監督循規
擁抱挑戰
Monitoring Compliance Embracing Challenges

合規及查詢科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 & Enquiries Section monitors and promotes compliance with the provisions of the Ordinance. In view of 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.

抽查以兒童為對象的網站及程式

公署於2015年5月抽查45個由本地機構開發，以兒童為對象的網站及手機程式（「程式」）。今次抽查是響應「全球私隱執法機關網絡」（Global Privacy Enforcement Network）舉行的全球聯合行動。公署聯同全球其他28個私隱執法機關抽查1,494個以兒童為對象的網站及程式，以了解它們在私隱保障上的做法。結果顯示有些網站及程式有良好的私隱措施，但當中也有部分的做法不太理想。

抽查結果

超過三成的本地網站及程式有收集兒童的香港身份證號碼。近一半的網站及程式在私隱政策中有提及會把資料轉移給第三者。下表列出抽查的主要結果，並將香港的抽查結果與全球的抽查結果作比對。

STUDY OF WEBSITES AND MOBILE APPS TARGETING AT CHILDREN

The PCPD conducted a study of 45 local websites and mobile applications ("apps") targeting at children in May 2015. The study was part of the Global Privacy Enforcement Network ("GPEN") Sweep exercise, in which the PCPD joined forces with 28 other privacy enforcement authorities around the globe to examine the privacy protection of 1,494 websites and apps targeting at children. The results showed that some local websites and apps applied good privacy practice while others were not satisfactory.

The Findings of the Study

More than a third of the local websites and apps asked for children's HKID Card number. Almost half of the local websites and apps indicated in their privacy policies that they might share the collected personal data with third parties. The table below summarises the major findings of the study, and a comparison between Hong Kong's and global results.

	香港（45個網站及程式） Hong Kong (45 websites and apps)	全球（1,494個網站及程式） Global (1,494 websites and apps)
收集用戶的香港身份證號碼 Collect user's HKID Card number	16 (36%)	不適用 Not applicable
收集用戶就讀學校的名稱 Collect name of school attending by the user	14 (31%)	無相關資料 Not available
收集用戶的住址 Collect user's home address	27 (60%)	19%
收集用戶的電話號碼 Collect user's phone number	33 (73%)	22%
向用戶收集第三者資料 Collect third parties' information from user	16 (36%)	18%
以簡單語言向兒童傳遞私隱政策 Convey privacy policy in simple language for children	2 (4%)	22%
有提及會把用戶的個人資料轉移予第三者 Indicate possible transfer of user's personal data to third parties	22 (49%)	51%
提供途徑讓用戶刪除帳戶 Provide means for user to delete his account	2 (4%)	29%

整體而言，抽查人員對14個本地網站（31%），有關其欠缺清晰的私隱政策、沒有明顯理由而收集香港身份證號碼，以及要求兒童提供朋友或家人的個人資料時沒有充分提示他們應先諮詢這些人士表示憂慮。對比全球調查而言，41%的抽查網站及程式受到類似的關注。

Overall, concerns were expressed in 14 local websites (31%) over the lack of visible privacy policy, the collection of HKID Card number without obvious reasons, and the request for children to share the personal data of friends or families without sufficient prompting that they should consult those people first. In comparison, the global Sweep exercise identified similar concerns in 41% of the websites and apps studied.

良好行事方式的例子

今次全球抽查行動亦發現一些具良好行事方式的網站及程式。有些網站及程式採取了保護措施來防止兒童不經意地分享了其個人資料，例如讓兒童選用預設的頭象或用戶名稱，而非任由他們輸入個人資料。在香港，值得一提的是香港女童軍總會的收集資料聲明頗具透明度，並且會因應對象而設計內容。其收集資料聲明是以精簡的方式說明收集個人資料的目的，並提供了總會的保障資料主任的聯絡資料。

給以兒童為對象的資料使用者的指引

針對今次的抽查結果，公署制定了一份名為《經互聯網收集及使用個人資料：以兒童為對象的資料使用者注意事項》的單張，為資料使用者提供實用建議及良好的行事方式作參考。例如：

- 避免使用開放式問題以減少及限制向兒童收集的個人資料的數量；
- 向兒童提供刪除帳戶及個人資料的途徑；
- 在使用個人資料作新用途前，要先得到兒童及家長／監護人的同意；
- 把個人資料加密；及
- 就私隱政策及行事方式，向兒童及其家長提供簡單易明的資訊。

給家長及老師的實用建議

公署曾於2015年5月公佈另一份有關香港兒童所面對的私隱問題的研究報告。報告顯示家長及老師對兒童私隱保障的議題認知不足。公署因此制定了一份名為《兒童網上私隱 —— 給家長及老師的建議》的單張，向他們作出以下建議：

- 積極參與 —— 家長及老師應以身作則，了解網上世界的運作，並積極參與兒童的網上活動；
- 保障兒童私隱基本功 —— 就保安措施、數碼腳印、私隱設定及尊重家人及朋友意願方面作出建議；及
- 樹立好榜樣 —— 家長及老師應該向兒童示範如何保障、尊重自己及他人的個人資料。

Examples of Good Practice

The global Sweep found some examples of good practice, with some websites and apps providing effective protective measures in the form of preset avatars or usernames to prevent children from inadvertently sharing their personal data. In Hong Kong, we found the transparent and fair collection statement of the Hong Kong Girl Guides Association worthy of mentioning. The collection statement sets out in a concise and simple manner the purposes for which personal data is collected, and the contact details of the Association's Data Protection Officer.

Guidance Note for Data Users Targeting at Children

To follow up on the findings of the Sweep exercise, the PCPD released a leaflet for data users entitled "Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children" to provide practical suggestions and good practice, such as:

- Avoid the use of open-type questions to reduce and limit the amount of personal data collected from children;
- Offer means for children to remove the accounts and all associated personal data;
- Obtain the consent of children, and their parents or guardians before using the collected personal data for a new purpose;
- Safeguard the personal data by encryption; and
- Offer easily-understood, user-friendly and age specific information to children and their parents regarding privacy policy and practice.

Practical Tips for Parents and Teachers

In May 2015, the PCPD released a separate report on an exploratory study which had been carried out to identify major privacy concerns and problems faced by children in Hong Kong. The results showed that parents and teachers seemed to have insufficient awareness about children's privacy issues. Addressing these issues, the PCPD published a leaflet entitled "Children Online Privacy – Practical Tips for Parents and Teachers". Recommendations include:

- Active Participation – Parents and teachers are encouraged to engage with children in the online activities and understand the operation of the online world;
- Basic Steps for Children Privacy – Suggestions are provided on security measures, digital footprints, privacy settings and respecting the privacy of family members and friends; and
- Setting a Good Example – Parents and teachers are role models for children. They should set good examples by protecting their own personal data and respecting others' personal data privacy.

在某些情況下，從幼小兒童收集第三者的個人資料可能會被視為不公平收集個人資料，違反條例附表1的第1(2)(b)保障資料原則。

在尊重他人的個人資料方面，家長及老師應樹立榜樣，在分享朋友及第三者的個人資料之前先諮詢他們。關於分享兒童的資料（例如相片、考試成績及參與體育賽事的資料），家長及老師應以兒童的利益為依歸，包括考慮任何可能會對兒童造成的傷害及在其長大後可能會產生的尷尬情況。然而，兒童對私隱的期望及作出決定的能力會隨著個人成長及智力發展而改變，家長及老師應經常與兒童坦誠地討論網上的活動。

公署亦改革了「兒童私隱」網站（www.pcpd.org.hk/childrenprivacy），為家長和老師提供一站式的保障私隱資訊，當中有不少實用建議及教材。

Collection of third party's personal data from young children may in some circumstances amount to unfair collection contrary to DPP1(2)(b) in Schedule 1 to the Ordinance.

On respecting the personal data privacy of others, parents and teachers should set an example by consulting their friends or third parties before sharing their personal data. In terms of sharing children's information (such as photographs, examination results and participation in sporting events), parents and teachers should invariably take into account the interest of the children, including any harm and potential embarrassment in the future. However, as children's expectations on privacy and ability to make decisions vary depending on individual maturity and intellectual development, parents and teachers are encouraged to discuss with them frequently and frankly on their online practices.

The PCPD has also revamped a thematic website entitled "Children Privacy" (www.pcpd.org.hk/childrenprivacy), which is a one-stop portal to provide teachers and parents with practical tips and teaching resources on personal data protection for children.

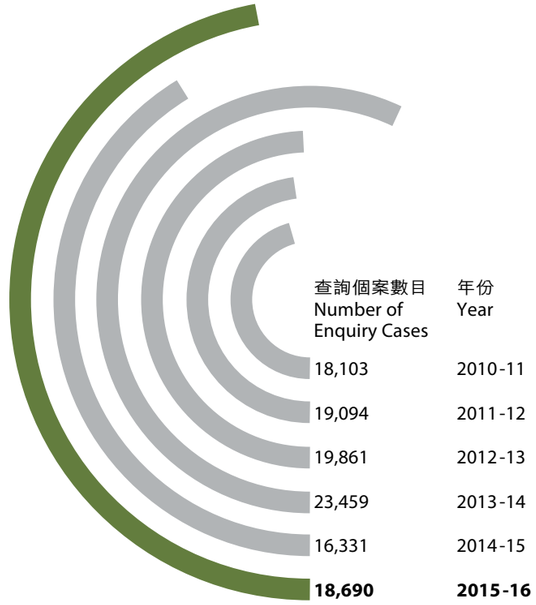
處理查詢

公署在本年度共處理18,690宗查詢個案，比上年度上升14%；平均每個工作天處理76宗查詢（圖 2.1）。

HANDLING ENQUIRIES

A total of 18,690 enquiries were handled during the year, up 14% from that of the previous year. On average, 76 enquiries were handled per working day (Figure 2.1).

圖 Figure 2.1 全年查詢個案
Annual enquiry caseload



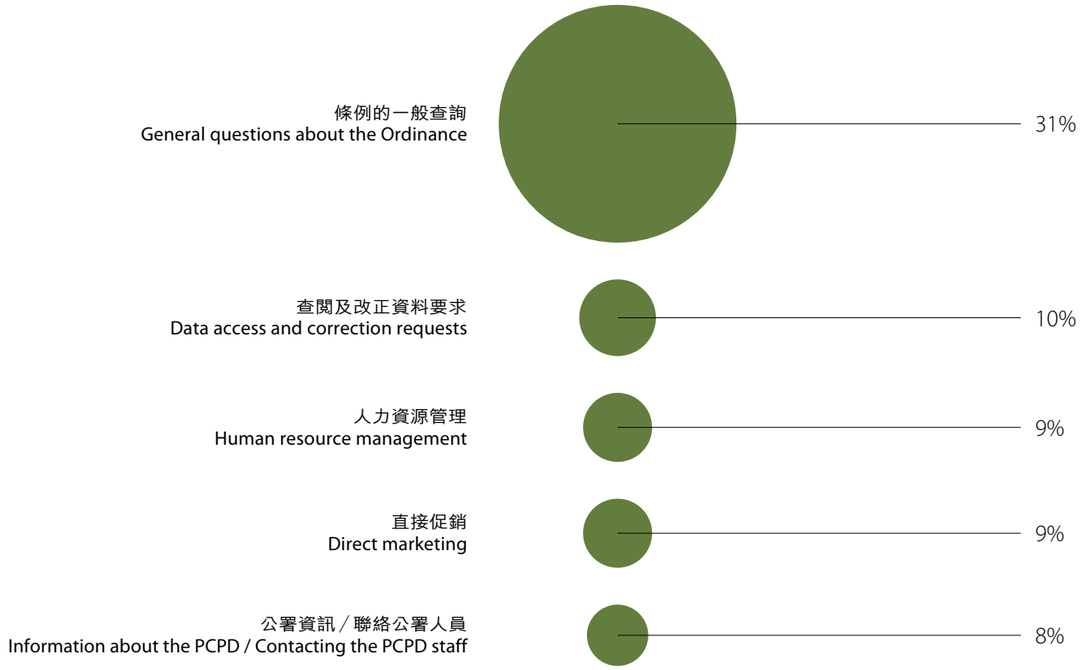
郭正熙
高級個人資料主任
（合規及查詢）
Brad KWOK
Senior Personal Data Officer
(Compliance & Enquiries)

感言 Sharing

我在公署已經工作十個寒暑，很感恩我能跟公署一起成長、一起經歷很多不同的挑戰。我十分欣慰市民大眾及機構越益重視個人資料私隱，並尊重及欣賞公署為保障市民個人資料私隱的工作。這都是我們致力保障市民的個人資料私隱所得到最正面的回饋。今年，我再次調任至合規及查詢科工作，希望能繼續運用我的知識及經驗協助公署執法及推廣條例，以迎接下一個十年所帶來的新挑戰。

It is my pleasure that I grew and experienced with the PCPD over the last 10 years. I am so pleased to see that the public and organisations have given greater attention to the personal data privacy, respected and appreciated what PCPD does in protecting personal data privacy of the community. This is the best reward for the commitment in our work. I have returned to the Compliance and Enquiry Section this year and would endeavour to assist the PCPD in enforcing and promoting the Ordinance and to meet the new challenges in the next decade.

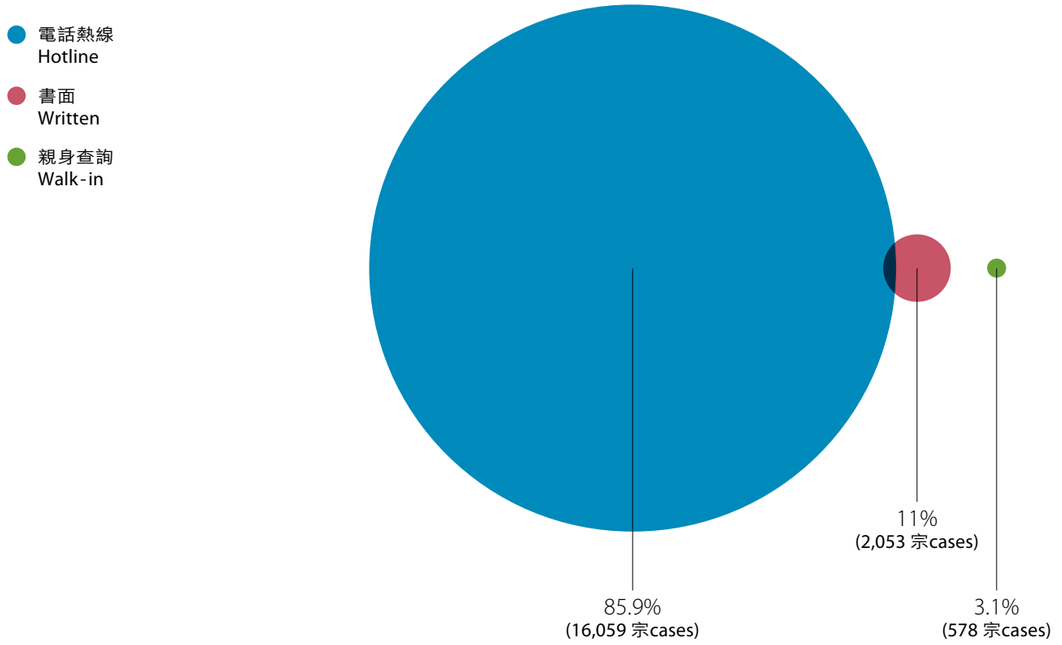
圖 Figure 2.2 查詢個案的性質 Nature of enquiries



大部分（85.9%）查詢經由公署的電話熱線（2827 2827）提出（圖2.3）。

The majority of the enquiries (85.9%) were made through the PCPD hotline (2827 2827) (Figure 2.3).

圖 Figure 2.3 提出查詢的途徑 Means by which enquiries were made



新入職員工 Newcomer

我現時的職責是負責處理公眾查詢。每星期接聽數以百計、內容牽涉不同範疇的電話查詢，對我來說確實是一大挑戰。然而，能令查詢者對條例有更深入的了解，幫助他們解決有關個人資料私隱的各種問題，這著實帶給我不少的滿足感，亦令我感受到工作背後的使命感。我很感謝公署給予機會，讓我能於各部門輪換工作，擴闊工作經驗。我會繼續努力，以誠懇有禮的態度，為市民提供優質及有效率的服務。

My current duty is to handle enquiries from the public. Although it is a challenge for me to answer hundreds of diversified enquiries every week, the job brings me enormous satisfaction and makes me realise the mission of work when I can help the enquirers to have a better understanding of the Ordinance and solve personal data privacy-related problems for them. I feel truly grateful for the valuable opportunity to broaden my work experience through job rotation amongst different divisions. I will continue to serve the public positively by providing them with quality and efficient service.

張穎聰
一級助理個人資料主任（合規及查詢）
Mavis CHEUNG
Assistant Personal Data Officer I (Compliance & Enquiries)

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。

在報告年度內，私隱專員共進行了286次循規審查行動。77%的循規審查對象為私營機構，其餘23%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。

11,655名香港客戶信用卡資料遭零日惡意程式入侵

據本地報章報道，一間國際酒店集團的信用卡系統遭零日惡意程式入侵，因此曾在該酒店集團使用信用卡購買其產品及服務之客戶的姓名及信用卡號碼有可能遭外洩。該酒店集團後來向公署表示事件涉及旗下兩間位於香港的酒店，合共影響11,655組信用卡資料。

該酒店解釋，它在2015年2月獲瑞士信用卡處理中心通知，其資訊系統可能遭惡意程式攻擊。法證調查結果顯示，黑客為了可以獲得信用卡資料，曾透過旗下一部位於印尼雅加達酒店的伺服器進入集團網絡，利用擁有管理員權限的系統帳戶在全球系統內種植惡意程式。有關調查表示並沒有證據證明信用卡資料遭洩漏或從其系統中刪除。

該酒店集團事發後立即通知所有受影響的客戶（包括香港客戶），引入抗電腦病毒解決方案的服務提供者制定新病毒數據以刪除有關惡意程式，更新所有系統密碼，封鎖所有不必要的網絡服務，及切斷過時伺服器與網絡的連接，以遏制事故。

COMPLIANCE CHECKS

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

During the report year, the Commissioner carried out 286 compliance checks. Of these, 77% were conducted on private sector organisations, while the remaining 23% were on government departments and statutory bodies, non-government organisations and government-funded educational institutions.

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

Credit Card Data of 11,655 Hong Kong Customers Hacked by a Zero-day Malware

It was reported in local newspapers that the credit card systems of an international hotel group were attacked by a zero-day malware and, as a result, names and credit card numbers of its customers who had used credit cards to purchase products and services were suspected to have been leaked. The hotel group subsequently reported to the PCPD that two of the group's hotels in Hong Kong were involved in the incident, affecting a total of 11,655 sets of credit card data.

The hotel group explained that the group was first notified by its card processing company in Switzerland of the possibility of the malware attack on its information systems in February 2015. The forensic investigations revealed that a hacker gained access to the group's network through a server in its hotel in Jakarta. He utilised a system account with administrative privileges and planted the malware in the systems worldwide in order to gain access to the credit card data. The investigations suggested that there was no evidence to show that the credit card data had been exfiltrated or removed from its systems.

Immediately after the incident, the group notified all affected customers (including Hong Kong customers) and engaged antivirus solution providers to develop new virus signatures to remove the malware. It also changed all the system passwords, blocked all unnecessary network services and disconnected decommissioned servers from its network.

該酒店集團採取了下述補救行動，防止日後再發生類似事件：

- 實施一份「二進制白名單」，避免未獲授權的原碼及／或軟件在其網絡中執行；
- 為管理員帳戶及遠端存取帳戶進行定期審計，減低可能損害其網絡的潛在風險；
- 改善重要系統或該些載有特別權限系統的記錄設定，以提升追蹤性及問責性；及
- 提高對外互聯網連接權限，以防範惡意通訊。

承辦商未獲授權下載210,000名銀行客戶的個人資料

一間銀行向公署通報，銀行委託了一名承辦商執行銀行的系統發展項目，並授權他使用銀行的原始資料進行有關的項目測試，惟該承辦商其後被發現在未獲授權的情況下從銀行的電腦下載了964個載有客戶個人資料的檔案至其個人流動裝置。涉及的個人資料包括約210,000名客戶的香港身份證號碼、住宅及郵寄地址，以及基金投資資料。

該銀行解釋，事件是由於銀行的資料遺失防護系統的配置有漏洞，以致系統只能阻止資料被儲存到外置的儲存裝置，但有關的儲存裝置卻不包括視窗便攜式裝置，例如智能電話及平板電腦。該銀行述明該名承辦商並沒有對外披露或使用其所下載的檔案資料。

該銀行採取了下述補救行動，防止日後再發生類似事件：

- 重新設置其資料遺失防護系統，以阻止資料被傳輸到視窗便攜式裝置；
- 加強其資料外洩偵測工具及安裝在電腦的端點保安軟件，以防止惡意或未獲授權的資料轉移；
- 透過雲端監控工具監察經互聯網傳輸的資料；及
- 更改其現有程序指引，要求承辦商日後只可以虛擬或匿名化的資料作系統測試及發展。

The hotel group had also taken the following remedial actions to prevent similar incidents:

- Implementing a binary whitelist to prevent any unauthorised code and/or software from being executed from its network;
- Conducting periodic audits of administrator and remote access accounts to reduce the potential threat that could harm its network;
- Improving logging record for all critical systems or systems with privilege access to increase traceability and accountability; and
- Increasing restriction on outbound Internet connections to protect against malicious traffic.

Unauthorised Download of 210,000 Customers' Personal Data by a Contractor

A bank informed the PCPD that its designated contractor had downloaded 964 data files from the bank's computer workstation to his personal mobile device without authorisation, although he was granted access to those raw data under the bank's supervision in a system development project. The personal data involved in the incident included the HKID Card numbers, residential and postal addresses, and fund investment details of approximately 210,000 customers.

The bank explained that the incident was caused by the misconfiguration of its data loss prevention system, which was set up to prevent unauthorised data transfer to external storage devices but failed to block the transfer of data from computer workstations to "Windows Portable Devices" such as smartphones and tablets. The bank stated that the data files downloaded had not been further disseminated or misused by the contractor.

The bank reported to the PCPD that it had taken the following remedial actions to prevent similar incidents:

- Re-configuring the data loss prevention system controls to block all data connection with Windows Portable Devices;
- Enhancing its inadvertent data disclosure tool and end-point security tool on its computer workstations to prevent malicious or unauthorised data transfer;
- Implementing an Internet cloud-monitoring capability tool to monitor external data transfers through Internet services; and
- Revising its procedures that allow only dummy or masked personal data to be used for the purposes of testing and system development in future.

學會誤信仿冒詐騙電郵導致6,131名會員資料外洩

一間學會向公署通報，該學會不慎地應一封仿冒詐騙電郵的要求而洩漏了會員的個人資料。該電郵看似來自該學會的行政總裁，要求索取會員資料。該學會不疑有詐，向該仿冒詐騙電郵的來件者發送一份載有6,131名會員的姓名、勳銜及電郵地址的名單。

該學會解釋，該仿冒詐騙電郵要求把有關資料傳送到兩個指定的電郵地址，其中一個是行政總裁的官方電郵地址，另一個看來是他的私人電郵地址。基於收到有關要求的職員相信其行政總裁急切需要有關資料，因此才遵從該要求而導致資料外洩。該學會再解釋，雖然載有會員資料的資料庫已受密碼保護及加密，但在事件中從資料庫所產生的名單，是沒有受到任何措施保護的。

該學會因應事件採取了下述補救行動，防止日後再發生類似事件：

- 要求所有職員以電郵通訊時須用密碼保護載有個人資料的檔案及限制他們使用私人電郵帳戶進行與業務有關的事宜；
- 提醒所有職員嚴格遵守其「資訊保安政策」及「可接受使用政策」所規定的要求；
- 提供培訓以加強職員對資訊科技保安的意識；及
- 聘請外間資訊科技顧問，提供持續的保安監控及對資訊科技和保障資料事宜的意見。

Data Leakage via a Phishing Email Involving 6,131 Members of an Institute

An institute reported to the PCPD that it had inadvertently sent a list containing the name with suffix and email address of 6,131 members to a deceptive phishing email, which purported to be the Chief Executive of the institute requesting for members' information.

The institute explained that the "phishing email" requested the information to be sent to two specified email addresses, one being the Chief Executive's official email address while the other purporting to be his personal email address. Since the staff member who received the request believed that the information was urgently required by the Chief Executive, he complied with the request and hence caused the leakage. The institute further explained that although its membership database was password protected and encrypted, the list generated from the database in the incident was not secured by any measures.

The institute subsequently took the following remedial actions to prevent recurrence of the incident:

- Requiring all staff to protect files containing personal data by password for email communications and restricting the use of personal email accounts for business related matters;
- Reminding all staff to strictly adhere to the requirements stipulated in its Information Security Policy and Acceptable Use Policy;
- Providing training to enhance staff awareness of information-technology security; and
- Engaging an external information technology consultant to provide continuous security monitoring and consultation on information technology and data protection matters.

訂購食物紀錄經互聯網外洩涉及62,539名客戶

公署接獲市民通知，一間專門提供食物外送服務的公司的客戶資料經互聯網外洩，公眾人士可透過互聯網開啟該公司伺服器內的超文本預處理器(即Hypertext Preprocessor)查閱該公司客戶的訂購食物紀錄及所提供的個人資料。涉及的個人資料包括62,539名客戶的名稱、地址、電話號碼及電郵地址。

該公司解釋，事件是源於其伺服器內相關資料夾的存取權限出現錯誤，以致無關人士可透過互聯網查閱客戶的個人資料。該公司在事發後立即更正有關資料夾的存取權限，並將有關的系統程式檔案重新命名及增設密碼，以防止無關人士透過該超連結再次開啟伺服器內的超文本預處理器。

該公司亦採取了下述補救行動，防止日後再發生類似事件：

- 委託系統開發公司定期檢查伺服器以確保有關的資料夾的存取權限正確；
- 將網上訂購紀錄的保存期限縮短為送貨完成日起計一天，並已編寫了相關程式以確保資料會被準時刪除；及
- 切換現有的電腦系統，在新系統中加入認證功能，以確保只有獲授權的網際網路協定位址或電腦才可以讀取新系統內的客戶個人資料。

Online Food Ordering Records Leaked to the Internet Involving 62,539 Customers

A citizen reported to the PCPD that public were able to access the food ordering records and personal data of customers of a company, which provided food delivery services, by clicking the hyperlink of the company's hypertext preprocessor posted on the Internet. The personal data involved in the incident included the names, addresses, telephone numbers and email addresses of 62,539 customers.

The company explained that the incident was caused by the incorrect setting of a folder's access right stored in the server, which allowed unintended parties access to its customers' personal data via the Internet. Immediately after the incident, the company rectified the access right of the folder, renamed and enabled password protection of the relevant system programme files so as to prevent unintended parties from accessing the company's hypertext preprocessor by using the said hyperlink.

The company also took the following remedial actions to prevent recurrence of the incident:

- Appointing a system developer to regularly inspect the server to ensure the correctness of the folder's access right;
- Shortening the retention period of the food ordering records to one day after the delivery, and compiling programmes to ensure that the ordering records would be erased timely; and
- Replacing the existing computer system - Authentication function was included in the new computer system so that only authorised IP addresses or computers could access customers' personal data stored in the new system.

感言 Sharing

蘇定欣
個人資料主任
（合規及查詢）
Ivy SO
Personal Data Officer
(Compliance & Enquiries)

作為個案主任，我經常處理不同案件，當中不乏涉及複雜的法律問題。公署為確保我們了解與條例相關的最新案例及科技發展，不時舉辦個案分享會及專題研討會，並鼓勵我們參與有關保障個人資料私隱的國際會議。此外，公署亦會聘請專業機構為我們提供語文及個人發展的培訓。我亦在上司的支持下在工餘時間攻讀香港中文大學法學碩士課程。

我認為公署十分重視員工的發展。我在此感謝公署挑選我調任至傳訊及教育部九個月，讓我擴闊視野及汲取多元化的工作經驗，使我在公署的各個職能上有更全面及靈活的發展。

展望將來，我相信公署在私隱專員的領導下能夠繼續弘揚「保障、尊重個人資料」的文化。

As a case officer, I handle a variety of cases that often involve complex legal issues. To keep staff members abreast of the judgments and the latest technologies relevant to the Ordinance, the PCPD organises internal case sharing and thematic seminars from time to time, and encourages us to participate in international conferences relating to personal data privacy. In addition, the PCPD invites professional organisations to provide staff trainings on language and personal development. With the support of my superiors, I further pursued my study for the Master of Laws degree at the Chinese University of Hong Kong during my leisure.

The PCPD places a lot of value on staff development. I am thankful to be selected for a secondment to the Communications and Education Division for nine months. I have broadened my horizon and gained diversified work experiences through this opportunity, and I found myself having a more comprehensive and versatile development in the PCPD.

Looking forward, I believe that under the leadership of the Commissioner, the PCPD will continue to strive to promote the culture of "Protect, Respect Personal Data".

主動調查

私隱專員就58則匿名招聘廣告不公平收集求職者個人資料發表報告

公署發現機構沒有披露其身份而刊登58則匿名招聘廣告（即「匿名廣告」），以不公平方式收集求職者的個人資料，違反條例下保障資料第1(2)原則。

2014年，公署審視了刊登於七個主要招聘媒體（即Career Times、JobsDB、青雲路、Recruit、Classified Post、招職及求職廣場）的9,016則招聘廣告，發現當中有311則匿名廣告，佔總數的3.45%。私隱專員隨機選了當中71則廣告展開調查，結果向69名僱主發出了執行通知。七個招聘媒體中，有六個向私隱專員承諾會做好把關工作，採取措施制止匿名廣告。

公署其後於2015年再次進行類似調查，發現匿名廣告的情況明顯有所改善。公署在此年度的同期審閱了上述七個媒體刊登的12,849則招聘廣告，從中只找到59則匿名廣告，佔總數的0.46%。換句話說，匿名廣告的比例從上年度的3.45%大幅回落至本年度的0.46%。

在進行調查的59則匿名廣告中，58則被發現違反條例下的保障資料第1(2)原則的規定。在餘下一宗個案中，私隱專員發現有關僱主已曾發出指引及在培訓中提醒員工不得刊登匿名廣告，本個案源於有僱員沒有依從僱主的指引行事，僱主根據條例第65(3)條可被免責。

執法行動

其中一位違反了保障資料第1(2)原則的僱主主動向私隱專員提出已刪除所有求職者的資料及作出書面承諾日後刊登招聘廣告時會緊遵條例的規定，其餘僱主全被私隱專員發出了執行通知，指令他們刪除已收集的求職者資料（除非求職者同意其資料被保留以繼續招聘程序等）。

私隱專員的意見

2015年的調查清楚顯示，匿名廣告的數量相比2014年大幅減少。毫無疑問，招聘媒體就此作出了明顯的改善。私隱專員對招聘媒體的努力表示讚許，並呼籲他們持續加大力度遏止匿名廣告，促使該些廣告最終在招聘市場上銷聲匿跡。

PCPD-INITIATED INVESTIGATIONS

The Commissioner Revealed 58 Blind Recruitment Advertisements for the Unfair Collection of Job Applicants' Personal Data

A number of organisations were found to be in breach of DPP1(2) of the Ordinance for placing 58 job advertisements without disclosing their identities ("Blind Ads"), thus soliciting job applicants' personal data in an unfair manner.

In 2014, the PCPD reviewed 9,016 recruitment advertisements on seven major recruitment media in Hong Kong, namely Career Times, JobsDB, JobFinder, Recruit, Classified Post, Jiu Jik, and JobMarket. 311 Blind Ads (3.45% of the total) were identified. Of these, 71 Blind Ads selected on a random basis were investigated and as a result, all 69 employers concerned were issued enforcement notices. Further, six of the seven recruitment media responded to the Commissioner's appeal and pledged to take actions to deter Blind Ads.

In 2015, the PCPD continued with similar investigations, and found that the situation of Blind Ads has improved. The PCPD examined 12,849 advertisements placed in the same seven recruitment media, and only 59 Blind Ads (0.46% of total) were identified. That is, the proportion of Blind Ads has dropped from 3.45% in 2014 to 0.46% in 2015.

Of the 59 Blind Ads, 58 were found to be in breach of DPP1(2) of the Ordinance. In the remaining case, the employer was found to have already issued guidelines on the prohibition of placement of Blind Ads and trained its employees on those guidelines regularly. As such, the company appeared to have already taken practicable steps to prevent the placing of Blind Ads and satisfied the defence provisions under section 65(3) of the Ordinance.

Enforcement Action

One of the employers in breach of DPP1(2) had proactively informed the Commissioner that it had deleted all job applicants' personal data and provided a written undertaking to the Commissioner that it would duly comply with the requirements under the Ordinance when placing recruitment advertisements in future. All remaining employers were issued an enforcement notice directing them to delete the personal data collected (unless the job applicants choose to have their personal data retained for a continuing recruitment process, etc).

The Commissioner's Comments

The result of the survey in 2015 indicated clearly that the proportion of Blind Ads has been reduced drastically compared with that of 2014. No doubt the recruitment media have played an instrumental role in the improvement. The Commissioner appreciates greatly their dedicated efforts and calls on the recruitment media to continue to step up such efforts so that Blind Ads can eventually be eliminated from the job market.

視察行動

公署根據條例第36條，在2015年3月至10月期間視察一間旅行社的個人資料系統；並於2016年1月發表視察報告。

視察原因

外遊是港人喜愛的消閒活動，而旅行社會收集和保存大量顧客的個人資料包括姓名、護照資料、出生日期、聯絡資料及信用卡資料等。私隱專員對旅行社的個人資料系統進行視察，藉以促進同一行業的資料使用者循規，以符合條例的規定。

香港有超過1,700間持牌旅行社，專員揀選視察對象的考慮因素包括客戶的人數，及旅遊業界收集個人資料的途徑（即分行、電話報名中心及網站）。是次視察的對象為康泰旅行社。

視察結果

公署注意到該旅行社在資料保障方面有一些值得參考的行事方式；包括重視私隱管理，委派高層管理人員監督私隱事宜；向親身報團的顧客只收集必需資料；適時銷毀載有個人資料的文件；以及謹慎處理敏感文件。

建議

公署亦向該旅行社提出建議，改善其資料保障措施，包括：

- 要符合「資料收集原則」：例如是否需要在網上報團時收集顧客的地址及香港身份證號碼；及是否需要收集其會員計劃參加者的出生年月日，以處理入會申請及換取優惠；
- 要符合「資料使用原則」及使用個人資料於直接促銷的規定：在表格上具體說明旅行團顧客的個人資料會轉移給甚麼類別的人士，及資料轉移的目的；如不會轉移尊享會會員的個人資料予任何人士，便應列明出來；讓參加者表示是否反對使用其個人資料作直接促銷的選項，列於表格上顯眼的位置；

INSPECTION

The PCPD inspected the personal data system of a travel agent between March and October 2015 pursuant to section 36 of the Ordinance, and published an inspection report in January 2016.

Reasons for Inspection

Vast amount of customers' personal data including the name, passport details, date of birth, contact information, and credit card details are collected and retained by travel agents in Hong Kong. The Commissioner considers that the inspection of a travel agent's personal data system can serve the purpose of promoting compliance by other travel agents.

There are over 1,700 licensed travel agents in Hong Kong. The particular travel agent was selected in the inspection because of the vast number of customers it had and the channels of personal data collection (namely branches, call centre and website) are commonly used in the travel service industry. Hong Thai Travel Services Limited was selected for the inspection.

Findings

The PCPD found some good practices adopted by the selected travel agent which can be used as a frame of reference by other agents. These practices include commitment to privacy management by assigning a high-ranking management officer to oversee privacy matters; only necessary data is collected from a customer when tour services are booked at a branch; timely destruction of documents containing personal data; and secure handling of sensitive documents.

Recommendations

The PCPD also made some recommendations to this travel agent in the following areas to improve its data protection practice.

- Collection principle of personal data: whether there is any need to collect the address and HKID Card number from a tour customer who books a tour online, and whether there is a need to collect full date of birth from loyalty programme members in order to process the membership application and the points redemption;
- Data use principle and the requirements of the use of personal data in direct marketing: specify precisely in the registration form the classes of persons to whom a tour customer's personal data may be transferred and the purposes of such transfer; state in the terms and conditions of its loyalty programme that there is no transfer of a loyalty programme member's personal data to any other parties, if this is the case; and relocate the tick box on the paper registration form (for customers to indicate objection to the use of their personal data in direct marketing) to a more prominent place;

- 在保安措施方面的建議：於現有的工作流程或指引中，列明保護敏感資料的措施；貫徹執行員工在互聯網傳輸個人資料時必須加密的規定，並書面訂明違規的後果；以及檢討及完善現行的資訊科技保安政策及管治方式，以確保全面性及完整性；完善處理資料外洩的指引；及
- 在私隱政策的透明度方面：制定私隱政策聲明，並於網上發佈。

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或其他方式呈報）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，指出明顯的不足之處，並建議他們採取補救措施，防止同類事故重演。

在本年度，公署接獲104宗資料外洩事故通報（44宗來自公營機構；60宗來自私營機構），牽涉854,476名人士的個人資料。公署對肇事機構展開循規審查行動。

- Data security measures: formally document the administrative measures in safeguarding sensitive documents in transit in its existing workflow or other procedural guidelines; fully enforce the requirement of encryption when transmitting personal data through the internet and spell out the consequence of non-compliance; review and improve the existing IT security policy and IT governance to ensure its comprehensiveness and integrity; improve the data breach handling guideline; and
- Transparency of the privacy policy: devise a privacy policy statement and make it available online.

DATA BREACH NOTIFICATION

A data breach is a 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 DPP4. Data users are strongly advised to give a formal data breach notification ("DBN") to the affected data subjects, the Commissioner, and other relevant parties after a data breach has occurred.

Upon receipt of the DBN from a data user (which could be submitted through the designated DBN form or other means of communication), the PCPD would assess the information provided in the DBN and decide whether a compliance check is warranted. If a compliance check is to be conducted, the Commissioner would alert the data user in writing, pointing out the apparent deficiency and inviting him, where appropriate, to take remedial actions to prevent a recurrence of the incident.

During the year, the PCPD received 104 data breach notifications (44 from the public sector and 60 from the private sector), affecting 854,476 individuals. The PCPD conducted a compliance check in each of these 104 incidents.

個人資料的核對程序

在本年度，私隱專員共收到46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44宗申請。截至2016年3月31日，私隱專員尚在考慮兩宗申請。

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 report year, the Commissioner received a total of 46 applications for approval to carry out matching procedures. All of the applications came from government departments and public-sector organisations.

Upon examination, 44 applications were approved, subject to conditions imposed by the Commissioner, and the remaining two applications were under consideration by the Commissioner as at 31 March 2016.

Some of the matching procedures approved by the Commissioner are as follows:

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
選舉事務處 Registration and Electoral Office	把選舉事務處從選民登記申請人收集的個人資料，與入境事務處收集的個人資料互相比較，以確定申請人的投票資格。 Comparing the personal data collected by the Registration and Electoral Office from voter registration applicants with the personal data collected by the Immigration Department, in order to determine the applicants' eligibility to vote.
稅務局 Inland Revenue Department	把稅務局根據《印花稅條例》和《稅務條例》所收集的個人資料互相比較，以確保所有由出租物業所得的收入已評稅。 Comparing the personal data collected by the Inland Revenue Department under the Stamp Duty Ordinance and the Inland Revenue Ordinance, in order to ensure all income from let properties is properly assessed of tax.
香港海關 Customs and Excise Department	把香港海關從部門宿舍申請人／居住人及其配偶收集的個人資料，與房屋署收集的個人資料互相比較，以避免有申請人獲取雙重房屋福利。 Comparing the personal data collected by the Customs and Excise Department from departmental quarters' applicants / occupants and their spouses with the personal data collected by the Housing Department, in order to prevent the collection of double housing benefits.
職業訓練局 Vocational Training Council	把職業訓練局從「學費減免及學習開支定額津貼」申請人收集的個人資料，與社會福利署從綜合社會保障援助計劃受助人收集的個人資料互相比較，以避免有申請人獲取雙重津貼。 Comparing the personal data collected by the Vocational Training Council from the applicants of "Tuition Fee Remission and Flat Rate Grant for Academic Expenses" with the personal data collected by the Social Welfare Department from the beneficiaries of Comprehensive Social Security Assistance, in order to prevent the collection of double benefits