根據《個人資料（私隱）條例》（第 **486** 章）第 **48**（**2**）條發表

調查報告：
香港航空旅遊有限公司經流動應用程式「俠客行・旅行」外洩顧客個人資料

（中文譯本）

（本報告以英文編寫，如此中文譯本與英文版報告有歧異或矛盾，概以英文為準）

報告編號： R14 – 6453

發表日期：**2014** 年 **12** 月 **15** 日

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

香港航空旅遊有限公司經
流動應用程式「俠客行・旅行」外洩顧客個人資料

個人資料私隱專員（「**專員**」）根據《個人資料（私隱）條例》（第486章）（「**條例**」）第38(b)條對香港航空旅遊有限公司進行調查，並根據條例第VII部行使賦權發表本報告。條例第48(2)條列明，*「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－*

(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。」*

蔣任宏
個人資料私隱專員

調查報告：香港航空旅遊有限公司經流動應用程式「俠客行・旅行」外洩顧客個人資料

本報告是就調查資料外洩事故而作出的，該事故涉及香港航空旅遊有限公司（「港航旅遊」）經運行於iOS平台的流動應用程式「俠客行・旅行」外洩顧客的個人資料。個人資料私隱專員認為港航旅遊沒有採取所有合理地切實可行的步驟，確保顧客的個人資料受保障而免受未獲准許或意外的查閱，違反《個人資料（私隱）條例》下的保障資料第4原則。

背景

香港航空有限公司前附屬的香港航空旅遊有限公司(「**港航旅遊**」) 於 2010 年開發及營運名為「俠客行・旅行」[1](「**俠客行**」) 的流動應用程式 (「**程式**」)。俠客行是一個旅遊助理程式，為流動裝置用戶提供在線服務，包括預訂及購買機票、航程管理、搜尋目的地資訊，及為旅客提供社交網絡平台。

2. 2013 年 9 月 30 日，港航旅遊向本署提交「資料外洩事故通報表格」，通報六名顧客的個人資料於 2013 年 9 月 19 日經運行於 iOS 平台[2]的俠客行外洩。事故中外洩的個人資料包括顧客的姓名、身份證或護照號碼、性別、電話號碼、電郵地址及出生日期。

3. 香港航空有限公司於 2013 年 9 月 25 日接獲一名顧客投訴俠客行外洩資料，因而揭發是次事故。該公司同日通知港航旅遊。

4. 個人資料私隱專員（「**專員**」）跟進事件，並依據《個人資料（私隱）條例》(「**條例**」）第 38(b)條向港航旅遊展開調查。

條例的相關規定

5. 條例旨在保障個人資料私隱。根據條例，資料使用者有責任依從條例附表 1 的六項資料保障原則的規定。條例第 2 條訂明，「資料使用者」是指獨自或聯同其他人或與其他人共同控制個人資料的收集、持有、處理或使用的人。與本調查直接有關的是條例附

[1] 根據蘋果公司的 App Store，這流動應用程式的名稱是「俠客行・旅行 (TravelBud)」。

[2] 由蘋果公司開發的流動操作系統，只限蘋果公司的流動裝置使用。

表 1 的保障資料第 4 原則及條例第 65 條。保障資料第 4 原則訂明：

> 「*(1) 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（包括採用不能切實可行地予以查閱或處理的形式的資料）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。*
>
> *(2) 在不局限第(1)款的原則下，如資料使用者聘用（不論是在香港或香港以外聘用）資料處理者，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。」*

6. 根據條例第 2 條，「切實可行」指合理地切實可行。

7. 條例第 65(2)條訂明：

> *「任何作為另一人的代理人並獲該另一人授權（不論是明示或默示，亦不論是事前或事後授權）的人所作出的任何作為或所從事的任何行為，就本條例而言須視為亦是由該另一人作出或從事的。」*

調查所獲得的資料

8. 在調查過程中，本署向港航旅遊作出查詢，並審視了該公司提供的文件證據。以下為本署所獲得的相關資料。

俠客行的開發及營運

9. 俠客行在兩個流動應用平台運行：Google 公司開發的 Android 及蘋果公司開發的 iOS。這程式於 2012 年 7 月 24 日及 2012 年 9 月 4 日分別於 Android 及 iOS 平台首次推出。是次事故只涉及在 iOS 平台運行的俠客行程式。

10. 港航旅遊把俠客行的開發工作外判予佰邦達科技（北京）有限公司(「**佰邦達**」)。該公司是一間以內地為基地的軟件開發商。除開發工作外，佰邦達亦根據港航旅遊的要求為俠客行的軟件提供維修支援、解決程式缺陷及提升版本等工作。在開發俠客行時或其後的保養期間，港航旅遊均沒有提供或託付任何顧客的個人資料予佰邦達作處理或測試。此外，佰邦達並無權查閱儲存於俠客行後端資料庫的港航旅遊的顧客個人資料。

俠客行的使用及用戶識別碼

11. 會員及非會員均可瀏覽及使用俠客行所提供的服務及功能。在是次事故發生之時，約有 25,000 會員使用俠客行。在 2012 年 7 月至 2014 年 6 月期間，會員及非會員透過俠客行共作出大約四萬宗交易及八萬次查詢。

12. 非會員可以瀏覽及使用該程式的大部分功能，包括預訂及購買機票和年票[3]，以及訂單查詢。在預訂過程中，非會員須提供乘客的個人資料，包括全名、性別、出生日期、身份證或護照號碼，及聯絡人的個人資料，包括姓名、電話號碼及電郵地址。

13. 在首次預訂及購買機票和年票時提供的個人資料會儲存於俠客行的後端資料庫。如果非會員日後進入俠客行預訂或購買機票及作出訂單查詢時，無需再次輸入個人資料。因為，港航旅遊會利用該流動裝置的 MAC 位址[4] 作為參數，連繫俠客行的後端資料庫中該非會員早前已輸入的資料。

14. 另一方面，會員除可瀏覽及使用俠客行的所有功能外，亦可在購買機票或年票時享有折扣。如登記為會員，用戶必須提供

[3] 包含多張機票，可在一年內使用。

[4] 媒體存取控制位址 （"**MAC 位址**"）是編配予網絡界面的獨一無二的識別碼，作為實體網絡分段的溝通之用。它是一組共有 48 位元的數字，以 16 進位表示，通常由網絡界面的製造商編配。此位址存在於所有具網絡接駁功能的流動電腦裝置中。

電郵地址及密碼以開立用戶登入帳戶。他們亦可利用現有的社交網絡帳戶開立用戶登入帳戶[5]。俠客行會以用戶登入資料識別每名會員。

15. 會員首次預訂或購買機票和年票時，必須輸入上述第 12 段所述的相同種類的個人資料。透過會員登入程序，會員在其後的交易（包括訂單查詢）可免卻再次輸入個人資料。

16. 下表列出俠客行向會員及非會員提供的主要功能及識別用戶的方式：

	俠客行的功能	**會員**	**非會員**
(1)	預訂及購買機票	✓	✓
(2)	購買年票	✓	✓
(3)	換取年票	✓	×
(4)	訂單查詢	✓	✓
連繫後端資料庫與用戶的識別參數		用戶登入資料	MAC 位址

俠客行的保安措施

17. 俠客行所收集的所有個人資料是儲存在其後端資料庫伺服器內。該伺服器是位於港航旅遊在中國北京的外判數據中心。港航旅遊確認，除了會員的登入密碼外，該伺服器所儲存的個人資料是沒有加密的。

事故原因

18. 當非會員首次預訂或購買機票或年票時，俠客行會要求其流動裝置的 iOS 操作系統（不論哪個版本）提供該裝置的 MAC 位址。這個 MAC 位址會記錄於俠客行的後端資料庫。

19. 當該非會員日後再預訂或購買機票或年票，或查詢訂單時，俠客行會再次提取其流動裝置的 MAC 位址，並與後端資料庫核對以識別用戶身份。在核對成功後，之前根據 MAC 位址所儲存的資料會從資料庫提取，顯示於流動裝置上。下列分段述明在成功核對後流動裝置會顯示的資訊：－

[5]俠客行接受騰訊及新浪微博帳戶作登記。

19.1 預訂機票

在輸入個人資料並完成預訂後，在同一螢幕版面中，乘客的全名及身份證或護照號碼會在「歷史乘機人」一欄下顯示，而聯絡人的姓名及電話號碼會在「歷史聯絡人」一欄下顯示。非會員可點擊「歷史乘機人」或「歷史聯絡人」的連結，存取及更新資料，以作進一步預訂及購買。

19.2 購買年票

情況與預訂機票類似，非會員在輸入個人資料並完成購買年票後，「歷史乘機人」及「歷史聯絡人」的資料會被建立，而其後可作存取及更新。

19.3 訂單查詢

非會員透過「訂單查詢」的功能，可檢視他的訂購狀況，包括訂購日期、付款進程、機票發出情況及已取消的訂單。

20. 在運行 iOS6 或之前版本的流動裝置中，利用其 MAC 位址以識別用戶身份的方式操作俠客行是沒有問題的。iOS6 或之前版本的流動裝置與後端資料庫的核對詳情，請參閱**附件 A**。

21. 2013 年 9 月 18 日（美國時間），蘋果公司推出新的流動操作系統 iOS7，用戶可於同日把其流動裝置更新至 iOS7。以保護私隱為由， iOS7 阻止所有程式讀取 MAC 位址作為流動裝置的識別參數。為回應程式要求流動裝置提供該裝置的 MAC 位址，iOS7 會向程式提供一組固定數字，而不是披露真正的 MAC 位址。

22. 結果是，每當非會員在 iOS7 版本的流動裝置透過俠客行預訂或購買機票或年票時，iOS7 均會以相同的虛假 MAC 位址[6] 回應。這組數字位址在所有運行 iOS7 版本的流動裝置都相同。基於

[6] iOS7 的固定 MAC 位址是 02:00:00:00:00:00。
參考資料:
https://developer.apple.com/library/IOs/releasenotes/General/RN-iOSSDK-7.0/index.html#//apple_ref/doc/uid/TP40013202-CH1-SW33

此情況，所有非會員在 iOS7 環境下進行的所有交易，均擁有相同的虛假 MAC 位址而被視為由同一個人所作出的。

23. 因此，在 2013 年 9 月 19 至 25 日（香港時間）期間，當非會員以運行 iOS7 版本的流動裝置作交易或查詢時，俠客行不單顯示他的記錄（訂購記錄及個人資料），還會顯示其他非會員（同樣使用運行 iOS7 版本的流動裝置）的個人資料。在事故中，共有六名顧客的個人資料因這方式而外洩予其他非會員。使用 iOS6 或之前版本的非會員沒有受影響。俠客行在 iOS7 的操作示範（特別是 iOS7 版本的流動裝置與俠客行的後端資料庫核對失敗的情況），請參閱**附件 B**。

調查結果

24. 根據保障資料第 4 原則，資料使用者須採取所有合理地切實可行的步驟，以確保個人資料受保障而不受未獲准許的或意外的查閱，尤其須考慮該資料的種類及如該等事情發生便能做成的損害。雖然保障資料第 4 原則並不是要求資料使用者對其持有的個人資料的保安提供絕對保證，但專員須考慮港航旅遊在營運俠客行時是否已採取所有合理地切實可行的措施，保護個人資料。

港航旅遊及佰邦達是否已迅速回應流動裝置操作環境的轉變

25. 正如第 10 段所述，港航旅遊把俠客行的開發外判予佰邦達。在公署調查期間，港航旅遊聲稱在事故前，他們負責就俠客行的功能和特點提出更改，而佰邦達負責更新該程式及每星期檢查蘋果公司最新的相關資訊。佰邦達承認直至外洩事故於 2013 年 9 月 25 日被揭發前，該公司沒有採取任何行動以更新俠客行。

26. 專員知悉 iOS7 更改 MAC 位址的操作模式有助保障用戶私隱，以防止用戶在不知情或沒有同意下被程式持續追蹤。蘋果公司於 2013 年 6 月 10 日在美國三藩市舉行的世界開發商會議首次告知程式開發商即將推出 iOS7。在會議後，該公司隨即把所有闡釋 MAC 位址的新操作模式的演示材料上載至互聯網。蘋果公司其後亦透過電郵把這項變更通知其付費程式開發商[7]（「**付費開**

[7] 它們是向蘋果公司登記參與 iOS 開發商計劃的程式開發商，每年繳付費用。付費開發商可預先得到蘋果公司的開發商工具及支援，並收取蘋果公司的最新消息和電郵通知。程式開發商亦可免費登記為蘋果開發商，藉以取得某些建立 iOS 程式的開發商工具和資源，以及蘋果公司的公告。

發商」）及其他已登記的程式開發商。

27. 2013 年 8 月 22 日， 蘋果公司在其開發商專屬平台向所有已登記的程式開發商（不論付費與否）重申 MAC 位址的操作模式的改變及影響：

> *「如你的程式使用 MAC 位址來識別 iOS 裝置，系統會回應所有運行 iOS7 的裝置一個相同不變的數值。請更新你的程式以使用 UIDevice 的 identifierForVendor 功能。如你需要識別碼作廣告用途，請使用 ASIdentifierManager 的 advertisingIdentifier 功能。」*

28. 此外，由 2013 年 6 月 10 日世界開發商會議日至 2013 年 9 月 18 日 iOS7 正式推出日這段期間，蘋果公司共向付費開發商提供了六個 iOS7 測試版，讓他們測試程式。

29. 然而，佰邦達經港航旅遊表示它在 2013 年 9 月才登記參與 iOS 開發商計劃，之前並沒有收到蘋果公司有關推出 iOS7 的任何通知。直至蘋果公司於 2013 年 9 月 11 日對外公告 iOS7 將於 2013 年 9 月 18 日正式推出，它才首次獲得有關資訊。

30. 專員認為佰邦達的解釋難以接受。作為專門從事程式開發的科技公司，佰邦達在 2013 年 9 月 11 日前一直未留意到蘋果公司就有關流動操作系統變更或更新所發出的任何通知或消息，令人難以置信。即使佰邦達在 2013 年 9 月才登記參與 iOS 開發商計劃而之前沒有收到蘋果公司的電郵通知，但它仍應跟貼蘋果公司的消息及最新科技資訊。

31. 事實上，蘋果公司於推出新的 iOS 版本前三個月作出通知（由 2013 年 6 月 10 日的世界開發商會議至 2013 年 9 月 18 日 iOS7 正式推出）是其慣常做法，與之前推出 iOS 各版本的做法一致。專員認為蘋果公司已就 iOS7 推出時間及有關 MAC 位址的變更向程式開發商給予充足的通知。在透過不同渠道重覆通知程式開發商有關的更新，並在正式推出前向他們提供 iOS7 測試版，蘋果公司已採取合理措施確保沒有現行程式因 iOS7 的變更而受到不利影響。

32. 然而，即使佰邦達真的在 2013 年 9 月 11 日才首次知悉 iOS7 將會推出，它仍有足夠時間（由該日至 2013 年 9 月 18 日 iOS7 正

式推出尚有一個星期時間）採取行動，更新程式以防資料外洩。

33. 鑑於以上所述，專員認為佰邦達未能應對 MAC 位址操作模式的變更，是導致是次資料外洩事故的主因。佰邦達作為程式開發公司，獲受聘以保養其開發的程式，但卻明顯地沒有盡其責任。雖則如此，佰邦達在事件中只是港航旅遊的外判代理。在開發時或其後保養俠客行的軟件期間，港航旅遊並沒有提供或託付顧客的個人資料予佰邦達作處理或測試，佰邦達亦沒有權限查閱俠客行後端資料庫內的個人資料。因此，佰邦達沒有控制個人資料的收集、持有、處理或使用，所以不屬條例下的資料使用者。亦正因如此，專員不能對佰邦達直接採取執法行動。

34. 然而，憑藉條例第 65(2)條，代理人獲某人授權而代該人所作出的任何作為或所從事的任何行為，須視為亦是由該人作出或從事的。基於上述規定，儘管港航旅遊已把開發及保養俠客行的工作外判予佰邦達，但港航旅遊作為資料使用者，仍須就是次個人資料被未獲准許或意外地存取的事件負責。

結論

35. 根據上述分析及結果，專員裁定港航旅遊沒有採取所有合理地切實可行的步驟，確保它經俠客行處理的個人資料受保護而不受未經准許或意外的查閱，違反了保障資料第 4(1)原則。

補救行動

36. 根據條例第 50(1)條，專員在完成一項調查後，認為有關的資料使用者現正違反或已經違反條例的規定，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。

37. 2013 年 9 月 25 日，港航旅遊在接獲顧客投訴後，立即停止非會員透過俠客行購買年票及查詢訂購記錄的功能。非會員因而不能查閱任何「歷史乘機人」及「歷史聯絡人」的資訊。其後，港航旅遊適時地通知所有受事故影響的人士，亦沒有再接獲投訴。

38. 2013 年 10 月 1 日，港航旅遊發出在 iOS 平台運作的俠客行更新版本，作出了下述補救措施：

(i) 非會員在預訂及購買機票時，俠客行不再以 MAC 位址作為流動裝置的識別參數；
(ii) 非會員查詢「歷史乘機人」及「歷史聯絡人」資訊的功能已停止；
(iii) 非會員的訂單查詢功能已停止。只有會員才可透過用戶登入帳戶查詢訂購記錄；
(iv) 限制只供會員利用其帳戶登入才可購買及換取年票；及
(v) 非會員仍可購買機票，惟在每次購買時均須提供乘客及聯絡人的個人資料。

39. 2013 年 10 月 12 日， 港航旅遊亦把第 38 段所述的措施應用於在 Android 平台操作的俠客行版本。

40. 基於港航旅遊已取消以 MAC 位址作為識別參數、停止非會員查詢「歷史乘機人」及「歷史聯絡人」資訊及訂單查詢的功能，以及限制只供會員購買年票等措施，專員認為港航旅遊已採取足夠步驟，補救違規情況及防止是項違反再發生。

41. 專員進一步知悉俠客行的法律擁有權已於 2014 年 1 月由港航旅遊轉移予內地的大新華運通國際旅行社[8] ，因此俠客行的繼後開發及保養會在香港管轄範圍以外的地方進行。

42. 基於上述情況，專員在本個案沒有向港航旅遊送達執行通知。雖則如此，專員已向港航旅遊作出警告，如它日後在類似情況中沒有遵守條例的相關規定，專員會考慮對港航旅遊採取執法行動，包括送達執行通知。

其他評論

給程式開發商及將流動應用程式開發工作外判的機構的建議

43. 流動應用程式已是日常工具，改變了商業運作模式及個人生活。人們時常透過流動裝置使用流動應用程式，例如查看帳戶餘額、購物、瀏覽新聞，以及即時與親友聯繫等。程式開發商經常透過流動應用程式收集及處理範圍廣泛的個人資料。因此，他

[8] 港航旅遊及大新華運通國際旅行社均屬一間在中國內地註冊的公司的附屬公司。

們在保障使用流動裝置的私隱事宜中擔當重要角色。雖然大部份的程式開發商屬中小型企業，然而它們就遵從條例的規定仍有不可推卸的責任。專員建議這些程式開發商應善加利用專員開辦的講座及發出的最佳行事方式指引。同時，它們亦有責任跟貼最新的科技發展及趨勢，以確保在更新其開發的流動應用程式並改進有關功能時，不會影響私隱及資料的保護。

44. 當機構外判程式的開發時，應小心揀選有良好辦事能力和信譽的程式開發商。如聘用外判代理時沒有採取妥善的措施，個人資料一旦因代理的疏忽而外洩或遭濫用，可能會對其顧客造成嚴重傷害並影響公司商譽。

聘用外判程式開發商時應採取的措施

45. 條例保障資料第 4(2)原則規定，如資料使用者聘用資料處理者代其處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。根據條例保障資料第 2(4)原則，「資料處理者」指代另一人處理個人資料；及並不為該人本身目的而處理該資料的人。

46. 在本案中，由於港航旅遊在聘用佰邦達開發及保養俠客行軟件時沒有向其提供或交託任何個人資料，佰邦達因此不屬條例下的資料處理者。然而，事件正因為佰邦達的疏忽而沒有更新程式，導致港航旅遊持有的客戶個人資料受影響。

47. 雖然保障資料第 4(2)原則未能直接應用於本事件，但是根據保障資料第 4(1)原則資料使用者仍有責任採取所有合理地切實可行的步驟，保障其持有的個人資料的安全。專員建議資料使用者在聘用外判程式開發商時，應採取合約規範方法或其他方法規定程式開發商[9]：

(i) 制定妥善的程式開發及變更控制政策、指引及程序；
(ii) 就程式的設計和運作制定風險評估程序；
(iii) 使用正版及可靠的開發工具和軟件；
(iv) 備有保安措施，例如加密、存取控制、密碼政策；

[9] 有關把個人資料的處理外判予代理的規定，請參閱本署於2012年9月發出的《外判個人資料的處理予資料處理者》資料單張。

(v) 制定向操作系統開發商查閱或索取最新資料的程序；

(vi) 如情況合理，受資料使用者或獨立第三方檢查及審核；及

(vii) 除非可保證有相同程度的保障，否則不得把工作分包或再外判。

個人資料加密

48. 專員知悉儲存於俠客行後端資料庫伺服器的所有個人資料，除了用戶登入帳戶的密碼外，其餘是沒有加密的。雖然這並非導致是次事故的直接原因，但作為審慎的資料使用者，應確保儲存於後端伺服器的敏感個人資料（例如身份證及護照號碼）獲存取控制及加密的保護，以免受未經准許的查閱，並減低一旦資料外洩時對資料當事人造成的傷害。