of personal data in different forms or ways as warranted by the circumstances, without a new purpose in mind, may be considered as done within the scope of the original purpose;

(3) There may be legitimate purpose(s) for transferring personal data to a third party. DPP3 might risk being violated only where there is excessive disclosure by the data user; When considering the issue of "directly related", the Board is urged to consider whether the act went beyond what was reasonably required; Similarly, forwarding personal data from one government department to another for further handling was also found not to be for a new purpose;

(4) In the present case, whilst there is no dispute that original purposes for collecting the data did include the provision of medical, healthcare and customer services, the use of the data collected could be also used for the same or directly related services provided by the brands within the same group for the same and related purposes, without creating any new purpose;

(5) As a matter of fact, there was no suggestion that the personal data of the Appellant's customers was for purposes other than the provision of medical, healthcare and customer services (e.g., telemarketing);

(6) Even in the Commissioner's view, the purposes for which the data was used by the Appellant remained the same as those for the

provision of medical, healthcare and customer services to the data subjects who provided their personal data with these purposes in mind;

(7) In the circumstances, the nature and purpose of the use of the personal data concerned had not changed at all, and the only difference was the parties who provided such services were those within the services provider group after acquisition or merger. This should fall within the lawful functions and activities of the Appellant to use its customers' personal data for the provision of medial, healthcare and customer services;

(8) Accordingly, there was no use of personal data for any new purpose, no consent would be required from customers and thus no contravention of DPP3(1);

(9) Given that the Commissioner acknowledged the Appellant's acquisition of the relevant brands and services provided; and raised no queries during the investigation (not referred to in the Report), it is a standard practice that for a successful merger or acquisition compliance with applicable personal data protection laws would have to be demonstrated in the buyer's representation and warranties - the due diligence exercise. Furthermore, it is often impractical to rely on the consent of all data subjects where the data subjects are more than a few individuals. It is for this reason that section 63B of the PDPO was added in the PDPO (as amended in 2012) specifically exempting from the application of DPP3 for personal data transferred or disclosed by a data user for the purpose of a due

diligence exercise to be conducted in connection with a proposed business transaction that involves acquisition or merger. It is obvious that this exemption seeks to address the practical needs of businesses to disclose or transfer information which may contain personal data in an intended acquisition, merger or transfer of businesses for the purpose of conducting a due diligence exercise by the proposed transferee. The Commissioner failed to consider section 63B of the PDPO and there was no justification for the Commissioner to make the findings in relation to the Appellant's acquisition and the related use of the personal data; and

(10) Even if there had been contraventions of DPP3(1) by the frontline staff (which are denied), the Appellant could not have been held liable for the contraventions as the statutory defence under section 65(3) of the PDPO would be invoked on the ground that the Appellant had taken such steps as were practicable to prevent the employees from doing the act or engaging in that practice in the course of their employment, act or practice.

64. Turning to the first argument, we do not think it can be made out upon proper analysis.

65. *First of all*, a fundamental flaw of such argument is to equate the purpose of collecting personal data for provision of medical, healthcare and customer services by Primecare or NYMG with the use of such personal data by any *other* company or entity for provision of *any other* medical, healthcare or customer services (which, in essence, is the logical extension of the argument in A's Skel §§27(4)-(8)). With due respect, the Appellant is seeking to brush aside the issue

by saying that the nature and purpose of the use of the personal data concerned had not changed at all, and the only difference was the parties who provided such services were those within the services provider group after acquisition or merger.

66. In our view, the starting point is that Primecare or NYMG could not reasonably suggest that they could, without the consent of its customers, disclose or transfer their personal data to any *other* third party company or entity as long as the latter is also in the business of providing medical, healthcare and customer services. A customer of Primecare or NYMG would not reasonably expect his or her personal data to be supplied to any *other* company or entity in the market without his or her consent. Should it be otherwise, a company would be able to freely disclose and transfer personal data of its customers to any other player in the field, which is plainly an unacceptable intrusion of privacy.

67. As a matter of principle and in the absence of prescribed consent, it should not matter even if such *other* company or entity happens to be in the same group, as they remain *separate* legal persons who provide *distinct* medical or healthcare services under different brands. This is not to mention that even within the field of medical and healthcare services, there are many *different* types or variants of services as demonstrated by various brands of the Appellant. Such differences could not, and should not, be lightly brushed aside and sidelined under the guise of entities within a "services provider group", particularly when the personal data was collected *before* the assimilation into the group.

68. In this regard, there is force in the argument in R's Skel §37 that, insofar as Case (1) is concerned, in the absence of a PICS (which cannot be located by the Appellant), the purpose of collecting the Daughter's personal data by Primecare, as a medical centre, should be for Primecare to provide medical and

customer services to the Daughter. Hence, even if Primecare was later acquired by the Appellant, the Daughter's reasonable expectation for privacy should be limited to allowing Primecare but not other organisations to use her personal data to provide medical and customer services to her. This is *a fortiori* the case for other organisations which provide *separate* and *distinct* medical, healthcare and customer services under brands that are different from that of Primecare. Indeed, such argument applies *mutatis mutandis* to NYMG in Case (2) (see R's Skel §38).

69. In the premises, we agree with the Commissioner's submissions in R's Skel §36. The fallacy of the Appellant's argument is to wrongly presume that, since the original purpose of collecting the personal data was to provide medical, healthcare and customer services to the Daughter and Complainant B, such data could be used for the purposes of providing the same or directly related services not only by Primecare or NYMG, but also by *other brands under the Appellant*, without creating any new purpose. With respect, this is nothing but a quantum leap. Primecare and NYMG collected the personal data of the Daughter and Complainant B *before* the acquisition by the Appellant. The use of such personal data by other brands (beyond Primecare and NYMG) can hardly be said to be for the original purpose or purpose directly related to the same.

70. In particular, it is misconceived to characterize such use by other brands as use of personal data in different forms or ways as warranted by the circumstances. It is one thing to suggest that Primecare or NYMG may still use the personal data in different forms or ways to provide similar services, but quite another to suggest that the personal data could be used by different entities altogether for separate and distinct services under different brands. Further, it cannot be said that such cross-brand sharing or disclosure of personal data was reasonably required. As mentioned below, even the Appellant has confirmed there was no functional need

for Primecare, Dr Reborn, NYMG and re:HEALTH to access personal data of other brands, and vice versa. There is also no need for further handling of data across different brands under the Appellant.

71. *Secondly*, on the facts of the present case, it does not assist the Appellant to point to (a) the explicit purposes, (b) the function or activity of the data user, and (c) the restrictions of use imposed by the data subject or the transferor (if any). In relation to explicit purposes, there is no record of any PICS for the Daughter, whilst the PICS signed by Complainant B does not extend to the use of personal data across different brands.

72. As regards the function or activity of the data user, it is true that the Appellant is a group company providing medical, healthcare and customer services under different brands. For such reason, one may say that the Appellant could reasonably be expected to use the personal data for continuity of provision of the same services by Primecare or NYMG under the umbrella of the Appellant. It would however be farfetched to suggest that, simply because Primecare and NYMG was acquired by the Appellant, their customers must be taken to have expected their personal data to be used not only for the same services provided by Primecare and NYMG, but also for services provided by other entities under different brands (albeit under the group of the Appellant).

73. With respect to the restrictions of use imposed by the data subject or the transferor (if any), they do not feature on the facts too. For instance, the scope of the purpose could be narrowed down by restrictions imposed by the data subject but in the present case, neither the Daughter nor Complainant B imposed such restrictions. Nevertheless, as rightly pointed out in §35 of R's Skel, even if the data subject does not impose any restriction on the use of his/her personal data

when or before providing personal data to the data user, this does not mean that the data user can use his/her personal data without limits. We tend to agree with the Commissioner that, when considering the original purpose of use of the personal data in this case, the applicable considerations should include (i) the content of the relevant PICS; (ii) the legitimate functions or activities of the data user; (iii) the nature of the relevant transactions, and (iv) the data subject's reasonable expectations of his/her privacy.

74. *Thirdly*, it does not assist the Appellant to point to its PICS which envisages and permits access of personal data across different brands of the Appellant. This would apply to new customers who consent to the PICS. However, it could not apply to personal data collected by companies or entities who were later acquired by the Appellant, unless the relevant customers have consented to the Appellant's PICS subsequently. At the time of collecting the personal data, these companies or entities were not part of a larger group providing medical and healthcare services, and it is untenable to suggest that their customers would have reasonable expectation that their data could be used by entirely different brands in future without their prescribed consent.

75. *Fourthly*, both the Appellant and the Commissioner refer to the decision of *Lam Shuk Yee v The Privacy Commissioner for Personal Data* (AAB No. 13/2011) as to the proper test for determining whether the Appellant's use of the personal data of the Daughter and Complainant B is directly related to the original purpose of use at the time of the collection of the data. In the Board's view, the proper question to be asked is whether the provision of medical and customer services to its clients by Primecare or NYMG would be affected if the Appellant did not share their personal data among other brands under the Appellant that use the System. In our view, it could not be reasonably suggested that the provision

of medical and customer services by Primecare or NYMG would be affected as a result, as there is no obvious reason or need for staff of other brands to gain access to such personal data to facilitate provision of services by Primecare or NYMG. Indeed, as pointed out in R's Skel §45, the Appellant had confirmed in its letters dated 5 and 18 October 2021 that the staff of Primecare, Dr Reborn, NYMG and re:HEALTH did not have a functional need to access the clients' personal data of the other brands of the Appellant.

76. In view of the foregoing, the Appellant's sharing of parts of the personal data of the customers of Primecare and NYMG among other brands of the Appellant using the System should constitute a new purpose under DPP3. Since the Appellant failed to seek prescribed consent from those customers (including the Daughter and Complainant B) for the use, disclosure and transfer of their personal data for a new purpose, the Appellant had contravened DPP3(1).

77. As regards the second argument, the Appellant relies on section 63B of the PDPO, which provides as follows:

> "**63B. Due diligence exercise**
>
> (1) Personal data transferred or disclosed by a data user for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction that involves—
>
> (a) a transfer of the business or property of, or any shares in, the data user;
> (b) a change in the shareholdings of the data user; or
> (c) an amalgamation of the data user with another body,

is exempt from the provisions of data protection principle 3 if each of the conditions specified in subsection (2) is satisfied.

(2) The conditions are—

(a) the personal data transferred or disclosed is not more than necessary for the purpose of the due diligence exercise;

(b) goods, facilities or services which are the same as or similar to those provided by the data user to the data subject are to be provided to the data subject, on completion of the proposed business transaction, by a party to the transaction or a new body formed as a result of the transaction;

(c) it is not practicable to obtain the prescribed consent of the data subject for the transfer or disclosure.

(3) Subsection (1) does not apply if the primary purpose of the proposed business transaction is the transfer, disclosure or provision for gain of the personal data.

(4) If a data user transfers or discloses personal data to a person for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction described in subsection (1), the person—

(a) must only use the data for that purpose; and

(b) must, as soon as practicable after the completion of the due diligence exercise—

(i) return the personal data to the data user; and

(ii) destroy any record of the personal data that is kept by the person.

(5) A person who contravenes subsection (4) commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years.

(6) In this section—

due diligence exercise (盡職審查), in relation to a proposed business transaction, means the examination of the subject matter of the transaction to enable a party to decide whether to proceed with the transaction;

provision for gain (為得益而提供), in relation to personal data, means provision of the data in return for money or other property, irrespective of whether—

(a) the return is contingent on any condition; or

(b) the person who provides the data retains any control over the use of the data."

78. As noted by the Commissioner (at R's Skel §§48-51), the Appellant's reliance on section 63B is a new allegation which was never advanced in the NOA, let alone in the course of the Commissioner's investigations. Without prejudice to the foregoing, we will consider the merits of the argument below.

79. To start with, section 63B of the PDPO is not applicable here as we are not concerned with a due diligence exercise for the purpose of M&A. Nevertheless, the Appellant stresses that the statutory exemption recognises that it is often impractical to obtain the prescribed consent of the data subject and seeks to address the practical needs of businesses to disclose or transfer information which may contain personal data in an intended acquisition, merger or transfer of businesses. Apparently, the Appellant seeks to rely on such exemption in support

of its argument that disclosure or transfer of information following M&A is widely accepted as the norm, and should not be treated as use for a new purpose.

80. With respect, if the disclosure or transfer of personal data for a due diligence exercise of M&A does not constitute use for a new purpose, there would have been no need for an exemption under section 63B to begin with. Hence, the Appellant's suggestion that the provision somehow supports its argument that there is no use for a new purpose, is putting the cart before the horse.

81. In his oral closing submissions, leading counsel for the Appellant suggests that it is very common for personal data to be acquired or transferred during M&A transactions, and he has cited the example of acquisition of various hotel groups around the globe. However, we are not concerned with a scenario where a company is taken over by another buyer *per se*. In that scenario, provided that the same business or services are carried out by the buyer, it may be said that the use of personal data by the buyer falls within DPP3(4) and hence does not constitute a new purpose. This is however different from the present scenario where the buyer (namely the Appellant) is engaging in various other businesses through different subsidiaries, and the personal data is accessed not only by the original business but also businesses of other subsidiaries of the group. Yet, these subsidiaries are separate legal persons. The disclosure or transfer of personal data to these subsidiaries is, by nature, not dissimilar to the disclosure or transfer of personal data to other third party company or entity. Notwithstanding the fact that the subsidiaries are within the same group, they remain separate legal persons pursuing their distinct and separate businesses (under different brands).

82. With respect to the third argument, the Appellant relies on the statutory defence in section 65(3) of the PDPO. Section 65 provides as follows:

"**65. Liability of employers and principals**

(1) Any act done or practice engaged in by a person in the course of his employment shall be treated for the purposes of this Ordinance as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) Any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him.

(3) In proceedings brought under this Ordinance against any person in respect of an act or practice alleged to have been done or engaged in, as the case may be, by an employee of his it shall be a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing that act or engaging in that practice, or from doing or engaging in, in the course of his employment, acts or practices, as the case may be, of that description.

(4) For the avoidance of doubt, it is hereby declared that this section shall not apply for the purposes of any criminal proceedings."

83. Yet, the Appellant has not condescended onto particulars as to the steps as were practicable which were taken by the Appellant to prevent the breaches by the employees of the Appellant's group. For instance, it is not the case that the

Appellant has produced internal guidelines and a breach resulted due to the non-compliance with such guidelines by a staff. It is, to say the least, questionable if the Appellant could indeed attribute the responsibility in any breach of DPP3(1) to employees alone. Taking Case (1) as illustration, as pointed out in R's Skel §30, the Appellant accepted in its letter dated 5 October 2021 that, since the Daughter and the Grandmother were both registered with the same phone number, when Dr Reborn's staff conducted a search using the Grandmother's contact number in the System, records of the Daughter and the Grandmother were shown together and were not accessed without authorization or accidentally. In other words, Dr Reborn's staff was simply doing what was allowed under the System. It is not a case of employees committing a breach for which the Appellant has taken such steps as were practicable to prevent.

84. Fundamentally, the underlying problem stems not from the acts or practices of employees *per se*, but rather the design and features of the System including in particular the ability of frontline staff to search and access personal data of customers across different brands of the Appellant, thereby resulting in a contravention of DPP3(1). Such systemic failure could not be lightly brushed aside to the employees of the Appellant's group or otherwise excused based on alleged steps as were practicable taken out by the Appellant.

85. For all these reasons, Ground 2 also fails.

F. ANALYSIS – GROUND 3

86. Ground 3 concerns alleged procedural irregularities leading to the Commissioner's findings and the Decision.

87. Nevertheless, as acknowledged in A's Skel §19, as the Board is exercising its appellate function and conducting this Appeal by way of re-hearing *de novo*, the procedural irregularities set out in Ground 3 are not a standalone ground, but considerations that the Board is urged to take into account when considering the Appeal. In other words, given the fact that the Appeal proceeds by way of re-hearing *de novo* and the Appellant is afforded the opportunity to adduce new evidence and arguments, any alleged procedural irregularities would have been cured by the process of hearing in the Appeal.

88. As such, the Appellant has fairly acknowledged in A's Skel §20 that the two issues to be decided remain those covered under Ground 1 and Ground 2. It follows that Ground 3 is not itself a standalone ground calling for intervention by the Board.

89. Without prejudice to the foregoing, the Appellant has focused on 3 matters in A's Skel §29, which the Board will address in turn.

90. *First of all*, the Appellant contends that the Commissioner failed to give adequate notice to the Appellant of the allegations or the materials intended to be relied upon against the Appellant, and thus failed to give reasonable opportunity to the Appellant to make response to them. By way of example, the Appellant complains that, whilst the Commissioner provided a draft Investigation Report to the Appellant on 16 September 2022 and invited for the Appellant's comments, there were some material differences between the draft and the final Investigation Report, including in particular Parts V and VI on Enforcement Actions and Recommendations.

91. With respect, there is little substance in such complaint. The Board notes the submissions in R's Skel §56 that, albeit not required under the PDPO, the Commissioner on her own initiative provided a draft of the relevant parts of the Investigation Report (i.e., the background of the case, the information and evidence obtained from the investigation, the information and responses provided by the Appellant, findings and contraventions) to the Appellant on 16 September 2022 for reference and response. By doing so, the Commissioner has informed the Appellant not only the gist of the allegations made against the Appellant, but also the particulars thereof and the evidence relied upon by the Commissioner. There is no sound basis to suggest that, on top of the foregoing, the Commissioner must also inform the Appellant the Enforcement Actions and Recommendations which may be imposed. The latter are obviously follow-up actions which the Commissioner could determine in the exercise of her powers and discretion under the PDPO, which would necessarily depend on the final investigation results and findings. There could not be an onerous obligation imposed on the Commissioner to provide those sections to the Appellant in advance for comments, as long as the Appellant has been adequately informed of the bases of the allegations.

92. In any event, the Appellant has had opportunity to deal with the issues of Enforcement Actions and Recommendations in this Appeal if it wishes to do so, and this should have cured any alleged procedural irregularity. Yet, despite having such opportunity, it speaks volume that the Appellant has advanced no substantive argument in its NOA and submissions to challenge the propriety of the Commissioner's Enforcement Actions and Recommendations.

93. *Secondly*, the Appellant contends that the Commissioner failed to provide adequate reasons for her decision, and failed to show how, on all the matters and materials before her, she was able to reach her conclusion. For example, the

Appellant says that the Commissioner failed to provide adequate analyses and reasonings on how the personal data of the customers were used for new purposes which were not directly related to the original purposes.

94. With respect, the Commissioner has set out her findings and reasonings in the Investigation Report with great details. Whilst the Appellant disagrees with the reasoning of the Commissioner, it is fair to say that the Commissioner did articulate why she considered there was a contravention of DPP3(1) in §§27-32 of the Investigation Report. Among others, the Commissioner reasoned in §29 of the Investigation Report that the disclosure and transfer of personal data of customers of Primecare and NYMG to frontline staff of other brands under the Appellant was plainly inconsistent with the original purpose of collection of such data, and also inconsistent with the data subjects' reasonable expectations of their privacy.

95. In any event, given that the nature of the Appeal is a *de novo* hearing by way of rehearing on the merits, any alleged deficiency in the reasoning of the Commissioner is not itself a sufficient ground for setting aside the Decision. Instead, the Appellant has had full opportunity to present its case and evidence before the Board, and the Board has also provided adequate reasons for its decision herein.

96. *Thirdly*, the Appellant contends that the surprise or undercover visits made by the Commissioner were irregular procedures for the purposes of investigating these two cases. The Appellant also argues that the complainants should have been asked to provide evidence and, alternatively, mediation or conciliation should have been pursued without investigations.

97. As can be seen from our analysis above, the Commissioner is not solely relying on the two complaints in Cases (1) and (2) or the surprise or undercover visits in reaching the Decision. Instead, the Commissioner also relies on other evidence including the Site Visit and the written replies and screenshots provided by the Appellant. The Commissioner has also made clear that she is not relying on any record of the text message itself in Case (1) as there is no record of the same. As the Commissioner has fairly relied on the totality of evidence before her and has also afforded opportunity for the Appellant to comment on the same, it is difficult to see how this would give rise to alleged procedural irregularity.

98. Insofar as the surprise or undercover visits are concerned, it is notable that section 43(1) of the PDPO provides as follows:

> "**43. Proceedings of Commissioner**
>
> (1) Subject to the provisions of this Ordinance, the Commissioner may, for the purposes of any investigation—
>
> (a) be furnished with any information, document or thing, from such persons, and make such inquiries, as he thinks fit; and
>
> (b) regulate his procedure in such manner as he thinks fit."

99. Given the wording of section 43(1) of the PDPO, the Commissioner should have a flexible and wide discretion as to how she may be furnished with any information, document or thing and make such inquiries as she thinks fit. There is no reason why the site inspections conducted by the Commissioner, which target specifically the issue in the present case, should fall outside the ambit of section 43(1).

100. Moreover, one must not forget that these were steps taken by the Commissioner to verify and confirm the findings based on other sources. Instead of being procedurally unfair to the Appellant, this seems to be an extra step taken by the Commissioner to verify the veracity of her findings. As mentioned, the Appellant is in any event afforded opportunity to comment on the same.

101. For all these reasons, there are no merits in Ground 3.

G. CONCLUSION

102. For the reasons stated above, the Appeal is dismissed.

103. As to the question of costs, we are not minded to award costs against the Appellant. Among others, we are not satisfied that the Appellant has conducted its case in a frivolous or vexatious manner: see section 22(1) of the Administrative Appeals Board Ordinance (Cap. 442).

104. Lastly, we thank Mr Stephen Wong and Mr Jay Koon for the Appellant and Ms Hermina Ng for the Commissioner for their assistance to the Board.

(signed)
(Mr Jenkin Suen, SC)
Deputy Chairman
Administrative Appeals Board

Appellant: Represented by Mr Stephen Wong and Mr Jay Koon, Counsels instructed by Messrs. P.C. Woo & Co.

Respondent: Represented by Ms Hermina Ng, Senior Legal Counsel

Persons Bound by the decision appealed against: Acted in person (absent from the hearing)