Monitoring Compliance with Technology Challenges

監督循規　迎接科技挑戰

審查及政策部監察和推動資料使用者要循規以符合條例的規定。隨著資訊科技急速發展而衍生的私隱風險，我們特別鼓勵機構採取所有方法和手段，以保障個人資料，並尊重消費者和用家的私隱。

The Compliance and Policy Division monitors and promotes compliance with the provisions of the Ordinance. Due to the privacy risks brought about by the rapid advances in information and communication technology, we specially encourage organisations to apply all means to ensure personal data protection and respect consumer and user privacy.

2014年的流動應用程式抽查及跟進行動

本地流動應用程式開發商應改善其私隱政策透明度

公署於2014年5月抽查60款由本地機構開發的熱門流動應用程式（「程式」），結果顯示這些程式的《私隱政策聲明》透明度明顯不足，而與2013年同樣的抽查比較，亦無顯著改善。

2014年抽查結果

在抽查的程式中，少於一半程式提供《私隱政策聲明》。而且大部分的聲明都有不足之處，例如相關性低、難於閱讀及不易查閱。此外，大部分程式要求的讀取權限，相比於該程式的功能，調查員都認為超乎適度。

2014 MOBILE APP SURVEY AND FOLLOW-UP

Privacy Policy Transparency Needed in Local Mobile Applications

In May 2014, the PCPD conducted a survey of 60 popular mobile applications ("apps") developed by Hong Kong companies and found that their transparency in terms of privacy policy statements ("PPSs") was clearly inadequate, and there was no noticeable improvement compared with the results of a similar survey conducted in 2013.

2014 survey findings

Less than half of the apps assessed did not provide any form of PPS. Most of the PPSs that were provided were inadequate in terms of relevance, readability and accessibility. Furthermore, most of the apps seemed to have sought permissions for data access beyond what the testers expected based on the app's functionality.

	2014年的抽查（總共60個程式） 2014 Survey (total = 60 apps)	2013年的抽查（總共60個程式） 2013 Survey (total = 60 apps)
程式沒有提供《私隱政策聲明》 Apps that did not provide PPSs	27 (45%)	24 (40%)
《私隱政策聲明》不是為程式而編寫的 PPSs that were not tailored to apps	28/33 (85%)	33/36 (92%)
《私隱政策聲明》所用的語文與程式不同或不易查閱 PPSs that were written in a language different from the app or not easily accessible	2/33 (6%)	4/36 (11%)
沒有提供或不能確定聯絡資料（電郵、電話、地址等） Contact details (email, phone, address, etc.) not provided or ascertained	5 (8%)	24 (40%)
沒有說明會否讀取資料、哪些資料及為何讀取；　或者上述資訊並不清晰 Unclear or missing information as regards whether data would be accessed, and if so, what data and why	43 (72%)	**沒有抽查** Not surveyed
與程式的主要功能相比，要求的權限可能屬超乎用家的期望 Permission for data access beyond users' expectations based on the app's functionality	51 (85%)	**沒有抽查** Not surveyed

保障私隱的程式是可行的

雖然抽查結果發現私隱政策透明度強差人意，但公署認為「我的天文台」程式是值得參考的。該程式提供了易於理解及具體的《私隱政策聲明》。而且，Android版本讓用戶選擇容許或不容許該程式讀取位置資料。這例子正好證明開發到既受歡迎、又實用及保障私隱的程式是可行的。

Privacy-friendly apps viable

Despite the prevalence of disappointing privacy features, the PCPD was impressed by the app *MyObservatory*, as it featured an easily understandable and specific PPS. Furthermore, the Android version allowed users to allow or disallow location information to be read by the app. This demonstrates that it is possible to develop an app that is popular, functional and privacy-friendly.

私隱專員的評論

「流動裝置非常普及，已改變了商業運作及我們的生活模式。置載有很多生活上的個人私隱。只需按鍵下，手機儲存的私密資料（包括相片、曾過的地方、在電郵中表達的政見）可能已傳送到互聯網，甚至在網上永久保留。因此，保障消費者使用這些裝置所引起的私隱事宜非常重要，而流動程式開發商便是肩負這重要責任的其中一員。」

The Commissioner's Comments

"Mobile devices are ubiquitous and have transformed business operations and our lives. For many people, they hold the privacies of life. With just a few clicks, the intimate details held in phones – photos, past locations, political opinions expressed in emails – may be transmitted to, and forever preserved on, the Internet. Safeguarding privacy in the use of these devices is therefore imperative and one major player who must live up to this responsibility is the mobile app developer."

開發流動應用程式最佳行事方式指引

由於抽查結果顯示程式私隱政策欠缺透明度，公署於2014年11月發出《開發流動應用程式最佳行事方式指引》（「指引」），協助開發商研發保障私隱的應用程式。

Best practice guide for mobile app development

As a result of the survey revealing the lack of privacy transparency among apps, the PCPD published the "*Best Practice Guide for Mobile App Development*" ("the Guide") in November 2014 to assist mobile app developers in building privacy-friendly apps.

這份指引是特別為中小企業提供支援而編製的，因為他們可能沒有足夠的資源，自行就個人資料私隱保障制訂詳細的程式開發指引。這份指引就有關法律的規定，提供簡便易明的概覽；並介紹如何以貫徹私隱的概念開發程式。這份指引亦提供詳細的檢查清單，為程式開發商闡述設計保障私隱的程式時須考慮的所有因素；亦建議一系列的最佳行事方式，讓程式開發商藉保障私隱爭取從商優勢，透過贏取客戶的信任而增強競爭力。

The Guide is especially tailored for small-to-medium enterprises which may not have sufficient resources to establish their own comprehensive app-development guide. It provides an easy-to-understand overview of the legal requirements and the Privacy by Design approach in developing apps. Adopting a comprehensive checklist approach, it draws the attention of app developers to all the factors that need to be considered in building a privacy-friendly app. It also recommends a set of best practices that enable app developers to distinguish themselves from the crowd by gaining enhanced trust from end-users.

這份指引對程式開發商、委託他人開發程式的人士，以及向程式開發商提供附加功能代碼的人士（例如廣告網絡或分析工具提供者）均可適用。

The Guide should be read by app developers and those who commission their work, as well as those who provide codes for app developers for added features, including advertising networks and analytics tool providers.

Android的權限模式有缺陷

在上述的程式抽查中，公署發現Android程式可以被編寫至在未有作出權限聲明的情況下，讀取Android　4.3或之前版本的流動裝置的公共記憶體。

Privacy failure in Android's permission model

During the app survey, the PCPD discovered that it would be possible for an Android app to read the shared memory in a mobile device running on Android 4.3 or earlier versions without the need to make a prior permission declaration.

Android一直以來聲稱，程式要讀取的資料會在安裝程式前呈現在「權限」頁面[1]。然而，公署的測試揭示，程式有機會在毋須於權限頁面作有關聲明的情況下，仍可讀取Android裝置內的記憶體內容，包括相片、檔案及其他程式儲存在該記憶體的資料。雖然可以讀取公共記憶體的缺陷已在Android 4.4的裝置糾正，但可以讀取部分內部記憶體的情況，仍有可能於Android 4.4發生，故值得關注。再者，在發現這漏洞之時，有三分之二的Android用戶仍在使用Android 4.3或更舊的版本，當中很多裝置因缺乏製造商的支援而無法更新至Android 4.4。

Android had all along claimed that, prior to app installation, all intended access to data stored in an Android device would be fully disclosed on the Permission Page[1]. However, the PCPD's tests revealed that it would be possible to develop an app that read the memory of Android devices, including photos, files, and any data other apps choose to store in the devices, without the need to inform app users on the Permission Page. Although the flaw was corrected for Android 4.4 for access to the shared memory, it could still be a cause for grave concern, as partial access to the internal memory was still possible for Android 4.4. Furthermore, at the time that the flaw was discovered, two-thirds of Android users were still using devices running on earlier versions of the platform, and many of them would never be upgraded to Android 4.4 due to the lack of support from their manufacturers.

私隱專員的評論

「隨著科技應用融入在生活細節之內，消費者在日常生活提供的個人資料愈來愈多，而且往往是不知不覺的。所有負責收集及使用個人資料的持份者，必須加倍小心，負起保障消費者私隱的責任。這些持份者不單是指直接收集資料的機構（例如程式開發商及軟件公司），亦包括提供網絡服務或其他基本設施的公司，裝置或操作系統生產商。」

The Commissioner's Comments

"As technology evolves, consumers are giving up more and more of their personal data, often without even knowing it. It is increasingly incumbent upon all stakeholders responsible for the collection and use of personal data to take greater care and responsibility to safeguard the privacy of consumers. They include not only the organisations collecting data directly, such as app developers and software companies, but also the infrastructure companies and device or operating system manufacturers."

下表概括描述由公署開發的一個測試程式，在未有事先聲明的情況下，仍可讀取裝置的記憶體：

The table summarises the flaw uncovered by using a test app developed by the PCPD which does not declare its access to the device's memory:

裝置上的Android版本 Versions on devices	權限頁面有否顯示任何權限？ Permission shown under Permission Page	可否讀取公共記憶體儲存的相片、檔案及其他程式的資料？ Access to shared memory containing photos, files or other app data	可否讀取部分內部記憶體可能含有關於裝置的敏感資料？ Partial access to internal memory containing potentially sensitive data about the device
Android 4.3**或之前** Android 4.3 or earlier	**否** No	**可** Yes	**可** Yes
Android 4.4 Android 4.4	**否** No	**否** No	**可** Yes

1 developer.android.com/guide/topics/security/permissions.html

公署已聯絡Google，證實這缺陷的存在。公署於2014年11月27日要求Google採取補救措施，及／或警告受影響的用戶有關惡意程式可以在其不知情、甚至不允許的情況下，讀取資料而存在風險。

The PCPD contacted Google Inc. and confirmed the flaw. Google was requested on 27 November 2014 to take corrective action and/or warn the end-users concerned that they are subject to the risk of data access by malicious apps without their knowledge and permission.

讚賞 Compliment

私隱專員明言情況（香港流動應用程式私隱政策透明度不足）不理想，除了會調查投訴個案外，更會主動就懷疑有問題的程式作出調查和執法。這個取態和行動，值得公　支持。

The Commissioner stated clearly the situation (privacy policy transparency of apps in Hong Kong was inadequate) was far from ideal. In addition to investigating the complaint cases, the PCPD also initiated an investigation and took enforcement action against flawed apps. This proactive approach deserves public support.

頭條日報社評
Editorial, Headline Daily
(2014.12.16)

新入職員工 Newcomer

儘管私隱法例在香港已有接近二十年歷史，但今日它仍是發展最快的其中一個法律與政策範疇，尤其是因為數碼科技發展迅速，以及經互聯網轉移個人資料的智能小型裝置應用廣泛。因此，公署密切注意科技發展對私隱的影響，並與海外規管者保持緊密聯系，分享執法和政策發展的見解，實在非常重要。我的工作包括國際關係及政策研究，刺激又變化多端，經常帶來新挑戰。

Even though privacy law has been in place in Hong Kong for the better part of nearly 20 years, personal data privacy is today one of the fastest evolving legal and policy areas – not least because of the rapid advances in digital technology and explosion of smart gadgets that transfer personal data via the Internet. For these reasons, it is of paramount importance for the PCPD to keep tabs on the privacy impact of advancing technology, as well as to maintain an effective working relationship with overseas regulators in sharing insights on enforcement and policy developments. My new role in international relations and policy research is an exciting and highly dynamic one that constantly brings fresh challenges.

周鳴飛
助理個人資料主任（研究）
Michael CHAU
Assistant Personal Data Officer (Research)

諮詢工作

本年度，香港警務處就擬議實施的電子定額罰款通知書（「電子通知書」）徵詢公署的意見。

這個電子通知書解決方案包括電子手帳、手提打印機及支援網絡系統。警員在發出電子通知書時，只需在電子手帳輸入最少量的資料，例如車輛登記號碼及違例事項編號，便可即場列印電子通知書。推行電子通知書是提高前線人員工作效率及減少紙張的一個方法。

私隱專員讚賞這正面措施，回應了他於2014年10月24日發出的「警務處接連遺失載有個人資料的警隊文件」調查報告所作的建議。警務處當時曾承諾檢視有關儲存有個人資料的警務文件器材，以提升資料保安的程度。

由於公署所得的資料有限，因此公署重點提出一些整體意見及關注範疇，讓警方考慮。

公署建議警方在實施電子通知書之前，由獨立專業人士進行私隱影響評估。

公署亦建議警方就採取的技術措施，進行資訊科技保安風險評估。

警方亦可考慮向公署提供下列詳情：(a)當遺失電子手帳時，銷毀手帳內資料的「計時炸彈」措施；及(b)在資料保安、裝置保安、網絡/連接保安及應用保安上，電子通知書解決方案的保密和整體措施。

由於警方在打擊交通罪行的執法工作上，以新方式收集及處理個人資料，警方應檢討目前的職員培訓、指引及管理控制措施，以確保能查閱電子通知書解決方案的警務人員有良好操守、審慎態度及辦事能力。警方制定有清晰的政策及指引，以免過度收集個人資料，更要避免為交通罪行以外的目的而追蹤個人行蹤及匯集個人的活動資料。警方亦應評估個人資料的保留期限，尤其當要延長檢控期限時，應保留資料多久。

公署亦建議警方檢討目前的收集個人資料聲明及私隱政策聲明，以衡量是否需要為增加透明度而作出修訂。

CONSULTATION

During the year, the Hong Kong Police Force (the "Police") sought our views on the proposed implementation of Electronic Ticketing ("E-Ticketing") for Traffic Fixed Penalty Tickets.

The E-Ticketing solution comprises a personal digital assistant, a portable printer and a supporting network system. When issuing E-Tickets, ticketing officers would need only to key in a minimum amount of data in the personal digital assistant, such as vehicle registration mark and contravention code, before printing out an E-Ticket on the spot. E-Ticketing is identified as a way to enhance frontline officers' efficiency and to reduce their reliance on paper-based processes.

The PCPD appreciated the initiative as a positive step in response to the Commissioner's recommendation in the Investigation Report entitled "Hong Kong Police Force's Repeated Loss of Documents Containing Personal Data", dated 24 October 2013, that a review of equipment used for holding police documentation containing personal data be undertaken to enhance data security.

Given the limited information available to the PCPD, the PCPD highlighted general comments and areas of concern for the Police's consideration.

The PCPD advised the Police to undertake a Privacy Impact Assessment, which should be conducted by an independent professional party before implementing E-Ticketing.

The PCPD also recommended the Police conduct an Information Technology Security Risk Assessment in respect of the technical measures to be adopted.

The Police may also consider providing the PCPD with further details of: (a) a "time-bomb" measure for data destruction in the personal digital assistant in the event of device loss; and (b) measures on the confidentiality and integrity of the E-Ticketing solution in respect of data security, device security, network/connectivity security and application security.

Given the new approach to collecting and processing personal data for enforcement work against traffic offences, the Police should review the existing measures for staff training, guidance and management control to ensure the integrity, prudence and competence of police officers who have access to the E-Ticketing solution. A clear policy and guidelines should be set up to avoid the excessive collection of personal data, and to prevent movement tracking and information compilation of the activity profile of individuals for purposes other than those related to traffic offences. The retention period of the personal data collected should also be evaluated as and when required by the Police, for example, in the event of an extension of the time bar for prosecution.

The PCPD also suggested that the Police should review its existing personal information collection statement and privacy policy statement to determine whether amendments are required for the purpose of transparency.

處理查詢

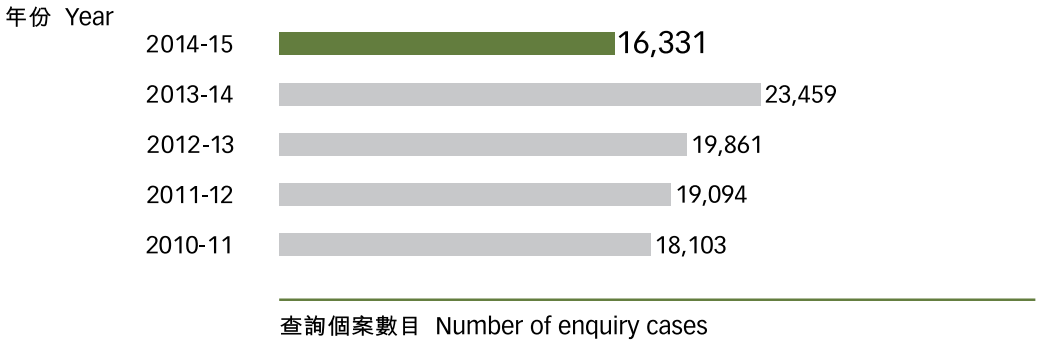
公署在本年度共處理16,331宗查詢個案，比上年度減少30%；平均每個工作天處理66宗查詢（圖2.1）。

HANDLING ENQUIRIES

A total of 16,331 enquiry cases were handled during the year, down 30% from that of the previous year. On average, 66 enquiry cases were handled per working day (Figure 2.1).

圖2.1：全年查詢個案

Figure 2.1: Annual enquiry caseload



讚賞 Compliment

非常感謝個人資料主任簡玉華的迅速回應，並提供了詳細資料，其中有不少值得探討和研究的論點，非常有用。

Thank you very much for your (Ms Loreen KAN, Personal Data Officer) quick and informative response. Even from the first brief look at your answers, I can see that there are a number of interesting points that will be very useful for our comparative overview.

Mr ILYUK
RESPECT ("Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies") research project

感言 Response

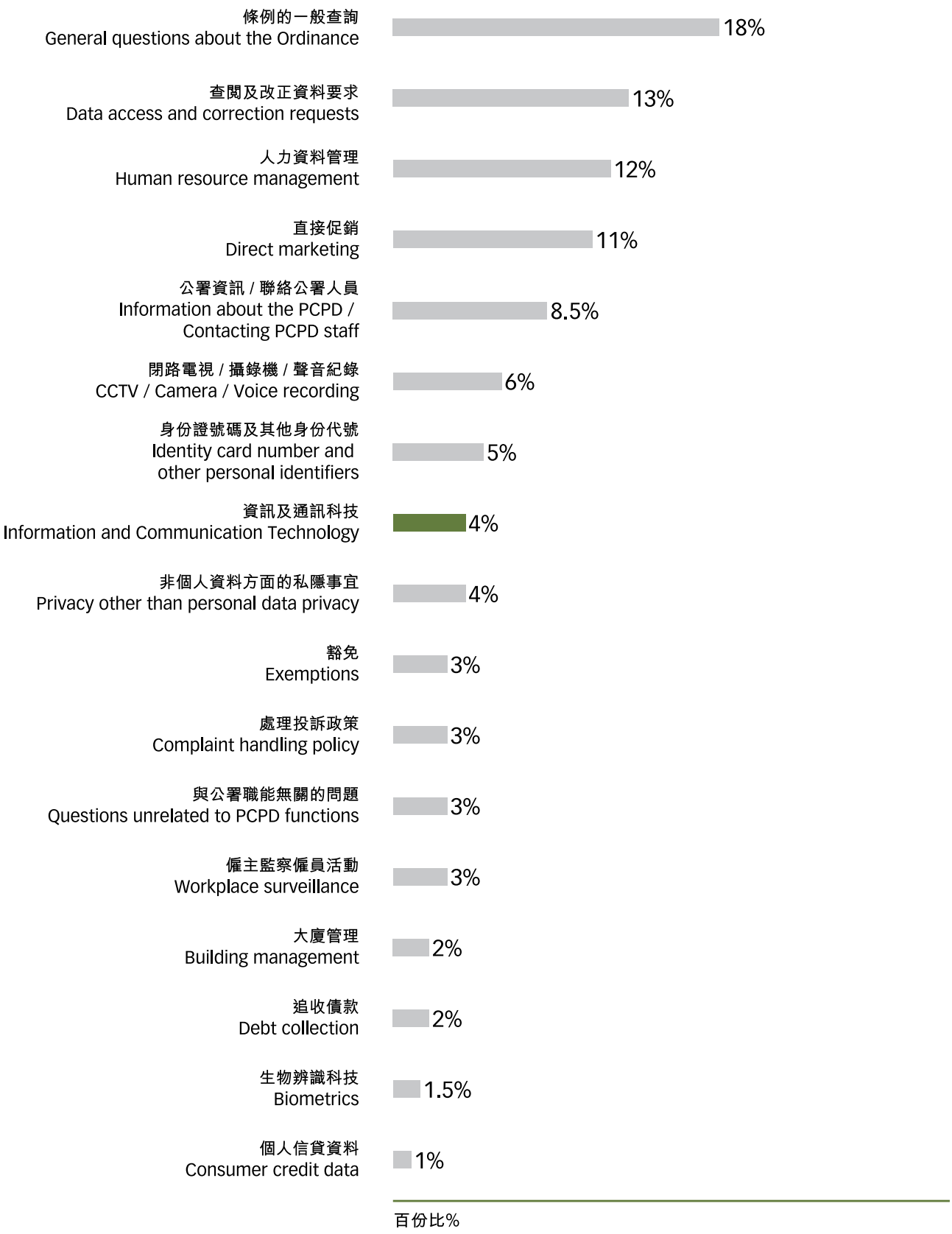
在收到研究項目RESPECT（該項目獲歐洲委員會支持，研究國家資料保障機構在官方監視中如何保障核心私隱利益）的一項查詢後，我們認為有責任提供資料，因這可能影響環球私隱保障的發展。在上司的支援下，我能夠於公署承諾的一半時間內回覆了這個查詢，並獲得負責這個項目的教授讚許，十分高興。

On receiving an enquiry from the research project RESPECT, which is supported by the European Commission to study the role of national data protection authorities in safeguarding core privacy interests from official surveillance, we felt duty bound to provide useful information which might have an impact on the development of privacy protection on a global platform. With the support of my superiors, I was able to answer their enquiries in half the time pledged by the Office and was delighted to receive a compliment from the professor in charge of the project.

簡玉華
個人資料主任
Ms Loreen KAN
Personal Data Officer

圖2.2：查詢個案的性質

Figure 2.2: Nature of enquiry cases

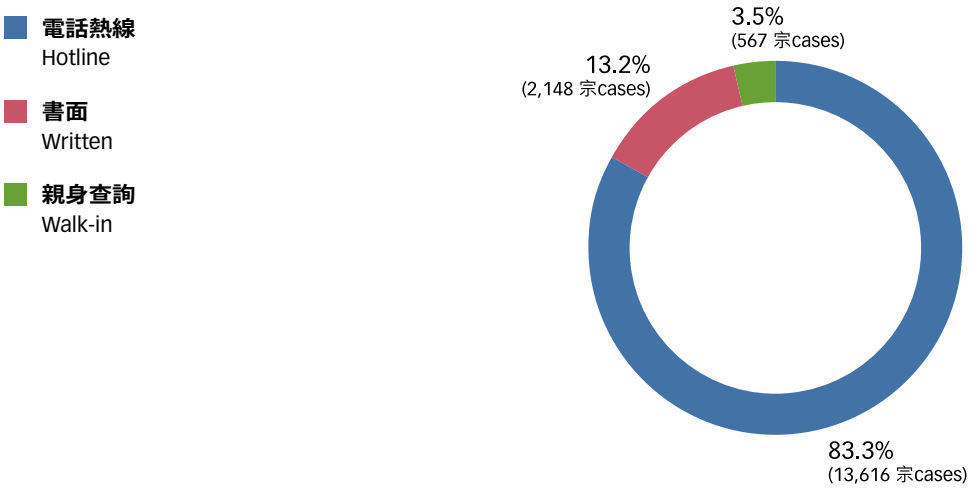


大部分（83.3%）查詢經由公署的電話熱線（2827 2827）提出（圖2.3）。

The majority of the enquiries (83.3%) were made via the PCPD hotline (2827 2827) (Figure 2.3).

圖2.3：提出查詢的途徑

Figure 2.3: Means by which enquiries were made



新入職員工 Newcomer

我的職責主要是為公眾人士解答與條例有關的問題，為他們提供建議，讓他們更了解條例的規定和保障。雖然我入職時間尚短，在審查及政策部可以處理不同類型的電話和書面查詢，很感謝公署及同事給我學習的機會。

My duty is to answer enquiries from the public and explain the provisions of the Ordinance. I am relatively a new member of the team. I feel truly grateful for the opportunity to learn from my colleagues in the Compliance and Policy Division that I can deal with a wide range of telephone and written enquiries.

陳溢珍
審查及政策部行政助理
Jenny CHAN
Administrative Assistant, Compliance & Policy Division

循規審查

當某機構的行事方式與條例規定看來有不相符時，私隱專員會展開循規審查。在完成循規審查行動後，私隱專員會書面告知有關機構，指出與條例規定不符或不足之處，並促請有關機構採取適當的補救措施糾正可能違規的情況，以防止類似情況再發生。

在本年度，私隱專員共進行了227次循規審查行動。74%的循規審查對象為私營機構，其餘26%則關乎公營機構，包括政府部門、法定機構、非政府機構及政府資助教育機構。

下文重點介紹在年內進行的部分循規審查行動。

在網誌張貼客戶的個人資料

一間銀行向公署通報，該銀行位於廣州的外判電話中心，其一名前僱員在一個中文網誌張貼了三名客戶（全是香港知名人士）的個人資料，包括姓名、香港身份證號碼、出生日期、辦公和住宅地址、電話號碼及電郵地址。

該銀行在回應公署的查詢時解釋，該名負責客戶關係及電話促銷信用卡產品的前僱員，把有關資料抄寫在紙上，回家輸入電腦後上載至該網誌。該電話中心已發信要求該網誌的營運者永久刪除該網誌訊息。有關資料已被移除。

該銀行採取了下述補救行動，防止日後再發生類似事件：

(1) 在電話中心實施無紙化的工作環境；
(2) 禁止在電話中心使用智能電話及攝影機，並規定所有職員在進入電話中心前把私人物品鎖在櫃內；
(3) 把巡邏電話中心的次數增加一倍；
(4) 每星期由主管進行審計追蹤及系統查閱的抽查；及
(5) 規定電話中心所有職員完成資訊保安的網上學習課程。

COMPLIANCE CHECKS

The Commissioner conducts compliance checks of practices that appear to be inconsistent with the requirements of the Ordinance. Upon completion of a compliance check, the Commissioner alerts the organisation in writing, pointing out any apparent inconsistencies or deficiencies, and advising the organisation, if necessary, to take remedial action to correct any suspected breaches and prevent any further breaches.

During the year, the Commissioner carried out 227 compliance checks. Of these, 74% were conducted on private sector organisations, while the remaining 26% were on public sector organisations, including government departments, statutory bodies, non-government organisations and government-funded educational institutions.

Below are highlights of some of the compliance checks conducted during the year.

Customers' Personal Data Posted on a Blog

A bank reported to the PCPD that the personal data, including name, Hong Kong Identity Card number, date of birth, office and residential address, telephone number and email address, of three of its customers (all Hong Kong celebrities) was posted on a Chinese blog by an ex-employee of the bank's contracted call centre in Guangzhou, China.

In response to the PCPD's enquiries, the bank explained that the ex-employee, who had been responsible for maintaining customer relationships and offering credit card products by making outbound calls, had accessed the data concerned, written it on paper, recorded it on his computer at home and uploaded it to the blog. The call centre issued a letter to the platform operator of the blog to request the permanent deletion of the concerned blog message and the data was taken down.

The bank took the following remedial action to prevent a recurrence of the problem:

(1) Implementing a paper-free operating environment in the call centre;
(2) Prohibiting the use of smartphones and cameras in the call centre and requiring all staff to leave their personal belongings in lockable pedestals before entering the call centre;
(3) Doubling the patrols in the call centre;
(4) Implementing weekly audit trails and system-access spot-checks by supervisors; and
(5) Requiring all staff of the call centre to complete an Information Security e-learning course.

載有15,747名人士個人資料的伺服器遭黑客入侵

一間大學向公署通報，某學院兩個連接網絡的儲存伺服器遭黑客入侵，導致載有15,547名病人及200名學生及／或職員個人資料的檔案被惡意加密，該大學被勒索比特幣以換取解密鑰匙。涉及的個人資料包括受影響人士的姓名、身份證號碼、出生日期、電話號碼、地址、化學測試資料及檢查結果。

該大學在回應公署的查詢時確認，事件是由於伺服器欠缺適當的保安修補程式，讓黑客有機可乘，利用勒索軟件在使用舊版作業系統的伺服器找出保安漏洞。不過，該大學表示，沒有證據顯示伺服器所載的個人資料外洩。

該大學因應事件採取了下述補救行動，防止日後再發生類似事件：

(1) 按大學的伺服器保障指引，協助該學院安裝新的伺服器；

(2) 定期維修新的伺服器，包括定期檢查和更新系統及修補管理，為儲存的資料提供最大保障；

(3) 找出該學院未做防護的檔案伺服器（如有），以防火牆保護；

(4) 按ISO/IEC 27001標準，檢討部門的資訊保安，以評估現行資訊系統及基建的潛在風險，並建議（如有）適當的跟進行動，以減低對該學院的風險；及

(5) 透過電郵及定期會議，提升部門資訊科技職員的資料保安的意識。

Servers Containing Personal Data of 15,747 Individuals Hacked

A university reported to the PCPD that two network-attached storage servers of a faculty had been hacked and, as a result, files containing personal data of approximately 15,547 patients and 200 students and/or staff members stored in the servers had been maliciously encrypted by a hacker, who subsequently attempted to blackmail the university for bitcoins in exchange for the decryption key. The personal data involved in the incident included the names, Hong Kong Identity Card numbers, date of birth, telephone number, address, clinical data and laboratory test data of the affected people.

In response to the PCPD's enquiries, the university confirmed that the incident had been caused by lack of proper security patches on the servers, which allowed the hacker to use ransomware to exploit the security vulnerabilities of some servers running older versions of the operating system. However, the university advised that there was no evidence that personal data contained in the servers had been leaked.

The university subsequently took the following remedial action to prevent recurrence of the incident:

(1) Assisting the faculty to set up a new server following the university's guidelines on server protection;

(2) Performing regular maintenance on the new server, including regular checks for system updates and patch management so as to provide maximum protection for the data stored in the servers;

(3) Identifying unprotected file servers used by the faculty, if any, and protecting them behind its firewall;

(4) Conducting a departmental information security review that adheres to ISO/IEC 27001 standards, to assess the potential risks of the existing information systems and infrastructure and to recommend, if any, appropriate follow-up action to mitigate risks within the faculty; and

(5) Reinforcing awareness of its departmental IT staff members of data security through emails and regular meetings.

資料經電郵外洩 涉及3,300名大學申請人

一間大學向公署通報，一名職員把入學活動的邀請電郵發給3,300名大學聯合招生辦法（「大學聯招」）申請人時，發生錯誤。錯誤起因是該職員進行郵件合併時出現人為錯誤，把個別申請人的電郵地址，錯配上另一位申請人的姓名及大學聯招申請編號。涉及的個人資料包括申請人的姓名及大學聯招申請編號。

該大學在事發後立即通知所有受影響的申請人，並要求並非收件人的大學聯招申請人刪除該電郵，不要向他人披露有關個人資料。

該大學在回應公署的查詢時表示，已採取下述補救行動，防止日後再發生類似事件：

(1) 制定個人資料管理及保安的新指引，規定職員(i)將資料輸入資料庫時，進行兩輪反複核對；及(ii)發出任何信件或電郵訊息前，進行兩輪反複核對；

(2) 設計資料保障的循規檢查清單，以供部門的資料保安及私隱人員使用；

(3) 除非有絕對需要發出個人化信件，否則一般大量郵件或電郵不應顯示個人資料；及

(4) 規定所有負責處理個人資料的職員，每年必須出席資料保障講座。

Data Leakage via Email Involving 3,300 Applicants for a University

A university informed the PCPD that a staff member had mistakenly sent an invitation email for admission activities to 3,300 Joint University Programme Admissions System ("JUPAS") applicants. The mistake was due to human error in conducting a mail merge, which caused a mismatch in the applicants' email addresses with their names and JUPAS application numbers. The personal data involved in the incident included the names and JUPAS application numbers of the applicants.

Immediately after the incident, the university notified all affected applicants and requested the applicants to delete the email and not to disclose the personal data to anyone.

In response to the PCPD's enquiries, the university reported that it had taken the following remedial action to prevent similar incidents:

(1) Establishing new guidelines on the management and security of personal data, which required staff to: (i) conduct two rounds of cross-checking for raw data entry into the database; and (ii) conduct two rounds of cross-checking before sending out any letters or email messages;

(2) Designing a compliance checklist on data protection for departmental data security and privacy officers to use;

(3) Sending general mass mails or emails with no personal data shown instead of personalised correspondence, unless absolutely necessary; and

(4) Providing annual talks on data protection for all staff responsible for handling personal data, to be attended on a mandatory basis.

主動調查

香港航空旅遊有限公司不慎使用流動應用程式「俠客行・旅行」外洩個人資料

俠客行由香港航空旅遊有限公司擁有，是一個提供在線服務的流動應用程式，包括預訂及購買機票、航程管理，及為旅客提供社交網絡平台。會員及非會員均可透過俠客行進行交易。

非會員首次使用預訂服務時，須輸入乘客的個人資料及聯絡人的個人資料。當再次進行交易時，非會員即可以其流動裝置的MAC位址[1]確認其身份。

2013年9月18日，蘋果公司推出新的流動操作系統iOS7。以保護私隱為由，iOS7阻止所有應用程式讀取MAC位址作為識別流動裝置的持有人。在回應應用程式要求讀取MAC位址時，iOS7會向程式提供相同的虛假數字。然而，俠客行的保養承辦商沒有就該改動作出任何相應的糾正，於2013年9月19日起，每當非會員在iOS7版本的流動裝置進行交易時，iOS7均會以相同的虛假MAC位址回應，所有交易均因此被視為由同一個人作出。當非會員以運行iOS7版本的流動裝置預訂機票或查詢訂購紀錄時，俠客行在裝置的螢幕上不單顯示他的紀錄，還會顯示其他非會員的個人資料。直至事件於2013年9月25日被揭發為止，共有六名顧客的個人資料因這方式而外洩予其他非會員。

私隱專員於2014年12月15日就此事發表調查報告，指出俠客行的保養承辦商並無就iOS7推出新增保障私隱的功能（阻止程式讀取MAC位址作為識別流動裝置）而及時地作出相應行動，以致香港航空旅遊有限公司外洩顧客的個人資料。

私隱專員的決定

俠客行的保養承辦商向公署提出不知情的解釋，私隱專員並不接受。即使俠客行的保養承辦商宣稱在2013年9月才登記參與iOS開發商計劃，而之前從未收過蘋果公司的電郵通知，但作為專門從事程式開發的科技公司，它應緊貼蘋果公司的消息及最新科技資訊。再者，保養承辦商最後亦承認

1 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。

PCPD-INITIATED INVESTIGATIONS

Personal Data Leaked through the Inadvertent Use of Mobile App "TravelBud" by HKA Holidays Limited

"TravelBud", owned by HKA Holidays Limited, was a mobile application providing online services for mobile device users, including flight ticket reservations and purchase, flight itinerary management, and a social networking platform for travellers. It supported transactions made by both registered members and non-member customers.

When making reservations for the first time, non-member customers had to input the personal data of the passenger and a contact person. For subsequent transactions, non-member customers were recognised by the MAC address[1] of the mobile device they used.

On 18 September 2013, Apple Inc. launched a new mobile operating system, iOS 7, which, for privacy protection, blocked apps from reading the MAC address as a mobile device identifier. In response to an app asking for the MAC address of a particular mobile device, iOS 7 provided the same fictitious number for all app requests. However, TravelBud's maintenance contractor failed to take any corrective action in response to this change of MAC address behaviour, so all non-member customers making transactions with devices using iOS 7 from 19 September 2013 onwards were identified by the same fictitious MAC address, as if they were all the same person. As a result, when a non-member customer sought to reserve a flight or order a history enquiry on a mobile device using iOS 7, TravelBud would show on the screen of the mobile device not only his records and personal data, but also those of other non-member customers who had made transactions through TravelBud on devices using iOS 7. The personal data of six non-member customers was leaked in this way before the incident was identified on 25 September 2013.

On 15 December 2014, the Commissioner published an investigation report on the leakage of the personal data of customers of HKA Holidays Limited through TravelBud, which concluded that TravelBud's maintenance contractor had failed to respond to the new privacy protection feature of iOS 7 that blocked apps from reading by the MAC address as a device identifier.

The Commissioner's determination

TravelBud's maintenance contractor pleaded ignorance of the change in MAC address behaviour, but this was rejected by the Commissioner. As a technology company specialising in app development, TravelBud's maintenance contractor should have kept abreast of the news and technology updates from Apple Inc., even though it did not register with the iOS Developer Program until September 2013 and would not have received the relevant email

1 A media access control address ("MAC address") is a unique identifier assigned to network interfaces for communications on the physical network segment. It is a 48-bit hexadecimal number most often assigned by the manufacturer of a network interface and exists on all mobile computing devices with network connectivity.

他在2013年9月11日知悉有關更新，這距離iOS7於2013年9月18日正式推出尚有一個星期時間，保養承辦商理應有足夠時間採取行動，防止資料外洩。

notifications from Apple Inc. before that date. Furthermore, as the maintenance contractor admitted that it learnt of the update on 11 September 2013 finally but iOS 7 was not launched until 18 September 2013, there was still time for the maintenance contractor to prevent the data breach.

由於俠客行的保養承辦商在事件中只是港航旅遊的外判代理，亦未有受託付處理顧客的個人資料，所以私隱專員認為該保養承辦商不屬條例下的資料使用者。

As TravelBud's maintenance contractor was only an outsourced agent of HKA Holidays and was not entrusted with any personal data of the latter's customers for processing, the Commissioner concluded that it was not a data user as defined in the Ordinance.

然而，根據條例第65(2)條，港航旅遊作為該保養承辦商的主事人，須為該保養承辦商的錯失負責。港航旅遊沒有採取所有合理地切實可行的步驟，確保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。

The Commissioner also held that HKA Holidays, as the principal of the maintenance contractor, was responsible for the latter's misdeed by virtue of section 65(2) of the Ordinance. It contravened DPP4(1) for failing to take all reasonably practicable steps to ensure that the personal data handled through TravelBud was protected against unauthorised or accidental access.

補救行動

非會員透過俠客行預訂及購買機票時，港航旅遊不再以MAC　位址作為識別流動裝置的持有人。由於在事件後，俠客行的法律擁有權已轉移予一間內地公司，私隱專員未有向港航旅遊送達執行通知。不過，私隱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，私隱專員會採取執法行動。

Remedial action

HKA Holidays stopped using the MAC address as the identifier of mobile devices for non-member customers who reserved and purchased flight tickets through TravelBud. As HKA Holidays sold TravelBud to a Mainland company after the incident, no enforcement notice was served on HKA Holidays. Instead, the Commissioner warned HKA Holidays that enforcement action would be taken should it fail to observe the relevant requirements of the Ordinance in similar situations in the future.

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_6453_c.pdf

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports files/R14_6453_e.pdf

翱翔旅遊的流動應用程式：未有提供私隱政策並收集過度個人資料

私隱專員於2014年12月15日發表一份調查報告，指翱翔旅遊有限公司(「翱翔遊」)在顧客(i)參加客戶獎賞計劃「翱翔天地」(「該計劃」)及(ii)於流動應用程式(「該程式」)查詢該計劃的積分時，收集過量的個人資料。該程式由縱橫旅遊有限公司(「縱橫遊」)開發及由翱翔遊營運。翱翔遊和縱橫遊兩間公司均沒有透過私隱政策、應用程式供應平台上的　述或其他溝通渠道，向該程式的用戶解釋收集資料的用途。兩間公司均違反保障資料第1原則。

縱橫遊是一間批發旅遊產品的本地旅行社，翱翔遊是縱橫遊的指定銷售代理。該計劃是由翱翔遊獨自管理。顧客購買旅遊產品後，可以加入成為該計劃會員，之後再惠顧便可賺取積分，積分可以在將來消費時兌換成折扣優惠。顧客填寫申請表格時要提供姓名、性別、出生日期、香港身份證號碼、住址、電郵地址、流動及住宅電話號碼。申請經接受後，顧客會獲發一個會員編號。

在三萬名登記會員中，約二千人沒有提供出生日期，三千人沒有提供身份證號碼，但申請仍然被翱翔遊接納。

會員要查詢積分餘額，可親身前往翱翔遊分行、致電客戶服務熱線或在流動裝置使用該程式。如使用該程式的話，會員須輸入英文姓名、出生日期及香港身份證號碼。

私隱專員的決定
過度收集個人資料
私隱專員接納該計劃在會員申請入會時，可收集上述的個人資料，惟不應收集相對比較敏感的出生日期及香港身份證號碼。

翱翔遊宣稱收集這些資料是為會員查詢其帳戶資料、查詢／換取積分時核實其身份。不過，從翱翔遊的實際運作反映，其他私隱敏感度較低的個人資料已達至同一目的。例如，在親身及致電熱線查詢時，會員只須提供會員編號或姓名、電郵地址及／或流動電話號碼，便足以辨識其身份。更重要的是，即使申請人在申請表上沒有提供出生日期或香港身份證號碼，翱翔遊其實仍會接受其申請。因此，收集出生日期及香港身份證號碼是不必要及過量的。

Excessive Collection of Personal Data through a Mobile App by Worldwide Package Travel Service Limited Operating with a No Privacy Policy

On 15 December 2014, the Commissioner published an investigation report concerning the excessive collection of personal data by Worldwide Package Travel Service Limited from customers when they enrolled in the company's loyalty programme and when making online enquiries about the reward points under the programme using the mobile app developed by Package Tours (Hong Kong) Limited and operated by Worldwide Travel. Neither Worldwide Travel nor Package Tours explained to app users through a privacy policy, app marketplace description or other communication means the purpose of use of their personal data they collected. The two companies therefore contravened DPP1.

Package Tours is a local travel agent providing wholesale travel products, and Worldwide Travel is its designated sales agent. The loyalty programme is exclusively administered by Worldwide Travel. After purchasing the company's travel products, customers can join the programme and earn reward points, which can be redeemed as discounts for future purchases. When completing the programme application form, the customers supply their name, gender, date of birth, Hong Kong Identity ("HKID") Card Number, home address, email address, and mobile and home telephone numbers. Upon enrolment, they are assigned a membership number.

There were about 30,000 registered members under the loyalty programme. Of these, around 2,000 members did not provide their date of birth, and around 3,000 members did not provide their HKID Card Number, but Worldwide Travel still accepted their applications.

Members can check their reward points balance by visiting Worldwide Travel branches in person, through its customer service hotline, or by using an app on a mobile device. When using the app, they have to input their English name, date of birth and HKID Card Number.

The Commissioner's determination
Excessive collection of personal data
The Commissioner concluded that Worldwide's collection of its customers' personal data for loyalty programme enrolment was acceptable, except for the relatively more sensitive data of date of birth and HKID Card Number.

The company alleged that these two data items were required to identify the customers when they enquired about their account details, or checked or redeemed reward points. However, the company's actual practice indicated clearly that other less sensitive personal data in the company's possession served the same purpose. For example, for in-person and hotline enquiries, customers were required to identify themselves only by providing their membership number or name, email address and/or mobile number. Importantly, the company accepted member enrolment even if the date of birth or HKID Card Number was missing on the application form. Accordingly, the collection of date of birth and HKID Card Number was unnecessary and excessive.

同樣地，在該程式處理網上積分查詢時，要收集顧客的出生日期及香港身份證號碼作為先決條件，也是不必要及過量的。顧客在查詢一些相對不太重要的事宜時，理應可以提供其他私隱敏感度較低的個人資料（如會員編號、姓名及／或聯絡資料）來核實其身份。

Similarly, the collection of date of birth and HKID Card Number as a requirement for online enquiries about reward points using the app was unnecessary and excessive. These enquiries were relatively inconsequential matters, and it should have been possible for customers making the enquiries to identify themselves by providing less sensitive personal data, such as their membership number, their name, and/or their contact information.

私隱政策欠奉
翱翔遊及縱橫遊在管理旅遊產品的銷售時，共用同一個資料庫及電腦系統。翱翔遊負責接收和確認流動裝置經該程式發送的網上訂單，縱橫遊則負責向航空公司購買機票及團體旅遊保險。就「網上訂購」功能而言，兩者均控制會員個人資料的收集、持有、處理及使用，所以在條例下被視為聯合資料使用者。

No privacy policy
Worldwide Travel and Package Tours share the same database and computer system for managing the sale of their travel products. Worldwide Travel is responsible for receiving and acknowledging online purchase orders made through mobile devices via the app, and Package Tours is responsible for issuing flight tickets and handling purchases of group travel insurance. They both control the collection, holding, processing and use of customers' personal data for the online purchases and are regarded as joint data users under the Ordinance.

根據保障資料第1(3)(b)原則，資料使用者須採取所有切實可行的步驟，以確保在收集個人資料之時或之前，資料當事人獲明確告知該資料會用於甚麼目的，及該資料可能轉移予甚麼類別的人。此外，在首次使用資料前，資料當事人應獲告知他有權要求查閱和改正資料，以及處理這些要求的人士的姓名或職銜及地址。

Pursuant to DPP1(3)(b), a data user is obliged to take all practicable steps to ensure that on or before collection of the data, the data subject is explicitly informed of the purpose for which the data is to be collected and the classes of persons to whom the data may be transferred. In addition, before the first use of the data, the data subjects must be informed of their right to request access to and correction of the data and the name or job title, and address of the individual who is to handle any such requests.

兩間公司都沒有遵從這項規定，因為他們在該程式的「網上訂購」功能沒有提供這些資訊。另外，翱翔遊作為該程式中的「積分查詢」功能的獨立資料使用者，同樣沒有提供相關資訊。

The two companies failed to comply with this requirement as they did not provide any such information in relation to the use of the app by customers making online purchases. Worldwide Travel also failed to provide such information in relation to the use of the app by customers making enquiries about reward points.

執法行動
私隱專員已向翱翔遊送達執行通知，指令他採取一系列的改善措施，包括(i)停止向該計劃的申請人及透過該程式的「積分查詢」功能，向顧客收集出生日期及香港身份證號碼；(ii)完全刪除在該計劃所收集的出生日期及香港身份證號碼；及(iii)根據保障資料第1(3)(b)原則的規定，聯同縱橫遊在該程式提供《收集個人資料聲明》述明資料的使用目的。

Enforcement action
The Commissioner served an enforcement notice on Worldwide Travel directing it to, among other things: (i) stop collecting the date of birth and HKID Card Number from customers when they enrol in the loyalty programme or when they use the app to make online enquiries about the programme's reward points; (ii) delete from the programme the date of birth and HKID Card Number collected in the past; and (iii) jointly with Package Tours, provide a Personal Information Collection Statement in relation to the use of the app as prescribed in DPP1(3)(b).

私隱專員亦向縱橫遊送達執行通知，指令縱橫遊要根據保障資料第1(3)(b)原則的規定，聯同翱翔遊在該程式提供《收集個人資料聲明》。

He also served an enforcement notice on Package Tours to provide, jointly with Worldwide Travel, a Personal Information Collection Statement in relation to the use of the app as prescribed under DPP1(3)(b).

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_9945_c.pdf

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_9945_e.pdf

私隱專員譴責69則匿名招聘廣告不公平收集求職者的個人資料

公署發現機構沒有披露其身份而刊登69則匿名招聘廣告（即「匿名廣告」），並以不公平方式收集求職者的個人資料。

過去五年，公署共接獲550宗有關匿名廣告的查詢。雖然公署曾向刊登匿名廣告的機構進行循規審查及發出勸喻信，但違規行為並無減少。公署於2014年3月15至22日期間審視七個主要廣告平台，發現以匿名方式刊登招聘廣告，依然常見。

私隱專員的決定

在隨機抽出進行調查的71則匿名廣告中，69則被發現違反保障資料第1(2)原則的規定（該原則規定個人資料必須以合法及公平的方式收集）。餘下2宗個案則沒有違反保障資料第1原則，因為私隱專員接納有關公司的解釋，即是招聘廣告中看來像是縮寫的公司名稱，實際上是有關公司日常營運時使用的正式名稱。

執法行動

私隱專員已向涉及匿名廣告的69個刊登廣告者發出執行通知，指令機構刪除已收集的個人資料，除非是必須為符合其他法律規定而保留資料，或為了繼續進行招聘程序；在這情況下，求職者須獲告知其資料會被保留，而他們亦有權要求刪除其個人資料。

六個主要招聘媒體，包括求職廣場(JobMarket)，Recruit，招職(JiuJik)，Classified Post，JobsDB及Career Times，已承諾會打擊匿名廣告。這些招聘媒體應

The Commissioner Condemned 69 Blind Recruitment Advertisements for the Unfair Collection of Job Applicants' Personal Data

A number of organisations were found in breach of DPP1(2) of the Ordinance for placing 69 job advertisements without disclosing their identities ("Blind Ads"), thus soliciting job applicants' personal data in an unfair manner.

The PCPD received 550 enquiries in relation to Blind Ads over the previous five years. Compliance checks were conducted and advisory letters were issued to the organisations placing the Blind Ads but the malpractice continued unabated. A survey conducted from 15 to 22 March 2014 in respect of seven major advertising platforms revealed that Blind Ads were preponderant.

The Commissioner's determination

Of 71 Blind Ads selected on a random basis for investigation, 69 were found to be in breach of DPP1(2) of the Ordinance, which requires that personal data be collected in a lawful and fair manner. In the remaining two cases, there was no contravention of DPP1, as the Commissioner accepted the company's explanation that what appeared to be an abbreviation of the company's name in a recruitment advertisement was in fact the company's trade name used in its day-to-day business operations.

Enforcement action

The advertisers involved in the 69 Blind Ads were issued an enforcement notice directing them to delete the personal data collected, unless it had to be retained to satisfy certain legal requirements, or for a continuing recruitment process, in which case the job seekers had to be informed and given the option of having their personal data deleted.

Six recruitment media, namely JobMarket, Recruit, JiuJik, Classified Post, JobsDB and Career Times, pledged to fight Blind Ads, heeding the Commissioner's advice to act as gatekeepers to prevent the unfair collection of job seekers' personal data through such ads.

私隱專員的勸籲，承諾會做好把關工作，防止有人透過匿名廣告不公平收集個人資料。它們積極打擊匿名廣告的做法包括：

(1) 篩選接到的廣告，如有需要，會要求刊登廣告者作出改正；

(2) 設立提示訊息及告示，以教育刊登廣告者及求職者，及

(3) 要求刊登廣告者提供商業登記證副本。

The proactive steps they are taking to combat Blind Ads include the following:

(1) Screening the ads and seeking advertisers' rectification where necessary;

(2) Setting up alert messages and notices to educate advertisers and job applicants; and

(3) Requiring advertisers to provide a copy of their business registration certificate.

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R14_9945_c.pdf

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R14_6242_e.pdf

視察行動

INSPECTION

公署根據條例第36條，在2014年3月至7月期間視察勞工處就業服務的個人資料系統。

The PCPD inspected the personal data system of the Labour Department's employment services, pursuant to section 36 of the Ordinance, between March and July 2014.

勞工處提供全面的就業服務，於2011至2013年期間，每年的登記求職者及就業轉介數目，平均分別有96,000人及172,000宗。勞工處為提供上述服務，所收集、持有、處理及使用求職者的個人資料類別相當多，包括姓名、香港身份證號碼、聯絡資料、教育背景、工作經驗及技能等。

The Labour Department provides comprehensive employment services. From 2011 to 2013, it handled an annual average of 96,000 registered job seekers and 172,000 job referrals. In providing these services, the Labour Department collects, holds, processes and uses a wide range of personal data of the job seekers, including name, Hong Kong Identity Card number, contact details, education background, work experience, skills, etc.

公署知悉勞工處實行多項的資料保障措施，均符合最佳行事方式，甚至高於法例的要求。

The Labour Department has a number of data protection measures in place which amount to best practices over and above the legal requirements.

不過，私隱專員也提出14項勞工處可以優化現時個人資料系統的建議，並促請勞工處尤其注意下列五項：

The Commissioner made 14 recommendations for improving the existing personal data system. In particular, the following five recommendations called for the Labour Department's prompt attention:

(a) 從僱主收集求職者的資料：在面試完成後，勞工處會向僱主收集面試結果、已聘職位、僱用日期及薪金資料，但勞工處並沒有清晰地告知求職者會從僱主收集個人資料的種類，以及收集該些資料的目的。私隱專員建議勞工處糾正這做法。

(a) Collection of job seekers' data from employers: After job interviews, the Labour Department collected from the prospective employers the interview results, position filled, date of employment and salary offered, without clearly informing the job seekers of the types of personal data that would be collected from the employer and the purpose of collecting the data. The Commissioner recommended that the Labour Department rectify this communication gap.

(b) 如期銷毀資料：根據勞工處的內部指引，求職者的登記表格會在完成資料輸入後兩年銷毀，但實地視察仍發現有2008年的登記表格未被銷毀。私隱專員建議勞工處引入管控機制，確保載有個人資料的表格如期銷毀。

(b) Destruction of data according to schedule: According to the Labour Department's internal guidelines, the registration forms of job seekers must be destroyed two years after data input, but registration forms dating back in 2008 were found during the site inspection. The Commissioner recommended introducing management controls to ensure the destruction of forms containing personal data according to the schedule.

(c) 僱主應披露身份，才要求求職者提供履歷：勞工處可能會要求求職者直接把履歷發送給準僱主。雖然勞工處會向求職者披露準僱主的身份及聯絡方法，但有關披露僱主身份的做法，未有列入在指引內。為確保僱主收集個人資料符合公平原則，披露僱主的身份是必要的。因此，私隱專員建議勞工處制訂明確指引，以便職員遵從。

(d) 防止擅闖儲存或處理個人資料的重地：由於勞工處職員面見求職者的服務櫃位設在辦公範圍內，因此存在未獲授權人士可以擅自闖入儲存或處理求職者個人資料重地的風險。私隱專員建議制訂措施，例如在入口處安裝電子鎖、陪同求職者進入內部辦公範圍，及在顯眼位置張貼告示，清楚分隔服務櫃位範圍和內部辦公範圍，以阻止擅自闖入的情況。

(e) 未有制訂閉路電視政策及／或程序：為保安目的，勞工處在就業中心的公共地方安裝了閉路電視，但沒有足夠措施防止閉路電視系統被未獲授權查閱，亦沒有就如何使用閉路電視制訂書面指示。例如，查閱影像和登入系統無需密碼，及查閱閉路電視的控制板及顯示器，無需存放在上鎖的櫃或房間內。私隱專員建議制訂及實施閉路電視政策及程序，指明獲授權查閱閉路電視影像的人士、閉路電視系統的保安措施及閉路電視影像的保留時期。

視察報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/inspection_reports/files/R14_3849_c.pdf

(c) Disclosure of employer's identity to a job seeker who was required to provide his resume: The Labour Department might ask a job seeker to send his resume to the prospective employer directly, and the unwritten rule is to disclose the prospective employer's identity and contact means to the job seeker during the referral process. To ensure the fair collection of personal data by the employer, the disclosure of the employer's identity is imperative; hence the Commissioner recommends devising clear guidelines for the staff to follow.

(d) Preventing trespass into restricted areas where personal data is stored or processed: The service booths where the Labour Department staff interview job seekers are located inside the office, so there is a risk of trespass by unauthorised persons into restricted areas where personal data is stored or processed. The Commissioner recommends introducing means to curb such trespass, such as installing electronic locks at the entrance to internal office areas, escorting job seekers, and posting prominent signs to clearly demarcate the service booth area and the internal office area.

(e) Lack of CCTV policies and/or procedure: The Labour Department has installed for security purposes CCTV cameras in the public areas of the Job Centres, but there are insufficient measures to prevent unauthorised access to the CCTV systems and no specific written instructions on the use of CCTV. For example, no login or password is required to access the footage or system; and CCTV control panels and monitors are not required to be stored in a locked cabinet or room. The Commissioner recommends devising and implementing CCTV policies and a procedure specifying who is authorised to access the captured CCTV images, measures to safeguard the security of the CCTV systems, and the maximum retention period of the captured CCTV images.

Inspection Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/inspection_reports/files/R14_3849_e.pdf

讚賞 Compliment

我們希望藉此機會，多謝公署協助我們檢視資料保障系統，並在視察過程中提供寶貴的改善建議。

We would like to take this opportunity to express our gratitude to PCPD for helping us review our data protection system and offering valuable advice for improvement throughout the inspection process.

嚴麗群女士
勞工處高級勞工事務主任
Ms Cindy YIM
Senior Labour Officer, Labour Department

資料外洩通報

資料外洩事故一般是指資料使用者懷疑其持有的個人資料保安不足，以致洩露資料，令資料可能被人未經授權或意外地查閱、處理、刪除、喪失或使用。資料外洩事故可能構成違反保障資料第4原則。公署敦請資料使用者一旦發生資料外洩事故，須通知受影響的資料當事人、私隱專員和其他相關人士。

公署在接獲資料外洩事故通報（可用公署的指定表格呈報）後，會評估有關資料，以考慮是否有需要對有關機構展開循規審查。若私隱專員決定進行循規審查，會書面通知相關的資料使用者，並向機構指出明顯的不足之處，建議他們採取補救措施，防止同類事故重演。

DATA BREACH NOTIFICATION

A data breach is generally understood to mean a suspected breach of security of personal data held by a data user which results in exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. The breach may amount to a contravention of Data Protection Principle 4. When a data breach occurs, data users are strongly advised to give formal data breach notification ("DBN") to the affected data subjects, the Commissioner, and any other relevant parties.

Upon receipt of a DBN from a data user (which can be submitted using the designated form), the PCPD assesses the information provided in the DBN and decides whether a compliance check is warranted. For DBN cases where the Commissioner decides to conduct compliance checks, the Commissioner alerts the data users in writing, pointing out the apparent deficiency and inviting them, where appropriate, to take remedial action to prevent a recurrence of the incident or a similar one.

在本年度，公署接獲66宗資料外洩事故通報（41宗來自公營機構；25宗來自私營機構），牽涉77,409名人士的個人資料。公署對肇事機構展開66項循規審查行動。

During the year, the PCPD received 66 data breach notifications (**41** from the public sector and **25** from the private sector), affecting **77,409** individuals. In response, the PCPD conducted **66** compliance checks.

個人資料的核對程序

在本年度，私隱專員共收到13宗個人資料核對程序申請，全部來自政府部門及公營機構。

經審閱後，私隱專員在有條件的情況下批准了七宗申請。截至2015年3月31日，私隱專員尚在考慮六宗申請。

以下是私隱專員核准進行個人資料核對程序的部分個案：

DATA MATCHING PROCEDURE

During the year, the Commissioner received a total of 13 applications for approval to carry out matching procedures. All of the applications came from government departments and public-sector organisations.

Upon examination, seven applications were approved, subject to conditions imposed by the Commissioner. As at 31 March 2015, the remaining six applications were under consideration by the Commissioner.

Following are some of the matching procedures approved by the Commissioner:

提出要求者 Requesting parties	核准的資料核對程序詳情 Details of the approved data matching procedures
香港房屋委員會 Hong Kong Housing Authority	**把香港房屋委員會從居者有其屋計劃申請人及其家人收集的個人資料，與轄下各項房屋資助計劃的個人資料互相比較，以避免公屋資源遭濫用。** Comparing the personal data collected by the Hong Kong Housing Authority ("HA") from applicants for the Home Ownership Scheme and their family members with the personal data collected in the HA's various subsidised housing schemes, in order to prevent the abuse of public housing resources.
入境事務處 Immigration Department	**把入境事務處從部門宿舍申請人及其配偶收集的個人資料，與香港房屋委員會從資助房屋的租戶、業主及申請人收集的個人資料互相比較，以避免有申請人得到雙重房屋福利。** Comparing the personal data collected by the Immigration Department from applicants for departmental quarters and their spouses with the personal data collected by the HA from the tenants, owners and applicants for subsidised housing, in order to prevent the collection of double housing benefits.
選舉事務處 Registration and Electoral Office	**把選舉事務處從地方選區登記參選人收集的個人資料，與民政事務局為居民代表選舉及街坊代表選舉的選民登記而收集的個人資料互相比較，以提高選民登記冊的準確性。** Comparing the personal data collected by the Registration and Electoral Office from the registered electors of geographical constituencies with the personal data collected by the Home Affairs Department for voter registration for the Resident Representative Election and Kaifong Representative Election, in order to enhance the accuracy of the voter register.
民政事務局 Home Affairs Bureau	**把民政事務局從關愛基金的「非公屋、非綜援的低收入住戶一次過生活津貼」申請人收集的個人資料，與土地註冊處收集的註冊業主資料互相比較，以確定申請人的資格。** Comparing the personal data collected by the Home Affairs Bureau from the applicants for the "One-off living subsidy for low-income households not living in public housing and not receiving Comprehensive Social Security Assistance" under the Community Care Fund with the personal data collected by the Land Registry from registered property owners, in order to ascertain the eligibility of the applicants.