查詢服務
Enquiry Service

在個人資料方面保障個人的私隱應是香港每間機構的標準政策。這不單只是因為條例規定，亦因為可以帶來更佳的客戶及僱傭關係、更好的資料質素，以及更有效的資料處理。公署致力加強這個訊息，並透過查詢服務，就保障資料的良好行事方式，向公私營機構提供指導及意見。

The protection of an individual's privacy in relation to personal data should be standard policy for every organization in Hong Kong, not just because of the legal requirements under the Ordinance, but also because it leads to benefits in terms of better customer and employee relations, improved data quality and greater efficiency in data processing. The PCPD strives to reinforce this message and provide guidance on good data protection practices to all public and private organisations, large and small.

例子
EXAMPLE
1

對性罪行定罪紀錄查核機制的意見
Views on the proposed Sexual Conviction Records Check Scheme (SCRC)

性罪行定罪紀錄查核機制(下稱「該機制」)的目的是讓僱主(下稱「相關僱主」)聘任他人從事與兒童及精神上無行為能力人士有關的工作時，得以查核僱員或求職者某些性罪行的刑事定罪紀錄。

The SCRC is intended to enable employers of persons undertaking child-related work and work relating to mentally incapacitated persons (Relevant Employers) to check any criminal-conviction records of employees or job applicants for a specified list of sexual offences.

香港警務處(下稱「警務處」)就該機制的處理申請程序方面徵詢公署的意見。

The Hong Kong Police Force (HKPF) sought the PCPD's views on procedures for handling applications under the proposed SCRC.

2011年3月，公署去信警務處，詳列有關資料私隱的多項關注。公署的主要關注是，即使求職者申請的工作無需接觸兒童或精神上無行為能力人士，也要接受潛在僱主查核其定罪紀錄的要求，因此必須設立足夠保障措施，確保該機制不被非相關僱主濫用。

In March 2011, the PCPD wrote to the HKPF with a number of data-privacy concerns set out in detail. The major concern of PCPD is that, given that job applicants may have to submit to potential employers' demands for checking their conviction records even if the jobs they applied for do not require them to interact with children or mentally incapacitated persons, sufficient safeguard must be in place to ensure that SCRC may not be abused by any person who is not the Relevant Employer.

公署亦關注，根據該建議的機制，警方所收集的求職者指紋的保留時間並不清晰、求職者的紀錄可能過早在招聘初期被查核。另外，公署關注求職者同意披露查核結果的同意表格，認為應改良這表格，給予求職者更佳的保障。

The PCPD also raised concern that, among other things, under the proposed SCRC, the retention period of the job applicants' fingerprints collected by the HKPF was unclear, job applicants' records may be checked prematurely when the recruitment exercise is only at the initial stage, and that the drafting of the consent form to be given by job applicants to the disclosure of the checking result should be improved for better protection of the job applicants.

例子
EXAMPLE
2

非永久性居民身份證持有人使用公營醫療服務資格核實系統
Online checking of the eligibility of non-permanent Hong Kong Identity Card holders for subsidised public health-care services

2011年1月，立法會衞生事務委員會審議「非永久性居民身份證持有人使用公營醫療服務資格核實系統」的討論文件。

政府建議為醫院管理局（下稱「醫管局」）及衞生署設立一個資格核實系統，就病人的居民身份向入境事務處（下稱「入境處」）查核，以確定他們是否享有以補助收費接受治療的資格。

由於該計劃不但關乎醫管局和衞生署查閱個人資料，又涉及入境處披露個人資料，因此，公署於2011年3月18日去信保安局和食物及衞生局，就該建議中有關資料私隱的事宜提出建議及意見，以供考慮。

In January 2011, a discussion paper entitled "Online checking of the eligibility of non-permanent Hong Kong Identity Card holders for subsidised public healthcare services" was tabled before the Legislative Council Panel on Health Services.

The Government proposed setting up an online system for the Hospital Authority (HA) and the Department of Health (DH) to check patients' resident status from the Immigration Department (ImmD) in order to ascertain whether they were eligible to receive health-care treatment at subsidised rates.

As the scheme would involve the online access of personal data by the HA and DH, as well as disclosure of personal data by the ImmD at the same time, the PCPD wrote to the Security Bureau and the Food and Health Bureau on 18 March 2011 with suggestions and comments on the proposal relating to data privacy for their consideration.

例子
EXAMPLE
3

網上查核駕駛執照狀況
Online checking of Driving Licence Status

運輸署就網上查核駕駛執照狀況的建議徵求公署的意見。

根據建議的查核機制，一名人士可透過印於駕駛執照的「參考編號」（由交易編號及簽發日期組成）查核駕駛執照的狀況（例如有效性）。

公署關注建議的查核機制可能會被沒有真正需要知道駕駛執照狀況的人士濫用。因此，公署建議運輸署應採取措施，確保執照持有人是同意有關查核。

The Transport Department ("TD") sought the PCPD's views on its proposal to enable online checking of driving licence status.

Under the proposed checking system, a person may check the status (e.g. the validity) of a driving licence with the "reference number" (which is a combination of transaction number and the issue date) printed on the driving licence.

PCPD expressed concern that the proposed checking system may be abused by a person who does not have a genuine need to know the status of the driving licence. In this regard, PCPD suggested TD that measures should be taken to ensure that the licence holders indeed agree to the checking.

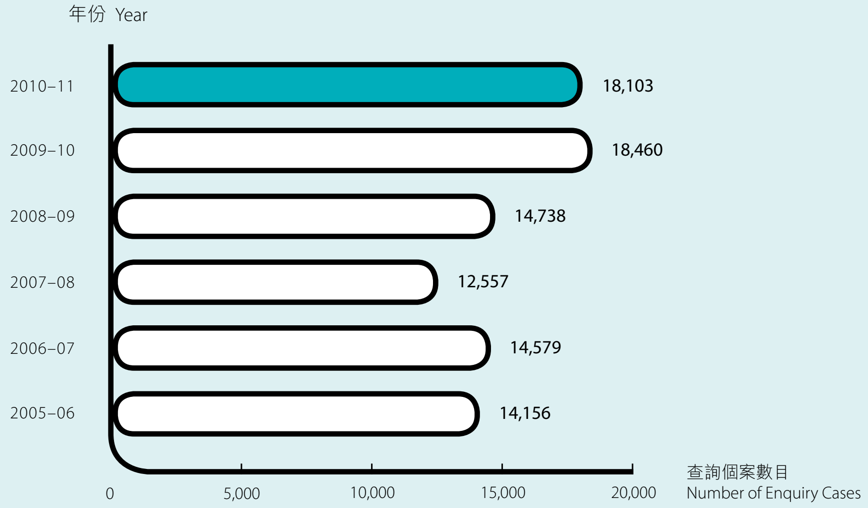
在二零一零至一一年度接獲的查詢
Enquiries Received during the Reporting Period

在本年度，公署共處理18,103宗查詢個案（較去年輕微下降2%），每日平均處理72宗。

A total of 18,103 enquiry cases were handled during the year (a slight decrease of 2% compared with the previous year). On average, 72 enquiry cases were handled each working day.

圖表 FIGURE 1

每年的查詢個案
Annual Enquiry Caseload



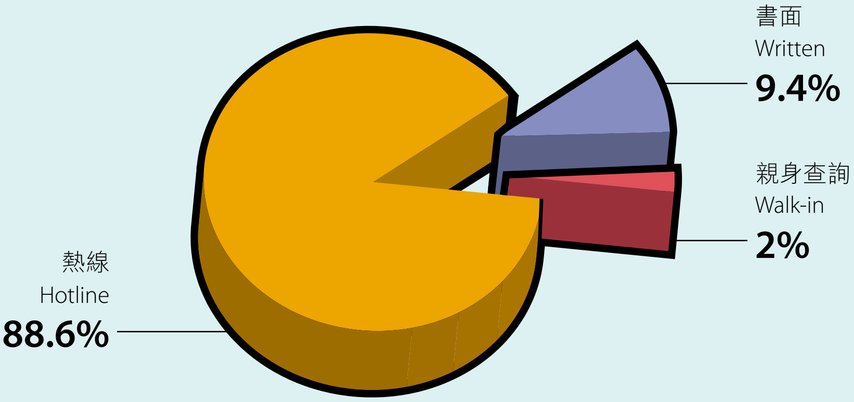
圖表 FIGURE 2

查詢個案的性質
Nature of Enquiry Cases

人力資源管理實務守則 Code of Practice on Human Resources Management	13%
僱主監察僱員活動 Workplace Surveillance	4%
生物辨識科技 Biometrics	1%
個人信貸資料實務守則 Code of Practice on Consumer-Credit Data	1%
直接促銷 Direct Marketing	8%
身份證號碼及其他身分代號實務守則 Code of Practice on Identity Card Numbers and other Personal Identifiers	6%
查閱資料要求 Data Access Requests	10%
追收債款 Debt Collection	2%
與互聯網有關 Internet-Related Issues	3%
其他 Others	52%

圖表 FIGURE 3

提出查詢的途徑
Means by Which Enquiries Were Made



大部分的查詢個案（約89%）是透過公署的查詢熱線電話2827 2827提出的。

The majority of enquiry cases (about 89%) were made via the PCPD hotline (2827 2827).

循規查察行動
Compliance Checks

發現某一機構的行事方式可能有違條例下的規定時，私隱專員便會展開循規查察行動。在此等情況下，私隱專員會以書面知會有關機構，指出看來與條例規定不符的事宜，並於適當時促請有關機構採取適當的糾正措施。

在大多數情況下，有關機構會主動採取即時措施，糾正涉嫌違例事項。在有些情況中，有關機構會就如何採取改善措施，以免重複涉嫌違例事項，向私隱專員尋求意見。在其他情況下，私隱專員會對涉嫌違例事項進行調查，並採取適當的跟進行動，確保有關機構遵從條例的規定（例如，向有關機構發出執行通知，指示它作出糾正）。

在年報期內，私隱專員共進行了129次循規查察行動，對資料使用者被指違反私隱條例下的規定的行事方式進行循規查察行動。

大部分循規查察行動（99次）是與私營機構的行事方式有關，其餘30次則關乎政府部門及法定機構。以下是在年內進行的循規查察行動的一些例子。

A compliance check is undertaken when the Commissioner identifies a practice in an organization that appears to be inconsistent with the requirements of the Ordinance. In these circumstances, the Commissioner alerts the organization in writing, pointing out the apparent inconsistency and inviting it, where appropriate, to take remedial action.

In many cases, the organization takes immediate action to correct the suspected breach. In some instances, advice is sought from the Commissioner on the measures that should be taken to prevent further breaches. In other cases, the Commissioner investigates the matter and takes action to ensure compliance with the Ordinance. This might include, for example, issuing an enforcement notice to the organization directing it to remedy the situation.

During the reporting year, the Commissioner carried out 129 compliance checks in total, in relation to alleged practices of data users that might be inconsistent with the requirements under the Ordinance.

The majority of the compliance checks (99) occurred in the private sector. The remaining 30 related to government departments and statutory bodies. The following examples highlight some of the compliance checks undertaken during the year.

例子
EXAMPLE
1

某政府部門職員出勤時遺失載有個人資料的文件
A staff member of a Government Department lost documents containing personal data when discharging outdoor duties.

2010年3月，一個政府部門（下稱「該部門」）向公署報告，指該部門一名職員在外執行職務時遺失了某些電腦打印文件，內載有126名個人的姓名、性別、地址及電話號碼。

公署進行循規查察中，該部門解釋該名職員在工作上確有需要將有關人士的姓名、地址及電話號碼帶離辦公室，以進行家訪。不過，該名職員在家訪當日只需探訪20名人士，因此該部門承認該名職員將超乎適度的個人資料帶離辦公室。

公署發現，雖然該部門有指引提醒職員不應將超乎適度的個人資料帶離辦公室，但有關指引沒有明確建議職員在離開辦公室進行家訪時應攜帶多少名人士的個人資料。

因應公署的關注，該部門其後發出書面指示，指令負責人員只可攜帶當日家訪服務所需要的個人資料離開辦公室。

In March 2010, a government department (the Department) reported to the PCPD that one of the Department's staff had lost certain computer printouts when he was carrying out outdoor duties. The lost printouts contained names, gender, addresses and telephone numbers of 126 individuals.

In the compliance check carried out by the PCPD, the Department explained that there was a genuine operational need for the staff member to take the individuals' names, addresses and telephone numbers off the office premises in order to conduct home visits. However, the Department admitted that the staff member had taken excessive personal data out of the office on the day of the home visits because the staff member was required to visit only 20 individuals.

The PCPD found that although Departmental guidelines included a general reminder that staff should not bring excessive personal data out of the office, the guidelines were not specific enough about the appropriate number of individuals whose personal data may be brought out of office when conducting home visits.

In response to the PCPD's concerns, the Department subsequently issued written instructions directing officers-in-charge to take only the personal data of service recipients that are required for conducting home visits on a particular date.

例子
EXAMPLE
2

某酒店將某客人的信用卡簽帳單給予另一客人以享用免費泊車服務

A hotel provided a customer's credit-card slip to another customer to claim free parking service.

某酒店向某客人提供一張信用卡簽帳單，讓他在附近一個商場免費泊車，但該客人發現該信用卡簽帳單並不屬於他本人，而是屬於另一名客人，而且該信用卡簽帳單內載了該另一名客人的姓名及完整的信用卡號碼。

在公署展開循規查察後，該酒店已停止向客人提供信用卡簽帳單以供客人享用免費泊車的優惠，改為向客人派發由該商場發出的「泊車券」。

該酒店亦接納公署的建議，停止在信用卡簽帳單上列印完整的信用卡號碼。

A hotel provided a credit-card slip to a customer to enable him to enjoy complimentary parking service at a nearby shopping mall. The customer found that the credit-card slip did not relate to his own bill, but to the bill of another customer, and contained the name and complete credit card number of that customer.

Upon commencement of the compliance check, the hotel ceased the practice of providing customers with a credit-card slip for complimentary parking service, and instead, started giving out parking coupons issued by the shopping mall.

The hotel also took the PCPD's advice and stopped printing the complete credit-card number on credit-card slips.

例子
EXAMPLE
3

某家庭傭工招聘公司在其櫥窗張貼超乎適度的菲律賓及印尼求職者的個人資料
A domestic-helper recruitment agency posted excessive personal data of job seekers from the Philippines and Indonesia on its shop window.

某間位於住宅大廈商場內的家庭傭工招聘公司在其櫥窗張貼菲律賓及印尼求職者的個人資料。該等個人資料包括求職者的全名、出生日期、婚姻狀況、住宅地址、護照號碼、星座、生肖、聯絡電話，以及其親屬的個人資料。

公署對該公司的做法展開循規查察。該公司解釋，張貼求職者的詳細資料是為了提高他們尋覓工作的機會。該公司補充，求職者在菲律賓及印尼的僱傭公司／培訓學校應已獲取求職者同意披露有關資料。不過，該公司承認他們沒有與有關海外公司或學校核實。

公署的初步意見認為，如此展示求職者的詳細資料可能構成違反保障資料第3及第4原則。該公司在知悉公署的初步意見後，向公署承諾，採取措施以確保在展示求職者的個人資料作求職用途前，會先取得求職者的同意，以及停止在櫥窗張貼求職者的全名、地址、出生日期、護照號碼、星座、生肖及其親屬的個人資料。

A domestic-helper recruitment agency in a shopping arcade in a residential building posted the personal data of job seekers from the Philippines and Indonesia on its shop window. The personal data included the full name, date of birth, marital status, home address, passport number, horoscope, Chinese zodiac and contact number of the job seekers, as well as personal particulars of their relatives.

The PCPD commenced a compliance check on the practice of the agency. The agency explained that the purpose of posting detailed information about the job seekers was to enhance their opportunity to find a job. The agency added that consent of the job seekers to such disclosure should have been obtained through the employment agencies/training schools in the Philippines and Indonesia. However, the agency admitted that it had not verified this with the overseas agencies or schools.

The PCPD expressed its preliminary view that display of such detailed information about job seekers might constitute a contravention of DPP 3 and DPP 4. Upon learning the preliminary view of the PCPD, the agency gave a written undertaking to the PCPD that it would implement measures to ensure prior consent was obtained from job seekers before displaying their personal data for employment purposes, and they would stop posting personal data such as full name, address, date of birth, passport number, horoscope, Chinese zodiac and personal data of relatives of job seekers on its shop window.

例子
EXAMPLE
4

載有1,497名客戶個人資料的電話帳單被置於街上無人看管
The telephone bills of 1,497 customers containing personal data were found unattended on the street.

2010年4月，警方向公署報告，在街上發現一批相信是由某電訊公司寄予客戶的信件。在公署進行的循規查察中，該電訊公司向公署確認該批信件共有1,497封，載有客戶的個人資料，包括姓名、地址及電話號碼的電話費帳單。

循規查察顯示，該公司的速遞服務承辦商的一名派遞員由於要離開晚膳，將該批信件放於街上，交托予一座大廈的保安員暫時代為看管，但該派遞員沒有回去取回信件。

該公司確認他們是有既定的的程序/指引規管承辦商如何派遞郵件。他們亦已向警方取回所有信件，並沒有迹象顯示信件曾被觸動。事發後，該公司向所有派遞人員發出通告，提醒並警告該承辦商，如再有類似事件發生，會撤銷派遞服務合約。

The Police reported to PCPD that letters believed to have been issued by a telecommunications company to its customers were found on the street in April 2010. In the compliance check carried out by the PCPD, the company confirmed to the PCPD that there were altogether 1,497 letters involved and that the contents were telephone bills containing personal data of its customers, including their names, addresses and telephone numbers.

It was revealed that the company had contracted delivery of the letters to a courier, whose employee, before leaving for dinner, had entrusted the letters to a security guard of a building on the street where the letters were later found, but the courier employee had failed to return to collect the letters.

The company confirmed that they had procedures/guidelines in place governing the delivery of mail by their contractors and had recovered from the Police all the letters, which showed no sign of having been tampered with. After the incident, the company issued a reminder notice to all of its delivery workers and warned the contractor at fault that its delivery service contract would be withdrawn if there were any further incidents.

例子
EXAMPLE
5

Google的街景拍攝車輛收集Wi-Fi網絡資料
Google Street View Car Collecting Wi-Fi Data

Google於2010年5月14日承認過去幾年Google的街景拍攝車輛在多個地點拍攝影像時，錯誤收集了可能載有個人資料而未被加密的Wi-Fi網絡資料（下稱「該等資料」）。Google解釋，街景拍攝車輛在運作時本應只記錄Wi-Fi站點的位置。公署因此於2010年5月17日對Google展開循規查察。

Google admitted on 14 May 2010 that it had mistakenly collected unencrypted Wi-Fi payload data which might have contained personal data (the Data) when taking pictures using the Google Street View Cars (SVC) in a number of locations in previous years. Google explained that only the locations of Wi-Fi stations should have been recorded during the operation. The PCPD commenced a compliance check against Google on 17 May 2010.

例子
EXAMPLE
5

Google的街景拍攝車輛收集Wi-Fi網絡資料
Google Street View Car Collecting Wi-Fi Data

Google與專員會面後，向專員簽署承諾書，承諾Google會停止街景拍攝車輛的運作，不會再收集Wi-Fi網絡資料或位置資料。Google亦承諾安全地儲存該等資料，並讓公署查閱該等資料，以進行循規查察。最後，Google答應就事件向公署提供獨立調查報告。

公署曾三次審視大部分該等資料。結果顯示Google只收集了少量的個人資料，且多數是零碎的。

2010年7月29日，Google向專員提供誓章，確認Google不知道或無意收集該等資料，以及它從來沒有使用、查閱或轉移該等資料。專員在循規查察期間亦沒有發現違反誓章的證據。

專員合理地信納該等資料沒有載有任何具意義的資料，可直接識別任何個人。

此外，專員沒有理由不相信Google的聲明：Google沒有意圖透過在香港的街景拍攝車輛匯集個人資料，及Google沒有查閱或使用該等資料。

循規查察報告的全文可瀏覽公署網頁(http://www.pcpd.org.hk/chinese/publications/files/Google_result_c.pdf)。

在公署視察Google的街景拍攝車輛，得悉沒有安裝收集Wi-Fi網絡資料的器材或軟件後，街景拍攝車輛於2011年1月恢復運作。公署會繼續與Google接觸，以確定其街景拍攝車輛的運作是否符合條例的規定及公眾的期望。

After meeting with the Commissioner, Google gave a written undertaking to the Commissioner to the effect that Google would cease operating SVC and that no Wi-Fi data, payload or locations would be collected by SVC again. Google also promised to securely store the Data collected and to allow the PCPD access to the Data for compliance checks. Finally, Google promised to provide the PCPD with a copy of an independent investigation report into the incident.

The PCPD examined most of the Data held by Google on three occasions. The results of the examination showed that only a minimal amount of personal data, often fragmented pieces, had been captured.

On 29 July 2010, Google provided a sworn statement to the Commissioner confirming that Google had no knowledge or intention to collect the Data and that it had never used, accessed or transferred the Data. The Commissioner found no evidence to contradict the statement during the compliance check.

The Commissioner was reasonably satisfied that the Data did not contain any meaningful details that could directly identify any one individual.

Furthermore, the Commissioner had no reason not to believe Google's assertion that Google had no intention of compiling personal information through the SVC operation in Hong Kong and that it had not accessed or used any of the Data.

A full report of the compliance check can be found on the PCPD website: http://www.pcpd.org.hk/english/publications/files/Google_result_e.pdf.

The SVC resumed its operation in January 2011 after PCPD had inspected the vehicle and found that no Wi-Fi data collection equipment or software had been installed. The PCPD is continuing its dialogue with Google to ascertain if its SVC operation is in compliance with the Ordinance and public expectation.

主動調查
PCPD-Initiated Investigations

如資料違規事件引起公眾極大關注，私隱專員可根據條例第38(b)條主動對事件作出調查，而無需等待投訴人提出投訴。此外，如在循規查察行動時發現有嚴重的違規情況，私隱專員亦會主動調查，以決定應否向有關的資料使用者發出執行通知，指令它改正某程序或採取適當的補救措施。

Where there is a data breach incident of great public concern, the Commissioner may initiate an investigation into the matter under Section 38(b) of the Ordinance without waiting for a complainant to come forward. Also, if a serious breach is found during a compliance check, a PCPD-initiated investigation will follow to determine whether an enforcement notice should be issued to the data user concerned requiring it to correct certain procedures or adopt appropriate remedial measures.

在本年度，私隱專員根據第38(b)條主動作出了10宗調查，其中包括調查八達通集團侵犯客戶資料私隱的事件，該集團的主要業務是營運智能卡付費系統。

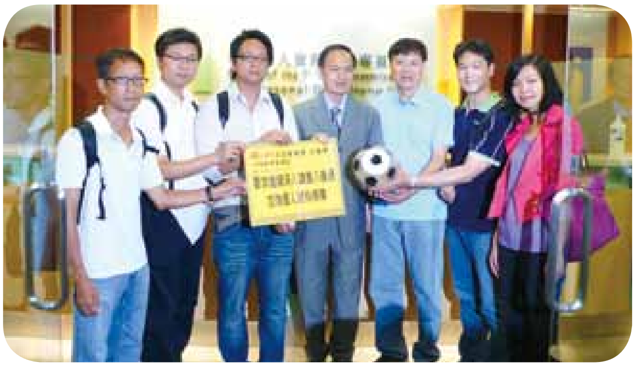
During the year under review, the Commissioner initiated 10 investigations under Section 38(b) of the Ordinance. This included investigation into a landmark privacy intrusion which concerned the use of customers' data held by the Octopus group of companies the core business of which is the operation of an extensive smartcard payment system.

收集及使用八達通日日賞計劃客戶的個人資料

在八達通獎賞有限公司(下稱「八達通獎賞公司」)營運的八達通日日賞計劃(下稱「該計劃」)下，會員用已登記的八達通卡向八達通的商業伙伴消費，可賺取日日賞$。已賺取的日日賞$可用作換取商業伙伴的貨品及服務。自2010年3月，該計劃的部分會員對於其個人資料在他們不知情或未同意的情況下被轉移予第三者作直接促銷，深表關注。其後，一名聲稱是該計劃的參與商戶的前僱員的人士，向傳媒及公署表示，八達通獎賞公司將該計劃的會員個人資料出售給該參與商戶，作直接促銷用途。

Collection and use of customers' personal data under the Octopus Rewards Programme

Octopus runs a Octopus Rewards Program (the Program) whereby registered members could earn Reward Dollars for making purchases from Octopus' business partners by presenting the Octopus smartcard. The Reward Dollars earned may be redeemed for goods and services from the business partners. Since March 2010, some members of the Program expressed concern about their personal data being transferred to third parties for direct marketing purposes without their knowledge or consent. Subsequently, an individual claiming to be a former employee of one of the business partners of the Program reported to the press and the PCPD that Octopus Rewards Limited (ORL) had sold the Program's customer personal data to the business partner for direct marketing purposes.



鑑於事件的嚴重性，私隱專員於2010年7月22日對八達通獎賞公司及其控股公司 — 八達通控股有限公司(下稱「八達通控股」))展開調查，並根據條例第43條行使其權力，對他們及其商業伙伴的要員進行公眾聆訊。

完成調查後，私隱專員認為八達通獎賞公司在收集及使用客戶的個人資料的過程中，違反了條例保障資料第1(1)原則、第1(3)原則及第3原則的規定。

私隱專員認為八達通獎賞公司為認證客戶身份目的而收集的個人資料收集身份證號碼、護照號碼、出生證明書號碼，以及出生年月是超乎適度及違反了保障資料第1(1)原則的規定。八達通獎賞公司使用所收集的其他侵犯私隱程度較低的資料(例如電話號碼及住址)，也可達到同樣目的。

私隱專員亦認為收集個人資料聲明使用細小的字體，且未合理地定出個人資料承讓人的類別，是違反了保障資料第1(3)原則的規定。

至於八達通獎賞公司在銷售個人資料予其合作商戶一事上，私隱專員認為該計劃的收集個人資料聲明沒有説明會銷售客戶個人資料，也沒有得到客戶的同意。雖然八達通獎賞公司出售個人資料沒有受條例禁止，但這不能被視為原本的收集目的或直接有關的目的。八達通獎賞公司因而違反了保障資料第3原則的規定。

私隱專員注意到八達通控股已公開聲明不會參與任何須向夥伴商戶提供客戶個人資料以作促銷用途的活動，並暫停登記新會員。此外，八達通獎賞公司向私隱專員書面承諾(a)徹底刪除及銷毀過量收集得來的個人資料(b)徹底刪除及銷毀為獲得金錢收益而向5間夥伴商戶轉移的客戶個人資料(c)重新設計收集個人資料聲明的描述和展示，讓一般正常視力的人士可

In view of the seriousness of the allegations, the Commissioner commenced investigations against ORL and its holding company, Octopus Holdings Limited (OHL) on 22 July 2010 and, in connection with this, conducted a public hearing by exercising his power under Section 43 of the Ordinance to examine the principal officers of ORL, OHL and their business partners.

Upon completion of the investigations, the Commissioner found that ORL had, in the processes of collection and use of members' personal data, contravened Data Protection Principles (DPP) 1(1), DPP 1(3) and DPP 3.

The Commissioner found that the collection of Hong Kong identity card number/passport number/birth certificate number, and month and year of birth for the purpose of customer authentication was excessive and in contravention of DPP 1(1). ORL could have achieved the same purpose by using other less privacy-intrusive data (such as telephone numbers and home addresses) it had also collected.

The Commissioner also found that through the use of small print in the Personal Information Collection Statement (PICS) and the failure to define in any reasonable degree of certainty the classes of data transferees, ORL had contravened DPP 1(3).

With regard to ORL's sale of its customers' personal data to its business partners, the Commissioner found that the sale was not stated in the PICS, nor was it consented to by ORL's customers. Although sale of personal data by ORL was not prohibited by the Ordinance, it could not be regarded as the original purpose of data collection or as a directly related purpose. ORL, therefore, contravened DPP3.

The Commissioner noted that OHL had publicly announced that it would no longer participate in any further activities that require the provision of customer personal data to its merchant partners for marketing purposes and that it had suspended the registration of new members. Further, the Commissioner obtained a written undertaking from ORL to the effect that (a) excessive personal data collected would be completely erased and destroyed; (b) customers' personal data transferred to the five business partners concerned for monetary gain

易於細讀（d）按其獨特性質來列出資料承讓人的類別，讓人以合理的程度了解個人資料會被移轉予甚麼人，以及（e）日後如要轉移現有的客戶的個人資料予該計劃下的參與商戶作金錢收益，必須取得客戶的明確及自願同意。

鑑於八達通獎賞公司已停止引致有關違反的作為，並作出有關書面承諾，私隱專員認為持續或重複違反行為的機會不大，所以沒有發出執行通知。

在總結調查時，私隱專員就涉及直接促銷產品和服務的資料使用者和有關各方的做法作出下述評論及建議，以促進對條例的遵守：

（1） 企業在收集及使用顧客的個人資料時，不可利用其相對於顧客而言較主導的地位而收集及使用顧客的個人資料。他們所從事的任何非常規行為將不合比例地削弱企業的誠信，及損毀其聲譽。

（2） 雖然條例並無規定在收集資料時須使用「接受服務」方式，但私隱專員亦認為「接受服務」方式可為個別人士提供更進一步的資料私隱保護。

（3） 企業不應收集超乎適度個人資料。尤其是香港身分證號碼屬敏感資料，應特別小心處理，以確保其收集屬必需。

（4） 為確保收集個人資料聲明有效，資料使用者應考慮的因素包括收集個人資料聲明的的描述和展示、所使用的語言，及向資料當事人提供進一步支援。

would be erased and destroyed; (c) the layout and presentation of the Personal Information Collection Statement would be re-designed to make it easily readable to people with normal eyesight; (d) classes of data transferees would be specified by distinctive features in order to provide a reasonable degree of certainty as to whom the personal data would be transferred; and (e) in future, express and voluntary consent would be obtained from existing customers before their personal data would be transferred to ORL's business partners for monetary gain.

Given the cessation of the practice giving rise to the contraventions and the written undertaking by ORL, the Commissioner considered that recurrence of the contravention was unlikely. In the circumstances, no enforcement notice was served on OHL or ORL.

In concluding the investigations, the Commissioner made the following comments and recommendations on the practice of data users and associated parties involved in direct marketing of products and services in order to promote compliance with the provisions of the Ordinance:-

(1) Enterprises should not exploit their dominant position vis-à-vis their customers in the collection and use of personal data. Any irregularities on their part would jeopardize their credibility and damage their reputation disproportionately.

(2) Although there is no requirement for "opt-in" at the data collection stage under the Ordinance, the Commissioner considers that "opt-in" would definitely afford better data privacy protection for individuals.

(3) Enterprises should not collect excessive personal data, in particular that Hong Kong Identity Card number is sensitive information and extra care should be exercised to ensure its collection is necessary.

(4) To ensure that a Personal Information Collection Statement ("PICS") is effective, data user should consider factors including the layout and presentation of, and the languages used in the PICS and the availability of further assistance to data subject.

（5） 資料使用者不應以寬鬆及模糊的條款，就使用目的及承讓人的類別作出定義，致令資料當事人實際上無法合理地確定他們的個人資料的會如何被使用及可使用該資料的人士。

（6） 如資料使用者打算向第三方出售其客戶資料而獲金錢收益，而此舉並非收集資料時的原本目的或直接相關目的，則必須向客戶尋求明示及自願的同意。

（7） 轉移資料的公司只應轉移用於進行議定的跨業直銷活動的個人資料。通常被轉移的資料只限於聯絡資料，讓夥伴公司能夠接觸客戶。

（8） 打算將個人資料轉移給第三方的資料使用者前，應對該等第三方進行評估，確保他們採取足夠的措施，保障轉移給他們的個人資料。

（9） 資料使用者把客戶的個人資料交託第三者處理時，建議的良好行事方式是，資料使用者定期進行審核或檢討，確保資料承轉人已採取適當的資料保障措施，遵從條例的規定。

（10）資料使用者不應使用欺騙或誤導的方法收集個人資料作直接促銷。例如，甲公司以乙公司名義促銷甲公司的產品／服務，接聽電話的人誤以為是乙公司在直接促銷乙公司的產品／服務，而基於這信賴，接聽電話的人在交易過程中提供了相關的個人資料。

(5) Data users should not define the purpose of use and class of data transferees in liberal and vague terms which would not be practicable for data subjects to ascertain with a reasonable degree of certainty how their personal data could be used and who could have the use of the data.

(6) Express and voluntary consent must be sought from the customer if a data user intends to sell its customer data to third parties for monetary gains and this is not the original purpose or directly related purpose for which the data were to be used at the time of data collection.

(7) Only the personal data used for the purpose of the agreed cross-marketing activities should be transferred by the transferor company. Typically, the data to be transferred should be confined to contact data, which enable the partner company to approach the customer.

(8) Data users who intend to transfer personal data to third parties for processing should conduct appropriate assessment of the third parties to ensure that they would provide adequate measures to protect the personal data transferred to them.

(9) When customers' personal data are entrusted to a third party for handling, it is recommended good practice that the data user shall undertake compliance audits or reviews regularly to ensure that the transferees of the data have taken appropriate data protection measures in compliance with the Ordinance.

(10) Data user should not use deceptive or misleading means to collect personal data for direct marketing. An example is where Company A holds itself out to be Company B in promoting the product/service of Company A in circumstances that the called party was misled to believe that it was Company B which was making the direct marketing approach for promoting Company B's product/service and it was based on such reliance that the called party's relevant personal data were provided in the course of transaction.

八達通完全漠視私隱及資料保障，對其影響是十分嚴重。事件所引起的公憤直到該公司採取連串補救行動才得以平息。有關行動包括：

（1） 該公司接納私隱專員及其他規管者有關加強營運程序以保障個人資料的所有建議。

（2） 該公司承諾加強企業及資料管理架構。

（3） 該公司將從轉移資料予第三者所賺取的總收入，即五千七百九十萬港元，捐贈公益金。

（4） 該公司承諾會專注於核心業務，向客戶提供智能卡服務，作為方便的電子付款途徑，及不會再參與向商業伙伴提供客戶個人資料作促銷的活動。

巧合地，該公司的行政總裁在私隱專員完成調查前突然離職，而其董事會主席在私隱專員公布調查報告後翌日亦宣布退休（據稱是公司正常接班計劃的一部分）。

說八達通事件把公眾對個人資料私隱權利的意識及了解推至前所未有的高水平，或許不算誇張。很多企業一定已經知道私隱違規對聲譽帶來的風險非常高，他們在企業管治中絕不能忽視私隱議題。

The effects on Octopus for its outright failure to observe privacy and data protection were detrimental. The public outcry that it has generated did not subside until it has taken a series of drastic remedial actions which included: -

(1) It accepted all the Commissioner's recommendations and those of other regulators as regards tightening up of operational procedures for personal data protection.

(2) It pledged to strengthen its corporate and data governance structure.

(3) It donated the total amount of revenue generated by its data transfer to third parties, viz. HK$57.9 million, to the Community Chest.

(4) It pledged that it would focus its core business on providing smart card services to customers as a convenient electronic means for payment, and it would no longer participate in any further activities that require the provision of customer personal data to merchant partners for marketing purposes.

Coincidentally, its CEO resigned abruptly before the Commissioner completed his investigations, and its board chairman also announced his retirement (purportedly as part of a natural succession plan) on the day following the Commissioner's publication of the investigation report.

It is perhaps no exaggeration to say that the Octopus incident has brought public awareness and understanding of their privacy rights over personal data to an unprecedentedly high level. Many enterprises must have realized that the reputational risks associated with privacy contraventions are so high that they can ill afford to ignore privacy issues in their corporate governance.

智能身份證系統的私隱循規評估

政府自2003年起經入境事務處（下稱「入境處」）簽發智能身份證。為確保入境處持有的所有個人資料是根據私隱條例而處理，政府向立法會承諾會要求私隱專員對智能身份證系統進行私隱循規評估。

私隱循規評估旨在評估入境處依從私隱條例規定的程度、識別入境處資料保障系統的潛在弱點，及提供檢討入境處資料保障系統的建議。私隱循規評估已經完成，私隱專員於2010年7月30日發出私隱循規評估報告。

私隱專員在該私隱循規評估報告對智能身份證系統作出的評論及建議包括：

（1） 入境處應就智能身份證資料的保安類別提供更具體的指引，方法是修訂現有的指引，列明保密資料及相關的保安規定；修改系統手冊，列明資料的分類及相當處理程序；以及進行培訓及提高意識的計劃，確保所有智能身份證系統的使用者熟悉智能身份證資料的分類及保障規定。

（2） 入境處應修訂身份證申請表上的目的聲明，加入資料當事人不提供其個人資料的後果。

（3） 入境處應向負責檢討的人士提供更具體、有效及一致的審核追蹤檢討指引，讓他們定期進行有效檢查，以識別不當的查閱權及未經准許的查閱。

（4） 入境處應進行提高意識的計劃，確保所有負責處理查閱資料要求及改正資料要求的職員熟悉相關指引。

Privacy Compliance Assessment on the Smart Identity Card System (SMARTICS)

The Government through the Immigration Department ("ImmD") has been issuing smart identity cards since 2003. To ensure that all personal data held by the ImmD are handled in accordance with the requirements under the Ordinance, the Government had undertaken to the Legislative Council that it would ask the Commissioner to conduct a Privacy Compliance Assessment ("PCA") on the Smart Identity Card System.

The purpose of the PCA is to assess ImmD's level of compliance with the requirements under the Ordinance, to identify potential weaknesses in ImmD's data protection system, and to provide recommendations to ImmD for a review of its data protection system. The PCA was completed and the Commissioner published the PCA Report on 30 July 2010.

Comments and recommendations on the Smart Identity Card System made by the Commissioner in the PCA Report include:-

(1) ImmD should provide more specific guidelines on the security classification of the Smart Identity Card data by amending their existing guidelines to describe the confidential information and the corresponding security requirements, revising the system manuals to document the classification of information and relevant handling procedures, and conducting training and awareness programme to ensure all SMARTICS users are familiar with the classification of the Smart Identity Card data and their protection requirements.

(2) ImmD should amend the statement of purpose in its identity card application form to include the consequences for a data subject if he fails to supply his personal data.

(3) More specifically, effective and consistent audit trail review guidelines should be provided to reviewers so that they can routinely conduct effective checks for identifying inappropriate access rights and unauthorized access.

(4) ImmD should conduct awareness programmes to ensure that all staff members responsible for handling data assess request and data correction request are familiar with relevant guidelines.

對環聯資訊有限公司的視察
Inspection on TransUnion Limited

根據條例第36條，私隱專員有權對個人資料系統進行視察。其目的在確定資訊以協助私隱專員向有關的資料使用者或一個類別的資料使用者作出建議。

條例下的個人信貸資料實務守則（下稱「守則」）規管香港的信貸資料機構及信貸提供者對個人信貸資料的處理。該守則涵蓋資料的收集、準確性、使用、保安，以及查閱及改正資料要求等方面的問題，這些問題與目前是或曾是個人信貸申請者的人士的個人資料有關。環聯資訊有限公司（下稱「環聯」）是本港主要信貸資料機構，管有約430萬個人信貸記錄，是信貸提供者的個人信貸資料的主要來源。

由於環聯持有大量個人信貸資料，這些敏感資料一旦處理不善，可能對個別人士造成嚴重不利影響，私隱專員因此於2010年3月31日對於環聯使用的個人資料系統進行視察。

視察涵蓋環聯的個人資料系統中整個資料處理程序，以確定是否符合六個保障資料原則及守則的建議。視察工作包括政策及指引的檢視、資料庫系統的運作查驗 、環聯員工及客戶的會面及實地考察。

私隱專員很高興發現環聯在妥善處理個人信貸資料方面制定了全面及詳盡的政策、指引及程序，而這次視察並無發現任何重大資料保安問題。不過，有些地方仍有改善空間，私隱專員就此向環聯提出20項建議，以增強環聯在資料收集、準確性、保留、保安及查閱，以及資訊科技保安審查等方面的控制系統。

私隱專員於2011年3月15日發表對環聯個人資料系統進行視察的報告。報告的全文可以從公署網站（http://www.pcpd.org.hk/chinese/publications/files/R11_3803_c.pdf）下載。

Inspection of a personal-data system is a power exercisable by the Commissioner under Section 36 of the Ordinance. The purpose of such inspections is to ascertain information to assist the Commissioner in making recommendations to the data user or class of data users.

The Code of Practice on Consumer Credit Data (the Code) under the Ordinance regulates the processing of consumer credit data by credit reference agencies (CRA) and credit providers in Hong Kong. It deals with the collection, accuracy, use, security, access and correction of personal data of individuals who are, or have been, applicants for consumer credit. TransUnion Limited (TU) is a major CRA in Hong Kong, maintaining credit records of about 4.3 million individuals and is the major source of consumer credit information for credit providers.

Given the vast amount of consumer credit data being held by TU and the serious adverse impact it may have on individual consumers if these sensitive data are mishandled, the Commissioner commenced an inspection of the personal-data system used by TU on 31 March 2010.

The inspection covered the entire data processing cycle of the personal data system of TU to ascertain compliance with the six Data Protection Principles (DPPs) and the Code. The inspection work included a review of policies and guidelines, interaction queries with the database system, interviews with TU staff and customers, and on-site inspection.

The Commissioner was pleased to find that TU had in place comprehensive and detailed policies, guidelines and procedures on the proper handling of consumer credit data, and that no major data-security issues had been found in the inspection. The inspection did, however, find room for improvement, and the Commissioner made 20 recommendations for TU to enhance its system of control in the areas of data collection, accuracy, retention, security and access, as well as in its IT security audit.

On 15 March 2011, the Commissioner published his report on the inspection of TU's personal-data system. A full version of the report is available for download from the PCPD website: http://www.pcpd.org.hk/english/publications/files/R11_3803_e.pdf.

核對程序
Matching Procedures

在本年報期內，私隱專員共收到20宗核對程序申請，全部來自公營機構。

During the reporting year, the Commissioner received 20 applications for approval to carry out matching procedures. All of the applications came from public sector organisations.

經審閱後，私隱專員根據條例賦予的權力，在有條件的情況下批准7宗申請。3宗申請其後被撤回。私隱專員在考慮了核對程序的定義及條例下的訂明事宜後，拒絕了7宗申請。截至2011年3月31日，餘下3宗申請正由私隱專員考慮。

Upon examination, seven applications were approved subject to conditions imposed by the Commissioner under the Ordinance. Three were subsequently withdrawn and seven were refused by the Commissioner, after taking into consideration the definition of the matching procedures and the prescribed matters under the Ordinance. As at 31 March 2011, the remaining three applications were under the consideration of the Commissioner.

以下為部份核准的核對程序個案：

The following are some of the matching procedures that were approved by the Commissioner:

提出要求者 Requesting Parties	獲准的有關核對程序 Related Matching Procedures that were Approved
社會福利署 Social Welfare Department	公署同意社會福利署進行核對程序，將社會福利署所收集的個人資料與教育局所持有的個人資料互相比較，以避免正在教育局轄下的特殊學校接受照顧的綜合社會保障援助／公共福利金計劃下的高額傷殘津貼受益人獲得雙重津貼的情況。 Consent was given to the Social Welfare Department to carry out a matching procedure to compare personal data collected by the Social Welfare Department with personal data kept by the Education Bureau to prevent double benefits being released to recipients of the Comprehensive Social Security Assistance Scheme/Higher Disability Allowance under the Social Security Allowance who are also receiving care in a special school under the Education Bureau.
房屋協會 Hong Kong Housing Society	公署同意房屋協會進行核對程序，將市區重建局、屋宇署與房屋委員會就「樓宇更新大行動」資助計劃所收集的個人資料互相比較，以避免有人獲得雙重津貼的情況。 Consent was given to the Hong Kong Housing Society to carry out a matching procedure to prevent double benefits in respect of Operation Building Bright, by comparing personal data collected by the Urban Renewal Authority, Buildings Departments and Housing Authority.
入境事務處 Immigration Department	公署同意入境事務處進行核對程序，將部門宿舍申請人的個人資料與房屋委員會為提供公共房屋而保存的個人資料互相比較，以避免有人獲得雙重房屋津貼的情況。 Consent was given to the Immigration Department to carry out a matching procedure to prevent double housing benefits, by comparing the personal data of applicants for the departmental quarters with personal data kept by the Housing Authority for the provision of public housing.
選舉事務處 Registration and Electoral Office	公署同意選舉事務處進行核對程序，將選舉事務處保存的個人資料與房屋協會所保存的個人資料互相比較，以確保選民登記冊準確。 Consent was given to Registration and Electoral Office to carry out a matching procedure to ensure the accuracy of the Register of Electors by comparing personal data kept by the Registration and Electoral Office with personal data kept by the Hong Kong Housing Society.