



二十三條立法入快車道 李家超今公布公眾諮詢

詳刊A5

私隱公署點名本港多間連鎖食店 揭蒐資料用作促銷

電子點餐有伏 私隱外洩難防



◆私隱專員公署昨日點名多間本港知名連鎖餐廳，指出這些食店通過電子點餐收集顧客個人資料用作促銷。

香港文匯報記者黃艾力 攝

在香港，餐廳掃碼點餐愈漸普遍，此種點餐方式在方便了消費者的同時，亦帶來過度收集個人信息、增加信息外洩等風險。私隱專員公署昨日表示，去年接獲 157 宗資料外洩事故通報，按年大幅增加 50%。公署並調查 60 間本地餐廳使用電子點餐的私隱情況，發現部分餐廳會透過二維碼及手機應用程式點餐服務，收集顧客的手機號碼、電郵地址等個人資料，所有提供手機應用程式點餐服務的餐廳，均會進行用戶追蹤及作直接促銷，可使用顧客資料以獲取其交易紀錄、位置資料、喜好及行為等信息。公署建議飲食業界提供不涉及收集個人資料的點餐方式，並提醒顧客進行電子點餐時，需仔細考慮是否提供個人資料。

◆香港文匯報記者 郭倩

私隱專員公署昨日總結去年工作，並發表《電子點餐的私隱關注》報告，指出公署去年 11 月至今年 1 月期間，派員走訪 60 間本地餐廳。

實測發現，全部被檢視的餐廳均有提供非電子點餐方式，而所有提供手機應用程式點餐服務的餐廳，均會進行用戶追蹤以及直接促銷，當中 4 間提供二維碼點餐服務的餐廳，會收集顧客的手機號碼及電郵地址。

10 餐廳要求填姓名手機號或電郵

麥當勞、星巴克、譚仔米線、譚仔三哥米線等 10 間提供手機應用程式點餐的連鎖餐廳，會要求顧客必須註冊賬戶，過程中要顧客提供姓名、手機號碼或電郵地址。

此外，大家樂、大快活、肯德基和香港吉野家這 4 間連鎖餐廳，雖然允許以訪客身份點餐，但結賬時仍會收集用戶的個人資料。

私隱專員公署首席個人資料主任郭正熙指出，所有提供手機應用程式點餐服務的餐廳，均會進行用戶追蹤及直接促銷，餐廳可使用顧客資料追蹤其在手機應用程式內進行的活動，涉及的資料包括裝置資料、交易紀錄、位置資料、喜好及行為、活動紀錄及購買紀錄等。

同時，這些餐廳均在收集個人資料聲明中表示，擬將顧客個人資料用作直接促銷，當中 9 間餐廳在顧客註冊時提供選項，讓顧客選擇是否同意接收推廣訊息或促銷資訊，但有 7 間餐廳把有關選項預設為同意，沙爹王更未有在手機應用程式提供選項，讓顧客選擇是否同意個人資料用作直銷用途。

郭正熙並指出，使用二維碼點餐有私隱風險，一旦二維碼遭他人篡改，顧客則可能被引導往假網站，且顧客手機被下載惡意軟件，可能令裝備儲存的個人資料外洩。



◆私隱專員鍾麗玲昨日發表工作報告。香港文匯報記者黃艾力 攝

私隱專員鍾麗玲表示，電子點餐愈趨普及，顧客在餐廳使用手機應用程式或二維碼進行自助點餐時，應了解程式會查閱、收集或分享哪些資料，仔細考慮是否需要提供個人資料，或下載及選用有關的應用程式。

忠告掃二維碼留意是否被竄改

郭正熙亦提醒市民要考慮實際需要，決定程式的存取權限，以及留意有關手機程式有否提供選項讓顧客選擇是否同意接受直接促銷。此外，掃描二維碼前亦要提高警覺，留意二維碼有否被竄改，不要掃描一些來歷不明的二維碼。

公署並建議飲食業界向顧客提供不涉及收集個人資料的點餐方式，並容許顧客以訪客身份點餐，不收集顧客的個人資料，或按實際所需收集最小量的個人資料。如擬使用個人資料作直接促銷，應清晰告知顧客並就此徵求他們的同意，有關選項不應預設為同意。

另外，應定期檢查所提供的點餐二維碼有否被惡意竄改，並需要制訂明確的資料保留政策，定期刪除過時或不必要的顧客資料，以減少資料外洩的風險。

市民使用電子點餐 保障私隱建議

使用手機應用程式點餐

- ◆應了解應用程式會查閱、收集或分享哪些資料，以決定是否下載及選用有關程式，應透過官方渠道下載應用程式
- ◆考慮是否僅為堂食點餐功能而使用應用程式並開立賬戶
- ◆以訪客身份點餐時，須考慮所需個人資料類別是否必需，不超乎適度及是否可在不提供有關資料下仍可點餐
- ◆仔細閱讀收集個人資料聲明，了解餐廳收集個人資料目的及用途
- ◆考慮實際需要而決定應用程式的存取權限，及檢查預設保安或私隱設定以設置最高私隱權限
- ◆留意有關手機應用程式有否提供選項讓顧客選擇是否同意接受直接促銷，並根據自身需要作出相應選擇

掃描二維碼點餐

- ◆掃描二維碼前要提高警覺，留意二維碼有否被竄改，不要掃描來歷不明的二維碼
- ◆檢查二維碼導向的網站及第三方點餐平台的真確性
- ◆先了解可否在不提供個人資料情況下完成點餐，或僅提供完成點餐所需的最小量資料
- ◆盡量使用在手機內置的功能掃描二維碼
- ◆切勿將點餐二維碼上載到社交平台，以免有機會令第三者使用二維碼進行點餐，導致財物損失

◆資料來源：個人資料私隱專員公署
◆整理：香港文匯報記者 劉明

議員批收集食客資料無王管

香港文匯報訊（記者 郭倩）顧客在餐廳進行電子點餐時被收集個人資料且有被洩露的風險，法律界立法會議員江玉歡昨日接受香港文匯報訪問時表示，特區政府現時對餐廳利用電子點餐收集顧客個人資料的行為缺乏監管，「幾乎完全沒有監管，也沒有對商家提供的電子點餐服務進行抽查，這樣令很多餐廳利用這種方式收集顧客個人資料，從而導致顧客的個人資料被洩露的風險更高，政府應該要思考如何對電子點餐時收集顧客個人資料的行為進行監管。」

她認為，政府至今未對該種行為進行規管最大原因，是缺乏資源，「因為採用電子點餐服務的中小型餐廳有很多，並且這些商戶很多都不熟悉法例，政府有需要將相關資訊對各個餐廳進行普及。」江玉歡指，即使餐廳收集資料的本意只是想做推廣，然而由於大部分中小型公司一般是向電腦公司購買服務，然後將顧客的資料上載到一個終端機，在此過程中，有可能導致顧客的個人資料洩露。

商家須明確告知收集資料目的

當顧客發現個人信息被洩露，江玉歡提醒市民需要第一時間向私隱專員公署舉報，「市民如果要索償，要開出各種證明，這是一件非常麻煩的事情，所以建議先向私隱專員公署舉報。」她續說，即便透過私隱專員公署追討，相關流程亦比較繁複，希望在執行追討的流程上能夠鬆綁。

此外，她指出政府現時對洩露顧客個人信息的公司懲罰力度不足，「幾乎沒什麼罰則，只是對這些洩露了顧客個人信息的公司進行譴責，這毫無阻礙力，難以保障顧客的權益。」

她認為，其實餐廳在讓顧客進行掃碼點餐時沒有必要收集個人信息，倘商家希望顧客註冊會員或獲取其資料以進行產品推廣，亦應給予顧客自主選擇權，「一定要明確告知顧客，商家收集顧客這些個人信息是出於什麼目的。除此之外，商家在顧客同意的情况下收集的個人資料，需要在達成目的後盡快銷毀這些信息，其實收集完的第二天就可以刪除。」



◆私隱專員公署提醒市民掃描二維碼時要留意有否被竄改。香港文匯報記者黃艾力 攝

黑客入侵個案年升逾倍

香港文匯報訊（記者 郭倩）黑客入侵盜取用戶個人資料是最普遍的個人私隱資料外洩情況。個人資料私隱專員公署昨日發表的工作報告指出，去年接獲的 157 宗資料外洩事故通報中，48 宗來自公營機構，109 宗則來自私營機構，較 2022 年的 105 宗大幅增近五成，當中涉及黑客入侵的資料外洩事故，由 2022 年的 29 宗，大幅增加逾一倍至去年 64

宗，佔去年資料外洩事故的 41%。遺失文件或便攜式裝置佔 27%，而經電郵、郵遞或傳真意外披露個人資料則佔 13%，其餘事故則包括僱員違規，以及系統錯誤設定等。

至於黑客入侵事件，當中以勒索軟體/黑客組織 Lockbit 佔最多，涉及 6 宗，涉及黑客組織 BlackCat 亦有 2 宗，其餘有入侵事件的黑客組織則包括 Aki-

ra、BianLian、C1oP、CUBA、eCh0ralx、Elbic、Faust、HIVE、Trigona，而數碼港遭黑客入侵事件，則是去年最大的外洩事故之一。

數碼港事件正撰寫調查報告

去年 8 月，數碼港電腦系統遭黑客組織 Trigona 入侵，盜取逾 400GB 資料。Trigona 將數碼港超過 400GB 數據放上暗網拍賣，底價 30 萬美元（約 234 萬港元），外洩資料包括一份人事相關的 Excel 文件，內有近 170 名數碼港員工及前員工資料，包括個人姓名、聯絡方式及信用卡資料等。

私隱專員鍾麗玲認為，去年出現大型外洩事故，亦導致接獲的資料外洩通報個案增加。對於數碼港資料外洩事故的調查進度，她表示已通知涉事單位盡快通知受影響人士，而私隱專員公署就數碼港個案已作出 4 次查詢，並獲得 3 次回覆，指出數碼港已委託網絡安全顧問公司撰寫獨立調查報告。

另外，私隱專員公署去年共接獲 15,914 宗公眾查詢個案，較 2022 年 14,929 宗上升 7%，當中收集及使用個人資料以 32% 佔最大類別。查詢中亦有 793 宗為有關套取市民個人資料用作詐騙用途，較 2022 年的 707 宗增加 12%。