調查報告

根據香港法例第 486 章《個人資料(私隱)條例》
第 48(2) 條發表

Carousell 用戶的個人資料

遭未獲准許的擷取

報告編號：R23 - 0665
發表日期： 2023 年 12 月 21 日

調查報告：

Carousell 用戶的個人資料遭未獲准許的擷取

香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）第 48(2)條訂明，「[個人資料私隱]*專員在完成一項調查後，如認為如此行事是符合公眾利益的，可－*

(a)　發表列明以下事項的報告－

(i)　該項調查的結果；

(ii)　由該項調查引致的、專員認為是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文（尤其是各保障資料原則）的任何建議；及

(iii)　由該項調查引致的、專員認為適合作出的任何其他評論；及

(b)　以他認為合適的方式發表該報告。」

現根據《私隱條例》第 48(2)條履行所賦予的權力，發表本調查報告。

鍾麗玲
個人資料私隱專員
2023 年 12 月 21 日

調查報告

根據香港法例第 486 章《個人資料（私隱）條例》第 48(2) 條發表

Carousell 用戶的個人資料遭未獲准許的擷取

I. 背景

1. 2022 年 10 月 26 日，Carousell Limited[1]向個人資料私隱專員公署（私隱專員公署）作出資料外洩事故通報，表示 Carousell Pte Ltd[2]於 2022 年 10 月 13 日在一個網上論壇發現一則銷售訊息，聲稱可出售 260 萬名 Carousell 用戶的個人資料，並於 2022 年 10 月 21 日發現有 324,232 個香港用戶的帳號受到影響。

2. 根據 Carousell Limited 所述，該資料外洩事件（該事件）源於 2022 年 1 月系統遷移（該系統遷移）過程中出現的一個保安漏洞（該保安漏洞）。

3. 在接獲上述資料外洩事故通報後，私隱專員公署隨即對 Carousell Limited 展開循規審查，以取得更多有關該事件的資料。在收到 Carousell Limited 提供的進一步資料後，個人資料私隱專員（專員）相信 Carousell Limited 在該事件中的作為或行為可能涉及違反香港法例第 486 章《個人資料（私隱）條例》（《私隱條例》）的規定，遂於 2023 年 1 月根據《私隱條例》第 38(b)條[3]就該事件對 Carousell Limited 展開調查。

[1] 一家在香港註冊的有限公司。

[2] 一家位於新加坡的公司。

[3] 根據《私隱條例》第 38(b)條，凡專員有合理理由相信有資料使用者已經或正在作出或從事關乎個人資料的作為或行為，而有關作為或行為可能屬違反《私隱條例》下的規定，專員可就有關的資料使用者進行調查，以確定有關作為或行為是否屬違反《私隱條例》下的規定。

II. 調查所得的資料

4. 調查在 2023 年 1 月至 10 月期間進行。在調查過程中，專員就 Carousell Limited 在該事件發生時採取的保安措施共進行了五次的查訊，並審視了 Carousell Limited 提供與該事件有關的各種資訊，包括由 Carousell 集團[4]委任的一間獨立資訊科技顧問公司（該顧問公司）提供的調查報告。專員亦考慮了 Carousell 集團在該事件發生後的跟進及補救工作。

5. 根據 Carousell Limited 所述，Carousell 集團以中央化模式整合集團內包括保安、法律及技術團隊等共同使用的服務。Carousell Pte Ltd 負責管控 Carousell 集團的系統基礎設施及資料庫，並將之提供予 Carousell 集團轄下不同地區的公司使用，當中包括香港的 Carousell Limited。Carousell Limited 確認控制 Carousell 香港用戶個人資料的收集、持有、處理及使用。

<u>Carousell 的背景</u>

6. Carousell 是一個網上多元分類及二手交易市場，供用戶買賣全新及二手商品。Carousell 集團於 2012 年在新加坡成立，並在香港、馬來西亞、印度尼西亞、菲律賓和台灣提供服務，擁有數千萬每月活躍用戶。

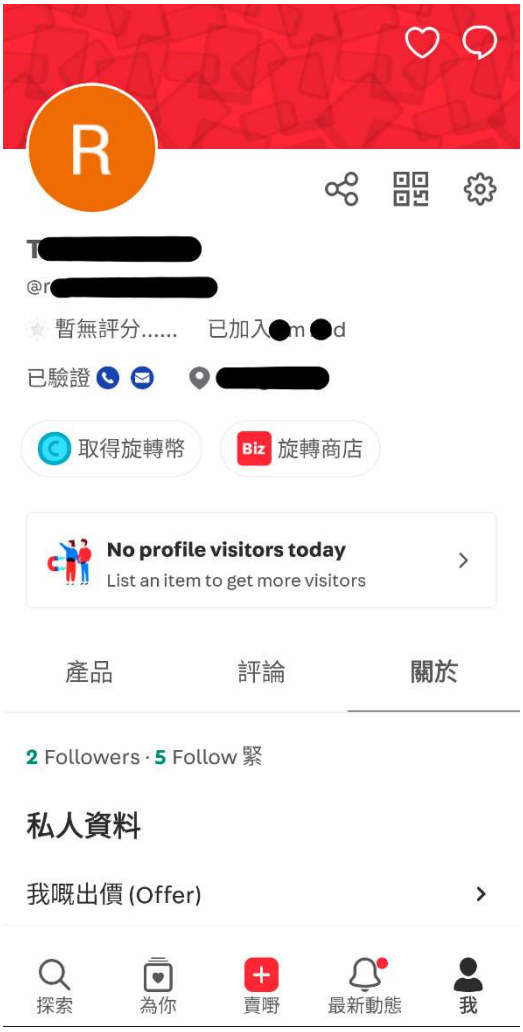
7. 希望透過 Carousell 買賣商品的用戶可在 Carousell 的網站[5]或其流動應用程式[6]建立一個用戶帳號。用戶在註冊時需提供其電郵地址、所在地區及流動電話號碼[7]。用戶可選擇提供額外資料，例如姓名、個人頭像、性別及出生日期。

---

4 Carousell 集團指營運 Carousell 的公司集團，包括 Carousell Pte Ltd 及 Carousell Limited。
5 https://www.carousell.com.hk/（供香港用戶使用的域名）
6 iOS 應用程式及 Android 應用程式。
7 用戶經 Carousell 網站使用電郵地址註冊用戶帳號時，必須提供其流動電話號碼。

8. Carousell 用戶的個人檔案一般會顯示其用戶名稱、姓名、個人頭像和所在地區（即公開版面）。用戶在註冊時提供的其他個人資料只會顯示給用戶本身（即私人帳號）。Carousell 亦包含類似社交媒體功能，允許用戶追蹤其他用戶或讓其他用戶追蹤自己。用戶的公開版面會顯示「Followers」和「Follow 緊」的數量。

用戶個人檔案



受影響的個人資料

9. 根據《私隱條例》第 2(1)條，「個人資料」是指任何直接或間接與一名在世的個人有關的資料，而從該資料直接或間接地確定有關的個人的身份是切實可行的；及該資料的存在形式令予以查閱及處理均是切實可行的。

10. Carousell Limited 表示共 324,232 個香港用戶帳號[8]受該事件影響。除了用戶公開版面中的資料（即用戶名稱、姓名和個人頭像）外，受影響用戶的電郵地址、電話號碼和出生日期（如有提供）亦在該事件中遭查閱及外洩。雖然如此，Carousell Limited 表示，身份證號碼、密碼相關資訊、信用卡或付款相關資訊未有在該事件中遭到外洩。

該事件及該保安漏洞

11. Carousell Limited 指出，Carousell 集團在 2022 年 1 月開始進行該系統遷移，並於 2022 年 1 月 15 日推出了一個使用者應用程式介面[9]（該應用程式介面），作為該涉及逾 200 個使用者應用程式介面的系統遷移過程的一部分。該應用程式介面用以顯示某一用戶所追蹤的所有用戶，而所顯示的資訊只應該包含用戶的公開資料，例如用戶名稱、姓名和個人頭像。

12. Carousell Limited 解釋， 由於人為錯誤，在該系統遷移過程中不慎遺漏了一個應該添加以把搜尋結果中涉及私人帳號的個人資料移除的編碼過濾器（該過濾器），導致該應用程式介面推出時顯示了額外無意被公開的個人資料。Carousell Limited 表示有關情況為編碼錯誤（即該保安漏洞）。

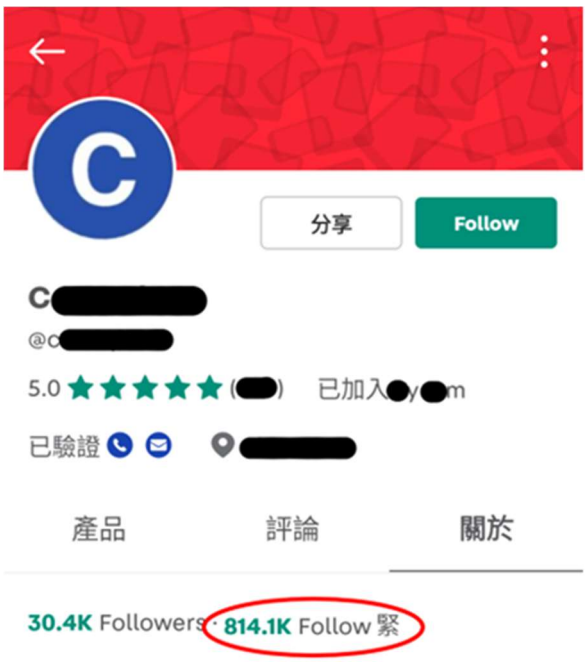
8 Carousell Limited 指出，個人可持有多於一個帳號。

9 即 user-facing Application Programming Interface (API)

13. Carousell 集團於 2022 年 9 月 15 日為一項新功能進行標準覆檢的過程中才發現該保安漏洞。Carousell 集團即日修復了該保安漏洞，以防止有人透過該應用程式介面未獲准許地查閱有關資料，並對 2022 年 1 月至 2022 年 9 月 15 日與該應用程式介面有關的數據進行了分析。分析結果顯示該應用程式介面在上述期間未有被異常濫用的情況，因此 Carousell 集團認為該保安漏洞已及時得到修補。

14. 2022 年 10 月 13 日，Carousell 集團注意到有人於網上平台放售 260 萬名 Carousell 用戶的個人資料。根據初步調查，Carousell 集團認為該事件只涉及影響新加坡用戶，但 Carousell 集團隨後於 2022 年 10 月 21 日確認香港用戶同樣受到影響。

15. 根據 Carousell 集團和該顧問公司的法證調查，攻擊者於 2022 年 5 月及 6 月通過一個來自緬甸的互聯網服務供應商的 IP 地址擷取了 46 個 Carousell 用戶帳號的資料。隨後，攻擊者利用這 46 個追蹤了大量其他 Carousell 用戶的帳號獲取了他們所追蹤的用戶的個人資料。下圖展示了該 46 個 Carousell 用戶帳號當中的其中一個帳號（已遮蔽個人資料）。



16. 根據 Carousell Limited 提供的資訊，以下為與該事件有關的主要事件:

日期／時段	事件
2022 年 1 月	該系統遷移開始進行。
2022 年 1 月 15 日	Carousell 集團推出該應用程式介面，作為該系統遷移過程的一部分。
2022 年 5 月至 6 月	攻擊者擷取 46 個 Carousell 用戶帳號的資料，並利用這 46 個帳號獲取他們所追蹤的 Carousell 用戶的個人資料。
2022 年 9 月 15 日	Carousell 集團發現及修復該保安漏洞。
2022 年 10 月 13 日	Carousell 集團在網上平台發現 260 萬名 Carousell 用戶的個人資料可供出售。
2022 年 10 月 14 日	Carousell 集團認為只有新加坡用戶受該事件影響。
2022 年 10 月 21 日	Carousell 集團確認香港用戶受該事件影響。

<u>Carousell Limited 就該事件的解釋</u>

17. Carousell Limited 承認，其負責並對遷移應用程式介面具有豐富經驗的高級工程師在該系統遷移的過程中不慎地遺漏了添加該過濾器，導致該應用程式介面顯示了額外無意被公開的個人資料。Carousell Limited 進一步表示，編碼覆檢員在編碼覆檢程序中亦未能發現有關的編碼錯誤。

18. Carousell Limited確認Carousell集團在展開該系統遷移前並沒有進行任何私隱影響評估。Carousell Limited指出，該系統遷移並非一項單獨事件，而是橫跨數月並牽涉數百個應用程式介面的遷移過程。Carousell 集團過往曾進行不同規模的系統遷移，有關過程中沒有個人資料受到影響。

19. 據Carousell Limited的說法，在完成任何功能及／或系統遷移的相關編碼程序後，Carousell 集團通常會先進行編碼覆檢，然後進行測試程序。然而，為該應用程式介面進行的上述兩項程序均未能發現遺漏了該過濾器。Carousell Limited解釋:-

「然而，考慮到有關的系統遷移涉及應用程式介面，我們需維持合約不變，以確保回溯兼容，並且不會對舊版客戶（iOS 應用程式和 Android 應用程式）產生任何問題。由於合約保持不變，我們的編碼覆檢程序未有發現遺漏了該過濾器。我們的團隊在測試過程中亦未有偵測到遺漏了的該過濾器，因為測試是針對用戶介面問題而進行，而遺漏的該過濾器不涉及用戶介面問題。

編碼覆檢程序主要針對該應用程式介面的功能，而非特定的保安問題。在進行該系統遷移時，我們沒有對每個應用程式介面的變更進行保安檢視，因為組建一個足夠龐大的保安團隊以進行這樣的人手覆檢對我們來說是不可行的。」[10]

20. Carousell Limited確認，在該事件發生之前，沒有就編碼覆檢和測試程序制定正式的書面指引。

21. 除上述個別的編碼覆檢和測試程序外，Carousell 集團根據其一般保安措施，在2022年2月委託了一家第三方網絡安全服務供應商進行滲透測試和安全評估，以檢查其網站和流動應用程式是否存在漏

[10] 翻譯自英文原文。

洞。在向該服務供應商查詢為何安全評估未能偵測到該保安漏洞時，該服務供應商解釋他們將有關評估的重點放在他們認為對 Carousell 更直接相關及風險更高的範疇，因此安全評估沒有涵蓋受影響的該應用程式介面。

22. 有關 Carousell 的監察系統，Carousell Limited 表示，Carousell 集團採用了「速率限制」[11]來偵測針對其網絡平台[12]和應用程式介面的異常活動。在該事件中，由於攻擊者的活動保持在速率限制以下，因此相關活動未能被偵測。

該顧問公司的調查結果

23. 根據 Carousell Limited，Carousell 集團在發現該事件後，委託了該顧問公司進行調查，以識辨針對該應用程式介面的潛在惡意活動，並判斷是否可以在更早的時間偵測得到該事件。

24. 該顧問公司確認攻擊者於 2022 年 5 月及 6 月擷取了 46 個 Carousell 用戶帳號的資料。攻擊者曾於 2022 年 10 月嘗試進行另一次帳戶擷取，但由於當時該保安漏洞已被修復，故攻擊者的行動沒有成功。

25. 該顧問公司的調查報告包含以下有關 Carousell 集團在該事件發生時的偵測能力的主要發現：—

(i) Carousell 集團進行的編碼覆檢程序沒有全面覆檢編碼的保安問題，如此的全面覆檢應可在推出該應用程式介面前偵測到其過於寬鬆的設定；

(ii) Carousell 集團就應用程式進行的滲透測試沒有發現該保安漏洞；及

[11] 一般指限制在指定時間內向伺服器或應用程式介面發出的請求數量。

[12] 網站及手機應用程式。

(iii) Carousell 集團沒有配置用於偵測應用程式介面異常活動的警報，因而沒有偵測到與該事件有關的惡意的指令。

Carousell 集團的改善措施

26. 根據 Carousell Limited，Carousell 集團在發現該事件後，已於 2022 年 10 月 13 日識辨攻擊者，並封鎖其帳號以及所有相關裝置和用戶。Carousell Limited 隨後向專員提交了資料外洩事故通報，並以電郵通知所有受該事件影響的用戶。

27. Carousell Limited 亦向專員表示，Carousell 集團已就員工意識、保安措施（包括偵測措施）、和安全評估方面採取了一系列的強化措施，以防止類似事件再次發生。基於 Carousell 集團保安措施的保密性，相關細節不會在本報告詳述。

III. 調查結果及違例事項

Carousell Limited 作為資料使用者

28. Carousell 是一個允許個人創建用戶帳號買賣商品的網上多元分類及二手交易市場。Carousell Limited 負責在香港營運 Carousell 市場。雖然 Carousell Limited 使用 Carousell 集團以中央化模式營運的資訊系統及資料庫，但 Carousell Limited 確認控制受該事件影響的 Carousell 香港用戶的個人資料的收集、持有、處理及使用。因此，Carousell Limited 屬《私隱條例》第 2(1)條釋義下的資料使用者[13]，須遵從《私隱條例》的規定行事，包括《私隱條例》附表 1 所列明的六項保障資料原則。

違反保障資料第 4(1)原則

29. 《私隱條例》附表 1 保障資料第 4(1)原則訂明，資料使用者須採取所有切實可行的步驟，以確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮 —

(a) 該資料的種類及如該等事情發生便能做成的損害；
(b) 儲存該資料的地點；
(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；
(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及
(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

[13] 根據《私隱條例》第 2(1)條，資料使用者，就個人資料而言，指「*獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人*」。

30. 經考慮與該事件有關的事實及在調查過程中所獲得的證據，專員認為該事件是由以下的缺失導致：—

(1) 未有在該系統遷移前進行私隱影響評估

31. 專員注意到 Carousell 集團的《Carousell 集團資料保護影響評估政策》[14]（該政策），連同其他規定，概述了應進行私隱影響評估的情況，其中包括「*建立涉及處理個人資料的新程序（包括人手程序）*」，以及「*更改現有系統或程序處理個人資料的方式*」[15]。

32. Carousell 集團於 2022 年 1 月 15 日推出該應用程式介面，作為該系統遷移過程的一部分，透過該應用程式介面顯示用戶公開版面的個人資料，屬改變處理個人資料的程序。然而，Carousell 集團在該系統遷移或推出該應用程式介面之前並未進行任何私隱影響評估。Carousell Limited 指出，該系統遷移並非一項單獨事件，而是橫跨數月並牽涉數百個應用程式介面的遷移過程，而 Carousell 集團過往曾進行不同規模的系統遷移，有關過程中沒有個人資料受到影響。

33. 專員不同意 Carousell Limited 的解釋。考慮到該系統遷移屬一項涉及數百個應用程式介面的大規模系統遷移，而且引入新的該應用程式介面導致了處理個人資料方式的變更，Carousell 集團理應加倍重視個人資料的保安，並按照該政策進行私隱影響評估，以徹底檢視該系統遷移的程序及識辨潛在的私隱風險和影響。專員認為，如果 Carousell 集團在該系統遷移前採取審慎的態度並進行私隱影響評估，理應可識辨潛在風險及採取適當措施（例如在推出該應用程式介面前進行有效的保安檢視）以防止該事件發生。

34. 專員認為，儘管 Carousell Limited 是使用由 Carousell 集團提供的中央化資訊系統及資料庫，但 Carousell Limited 作為資料使用者仍有確

[14] 譯自英文「Carousell Group Data Protection Impact Assessment Policy」；自 2021 年 4 月生效。
[15] 相關內文譯自該政策的英文版本。

切責任保障其控制的個人資料的安全。因此，Carousell Limited 在任何涉及香港用戶個人資料的系統遷移的過程中採取適當措施評估及減少保安風險是不可或缺的。在欠缺私隱影響評估的情況下，而 Carousell Limited 在該系統遷移進行前亦沒有查核有否進行私隱影響評估，明顯地使到 Carousell 用戶（包括香港用戶）的個人資料面臨重大風險。

(2) 不全面的編碼覆檢程序

35. 在推出新產品或新功能前進行安全評估，是識辨及修補保安漏洞和確保資料保安的重要步驟。雖然 Carousell 集團在完成該應用程式介面的編碼程序後進行了編碼覆檢及測試程序，但 Carousell Limited 承認有關編碼覆檢程序只針對該應用程式介面的功能而非保安問題，而有關測試程序亦是基於用戶介面進行，因而未有發現遺漏了該過濾器。Carousell Limited 解釋，在該系統遷移的過程中，由於 Carousell 集團無法組建一個足夠龐大的保安團隊以進行人手覆檢，因此他們沒有對每個應用程式介面的變更進行保安檢視。

36. 正如該顧問公司所指出，如果在該應用程式介面的推出前對其保安問題進行全面審查，應可偵測到其過於寬鬆的設定。進行全面的編碼覆檢程序以識辨潛在的保安問題，是防止資料外洩及確保應用程式或系統保安的有效方法。專員認為就新推出的應用程式介面進行全面的編碼覆檢程序尤其重要，而人手不足絕非不進行此類覆檢的理由。

37. Carousell 集團沒有進行全面的編碼覆檢程序以識辨潛在的保安問題，直接影響了包括香港用戶在內的所有 Carousell 用戶。因此，作為該事件中的資料使用者，尤其是就其控制的香港用戶的個人資料而言，Carousell Limited 仍然有責任採取所有切實可行的步驟保障由其持有或控制的個人資料，並須為沒有查核有否根據《私隱條例》下的資料保安規定進行全面的編碼覆檢程序負責。

(3) 與該系統遷移有關的安全評估有缺失

38. 專員注意到 Carousell 集團在 2022 年 2 月委託了一家第三方網絡安全服務供應商進行滲透測試和安全評估，以檢查其網站和流動應用程式是否存在漏洞，而這屬 Carousell 集團的一般保安措施的其中一部分。然而，由於有關滲透測試及安全評估並沒有涵蓋該應用程式介面，因此未能發現該保安漏洞。

39. 對整套系統進行定期和全面的安全評估是偵測保安漏洞和確保資料安全的重要步驟，特別是進行任何重大事件（例如系統遷移）之後。考慮到該系統遷移的龐大規模和該應用程式介面的功能（即顯示 Carousell 用戶的個人資料），Carousell 集團應明確指示服務供應商對特定應用程式介面進行安全評估。如果安全評估涵蓋了該應用程式介面，該保安漏洞理應會被發現，而該事件或可避免。專員對上述缺失表示遺憾。

40. 專員認為與該系統遷移有關的安全評估的缺失使到包括香港用戶在內的 Carousell 用戶的個人資料面臨重大風險。專員重申，就其控制的香港用戶的個人資料而言，Carousell Limited 沒有確保有否就系統遷移進行全面的安全評估一事，反映了他們就《私隱條例》下的資料保安規定執行上有缺失。

(4) 欠缺與編碼覆檢程序相關的書面政策

41. 人為錯誤往往是其中一個導致資料外洩的主要原因，而制訂書面政策設立明確的處事程序，可以大幅降低人為錯誤的風險。

42. 在該事件中，該過濾器的遺漏涉及雙重的人為錯誤。負責遷移該應用程式介面的高級工程師不慎地遺漏了添加該過濾器，而編碼覆檢員在該應用程式介面的編碼覆檢程序中亦未有發現編碼錯誤。

43. 專員注意到，Carousell 集團在該事件發生前沒有制訂任何與編碼覆檢程序有關的正式書面政策，專員認為這會導致進行任何編碼覆檢和測試時出現不一致的情況。如果 Carousell 集團制定了書面政策，具體說明編碼覆檢程序的內容／範疇和覆檢標準，員工便能更了解應如何進行編碼覆檢程序，從而減少人為偏差和錯誤的風險。

44. 此外，如上文第 35 及 36 段所述，在推出新產品或新功能前進行安全評估是重要的步驟。Carousell 集團應視保安檢視為編碼覆檢程序的其中一部分，並將此納入書面指引，以防止在審查程序中沒有進行安全評估。

45. 專員注意到，Carousell 集團在該事件發生後已採取補救措施，實施自動編碼覆檢程序以偵測任何個人資料外洩的可能，並已於新制定的書面政策詳細說明該程序。如果上述措施在該事件發生前已實施，該保安漏洞便可以在更早的階段被發現。

46. 如上文第 34 段所述，專員認為儘管 Carousell Limited 是使用由 Carousell 集團提供的中央化資訊系統及資料庫，但 Carousell Limited 作為資料使用者仍有確切責任因應經由資訊系統處理個人資料的程序實施合適的政策及流程，以保障由其控制的個人資料的安全。因此，專員認為 Carousell Limited 亦須為沒有查核有否制定與編碼覆檢程序相關的書面政策一事負責。

(5) 欠缺有效的偵測措施

47. Carousell Limited 表示，Carousell 集團已採用了速率限制來偵測異常活動，防止壞份子查閱其網絡平台及利用應用程式介面。然而在該事件中，由於攻擊者的活動保持在速率限制之下，因而未能偵測到其擷取活動。

48. 專員認為，機構必須採取有效措施偵測任何入侵或攻擊的跡象，以保護其系統內的資料免遭外洩。速率限制並非預防濫用的萬能措施。正如該事件所顯示，攻擊者可繞過速率限制作出攻擊，因此機構有需要採取額外措施偵測潛在惡意使用應用程式介面的活動。

49. 專員認為，Carousell 集團在事發前未有採取適當措施偵測異常模式或活動，也未有配置用於偵測潛在惡意使用應用程式介面的活動的警報，導致未能防止或偵測 Carousell 用戶的個人資料從該應用程式介面被擷取的情況。

50. 同樣地，專員認為 Carousell Limited 亦須為沒有確保已採取有效措施偵測異常活動負責，這屬另一項資料保安的缺失。

結論

51. 在考慮本個案所有證據後，專員認為 Carousell Limited 須為下列缺失負責：

(1) 沒有查核在該系統遷移進行前有否進行私隱影響評估。如有在該系統遷移前進行私隱影響評估，理應可識辨潛在風險及採取適當措施以防止該事件發生；

(2) 沒有查核有否進行全面的編碼覆檢程序，以致未能在該應用程式介面推出前偵測到其過於寬鬆的設定；

(3) 沒有確保有否就系統遷移進行全面的安全評估。如果安全評估涵蓋了該應用程式介面，該保安漏洞理應會被發現，而該事件應可避免；

(4) 沒有查核有否制定與編碼覆檢程序相關的書面政策。如果制定了書面政策，具體說明編碼覆檢程序的內容／範疇和覆檢

標準，員工便能更了解應如何進行編碼覆檢程序，從而減少人為偏差和錯誤的風險；及

(5) 沒有確保已採取有效措施偵測異常活動，導致未能防止或偵測 Carousell 用戶的個人資料從該應用程式介面被擷取的情況。

52. **考慮到 Carousell 廣泛的國際業務及服務的龐大活躍用戶數量，公眾會合理地期望 Carousell 集團（包括 Carousell Limited）投入足夠資源確保其資訊系統的穩健安全。然而，該事件揭示了 Carousell 在保障由其集團持有的個人資料的安全方面犯了根本性的失誤，實令人非常失望；專員認為，若當時有實施一般風險及安全評估及措施，該事件應可避免發生。專員對有關失誤導致 260 萬名 Carousell 全球用戶的個人資料及超過 32 萬名香港用戶的帳號遭到外洩表示遺憾。**

53. **雖然 Carousell Limited 在該事件發生時是使用由 Carousell 集團中央化模式下的資訊系統及資料庫，但 Carousell Limited 作為資料使用者仍有確切責任保障由其控制的個人資料的安全。在該事件中，專員認為 Carousell Limited 在查核和確保該系統遷移進行前有否實施妥善的檢查、政策及措施上存在明顯缺失，導致超過 32 萬的 Carousell 香港用戶的個人資料受影響。基於上述原因，專員認為 Carousell Limited 沒有採取所有切實可行的步驟確保涉事的個人資料受到保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，因而違反了保障資料第 4(1)原則有關個人資料保安的規定。**

54. 雖然 Carousell Limited 在該事件中有需要改善之處，但專員樂見 Carousell Limited 及時向公署及受影響的 Carousell 用戶作出資料外洩事故通報、積極配合公署的調查工作，並主動承認在事件中的不足。在該事件發生後，Carousell 集團致力從該事件中汲取教訓，並

已實施多項機構性及技術性的措施，以加強保障數據安全及防止類似事件再次發生。

IV. 執法行動

55. 根據《私隱條例》第 50(1)條，如專員在完成一項調查後，認為有關資料使用者正在或已經違反《私隱條例》下的規定，專員可向該資料使用者送達書面通知，指示該資料使用者糾正該項違反，以及（如適當的話）防止該項違反再發生。

56. 專員認為 Carousell Limited 在該事件中違反了《私隱條例》附表 1 的保障資料第 4(1) 原則，因此依據《私隱條例》第 50(1)條所賦予的權力向 Carousell Limited 送達執行通知，指示 Carousell Limited 採取以下步驟以糾正其違反事項，以及防止有關違規情況再次發生：

(1) 聘請獨立的數據安全專家檢視網站和流動應用程式，確保它們沒有編碼錯誤和已知的保安漏洞；

(2) 制訂本地政策及程序，以保障香港的 Carousell 用戶的數據安全，包括但不限於在系統及／或應用程式發生重大改變或引入新科技時，進行私隱影響評估、漏洞掃描和安全評估的政策和程序；

(3) 制訂本地政策及程序，以確保對用於偵測潛在惡意使用應用程式介面的安全措施足夠及達至行業標準，並進行定期檢視；

(4) 制訂本地政策及程序，以確保已制訂及定期檢視有關進行及檢查系統遷移和編碼覆檢的政策及程序；

(5) 制訂有效措施以確保員工依循與上述第(2)至(4)項的指示有關的政策及程序；

(6) 加強數據安全及資料保護的培訓，每年至少為全體員工舉辦一次講座／研討會／工作坊，並建立評估機制，確保員工準

確理解相關課程內容；及

(7) 由執行通知的日期起計兩個月內向專員提供文件，證明已完成上述第(1)至(6)項的指示。

57. 根據《私隱條例》第 50A 條，資料使用者違反執行通知，即屬犯罪，一經首次定罪，最高可被判處第五級罰款（即港幣 50,000 元）及監禁兩年。

V. 建議

58. 《私隱條例》第 48(2)條訂明，專員在完成一項調查後，如認為如此行事是符合公眾利益的，可發表報告列明該項調查的結果及由該項調查引致的、專員認為適合作出的任何建議或其他評論。專員希望藉此報告，就個人資料的資訊系統遷移，向機構作出以下建議，以加強數據安全：—

(1) 進行私隱影響評估

59. 專員建議機構在推出任何涉及處理大量個人資料的新項目、系統或服務前，應進行私隱影響評估。當機構涉及處理個人資料的系統或行事方式出現重大改變及引入新科技時，機構亦應進行私隱影響評估。

60. 進行私隱影響評估可幫助機構及早發現潛在的安全風險，並作出必要的改進，同時釋除公眾和持份者對私隱的疑慮。在進行私隱影響評估時，機構應全面檢討個人資料私隱所面對的影響和風險，並針對有關影響及風險採取足夠的措施，以防止或減低資料外洩所造成的不良影響，以及確保有關個人資料的收集、保留、使用及保安符合《私隱條例》的規定。

(2) 制定確保數據安全的遷移計劃

61. 機構應在考慮與系統遷移有關的所有資料保安風險後，制定明確的遷移計劃。這包括評估需要遷移的系統和應用程式的敏感程度，並確定在遷移期間及之後應採取的步驟以維護系統和應用程式的安全。機構應制訂明確的書面政策及程序，讓員工全面了解實施的細節，從而減少出現人為錯誤的風險。

(3) 進行有效的漏洞評估

62. 機構應在系統遷移後進行漏洞評估，以查找任何可能被攻擊者利用的潛在保安漏洞。不論是由內部員工抑或第三方服務供應商進行該評估，機構必須清楚地向評估人員述明評估的範圍及與評估的系統和應用程式相關的所有必要信息。如聘用第三方服務供應商，機構應盡力確保他們有足夠能力進行評估，並向他們發出清晰指示，以確保評估的範圍足夠。

(4) 提供相關的員工培訓

63. 員工培訓對於確保參與系統遷移的員工了解數據安全的重要性及遵循最佳做法至關重要。如果遷移涉及編碼，則應培訓或指導員工掌握編碼覆檢的最佳做法，以維護數據安全。通過提供相關的員工培訓，讓機構可確保員工掌握在遷移過程中保護個人資料所需的知識和技能。

(5) 實施有效的檢測機制偵測異常活動

64. 為偵測潛在惡意使用應用程式介面的活動，機構應該監控公共應用程式介面流量。除了實施速率限制以限制請求數量外，機構亦應監控已知的攻擊模式及實施適當措施來預防這些攻擊，例如設立 CAPTCHA 驗證碼、使用機器學習和異常檢測、掌握最新的威脅情報等。

(6) 制訂地區性政策及程序

65. 跨國企業除採用全球通用的政策以外，亦應因應地區的環境因素及法規制訂地區性政策及程序，從而確保在香港的資料當事人的個人資料私隱受到保障，並遵從《私隱條例》的規定。

－完－