提倡私隱保障納入企業管治

Promoting Privacy Protection as Corporate Governance

從符規躍升為問責
From Compliance to Accountability

審查及政策部不只監察和推動資料使用者要循規以符合條例的規定，更鼓勵機構從符規躍升為問責，把資料保障納入為企業管治的重要一環。

The Compliance and Policy Division monitors and promotes compliance with the provisions of the Ordinance. We encourage organisations to take a step forward, making the shift from compliance to accountability, and to embrace personal data protection as an integral part of their corporate governance.

審查及政策部
Compliance & Policy Division

資訊科技部
Information Technology Division


From Compliance to Accountability
Privacy Management Programme
PLEDGE CEREMONY
ACE Life
FWD 富衛
QBE
TRANSAMERICA
HKT
CLP 中電
RSA
中國移動 China Mobile
新世界傳動網
煤氣 Towngas
HKFi
中国太平 CHINA TAIPING
Liberty Insurance
CMMobile 漫遊移動
SmarTone
港燈 HK Electric
CAHK
Cigna
MassMutual
Swiss Re
Telecom Digital 電訊數碼
HOSPITAL AUTHORITY
大新保險 TAISANG INSURANCE
Hutchison Telecom Hong Kong
八達通 OCTOPUS

私隱管理系統

鑑於公眾對保障個人資料私隱的期望與日俱增，而大數據帶來更高的潛在私隱風險，私隱專員提倡機構應把個人資料和私隱保障納入為企業管治責任不可或缺的一環，並且由上而下貫徹地在機構中執行，而不止於停留在依循法律規定的層次。這需要企業管治的概念由「符規」躍升為「問責」，並制定及實施全面的私隱管理系統。

在私隱及資料保障方面，普遍現象是欠缺機構最高管理層的參與。這方面的事宜一般只交由法律及循規人員負責，以致企業只管符合條例的最低要求。私隱專員認為作為負責任的企業，機構應從較宏觀的管理角度考慮私隱事宜，並考慮企業聲譽及尊重顧客或客戶基本權利這些因素。

公署在過去一年與香港特區政府、香港保險業協會、香港通訊業聯會及香港銀行公會等機構合作，倡導業界內的機構推行私隱管理系統。截至 2014 年 2 月 18 日為止，特區政府（包括所有決策局和部門）、2 5 間保險公司、九間電訊公司和五間其他行業的機構（名單見圖 2.1）承諾在機構內推行私隱管理系統。私隱專員期望推行私隱管理系統的機構履行承諾，為其他資料使用者樹立良好榜樣。

香港銀行公會雖然未有參與承諾，但表示銀行業支持以自願性質推展的私隱管理系統，個別銀行亦會因應其各自的私隱保障管理框架，採取所需措施以落實私隱管理系統的原則。

PRIVACY MANAGEMENT PROGRAMME

In response to rising public expectations for privacy protection, along with increased privacy risks brought about by the era of Big Data, the Commissioner has been advocating that organisations should make personal data protection part of their corporate governance responsibilities and implement it throughout their organisations using a top-down approach. This calls for a paradigm shift from compliance to accountability, and the formulation and maintenance of a comprehensive privacy management programme ("PMP").

On matters of privacy and data protection, it is not uncommon for top management to be seldom involved, if at all. The issue is often relegated to the legal and compliance staff. This often leads to the adoption of a minimalist approach focused on just meeting the basic legal requirements set out in the Ordinance. The Commissioner submits that organisations, as responsible corporate citizens, should consider privacy from a broader management perspective and take into account factors such as corporate reputation and respect for the basic rights of their customers or clients.

Over the past year, the PCPD has been working with the HKSAR Government, the Hong Kong Federation of Insurers, the Communications Association of Hong Kong, and the Hong Kong Association of Banks to advocate the implementation of an accountability-based PMP in the sectors concerned. As at 18 February 2014, the following organisations (figure 2.1) had pledged to implement a PMP: the HKSAR Government (including all bureaux and departments), 25 insurance companies, nine telecommunications companies and five organisations from other sectors. The Commissioner looks forward to these organisations fulfilling their pledges, thus setting an example of responsible privacy management for other data users to follow.

Although the Hong Kong Association of Banks did not join the pledge, it has indicated to the PCPD that the banking industry supported the voluntary PMP and that individual banks would take the necessary steps, having regard to their own privacy protection frameworks, to implement the PMP principles.

圖 2.1

承諾推行私隱管理系統的機構（按英文名稱順序排列）：

香港特別行政區政府
所有決策局及部門

保險業
安達人壽保險有限公司
友邦保險（國際）有限公司
安盛保險（百慕達）有限公司
安盛保險有限公司
中國太平保險（香港）有限公司
信諾環球保險有限公司
信諾環球人壽保險有限公司
大新保險（1976）有限公司
富衛保險有限公司
富衛人壽保險（百慕達）有限公司
豐隆保險（亞洲）有限公司
利寶國際保險有限公司
美國萬通保險亞洲有限公司
民安財產保險有限公司香港分公司

保誠保險有限公司
保誠財險有限公司
昆士蘭保險（香港）有限公司
昆士蘭聯保保險有限公司
昆士蘭按揭保險（亞洲）有限公司
RGA 美國再保險公司
皇家太陽聯合保險有限公司
香港永明金融有限公司
瑞士再保險有限公司（香港分公司）
東京海上火災保險（香港）有限公司
全美人壽百慕達

電訊業
中國移動香港有限公司
潤迅通信（香港）有限公司
香港移動通訊有限公司
香港電訊有限公司
和記電訊（香港）有限公司
新世界傳動網有限公司
數碼通電訊有限公司
電訊數碼控股有限公司
九倉電訊有限公司

其他行業
中電控股有限公司
香港中華煤氣有限公司
香港電燈有限公司
醫院管理局
八達通控股有限公司

Figure 2.1

Organisations which have made the pledge to implement a PMP (listed in alphabetical order):

Hong Kong Special Administrative Region Government
All bureaux and departments

Insurance sector
ACE Life Insurance Company Limited
AIA International Limited
AXA China Region Insurance Company (Bermuda) Limited
AXA General Insurance Hong Kong Limited
China Taiping Insurance (HK) Company Limited
Cigna Worldwide General Insurance Company Limited
Cigna Worldwide Life Insurance Company Limited
Dah Sing Insurance Company (1976) Limited
FWD General Insurance Company Limited
FWD Life Insurance Company (Bermuda) Limited
Hong Leong Insurance (Asia) Limited
Liberty International Insurance Limited
MassMutual Asia Limited
Minan Property And Casualty Insurance Company Limited, Hong Kong Branch
Prudential Hong Kong Limited
Prudential General Insurance Hong Kong Limited
QBE General Insurance (Hong Kong) Limited
QBE Hongkong & Shanghai Insurance Limited
QBE Mortgage Insurance (Asia) Limited
RGA Reinsurance Company
Royal & Sun Alliance Insurance plc
Sun Life Hong Kong Limited
Swiss Reinsurance Company Limited, Hong Kong Branch
The Tokio Marine & Fire Insurance Company (HK) Limited
Transamerica Life (Bermuda) Limited

Telecommunications sector
China Mobile Hong Kong Company Limited
China Motion Telecom (HK) Limited
CSL Limited
Hong Kong Telecommunications (HKT) Limited
Hutchison Telecommunications (Hong Kong) Limited
New World Mobility Limited
SmarTone Mobile Communications Limited
Telecom Digital Holdings Limited
Wharf T&T Limited

Other sectors
CLP Holdings Limited
The Hong Kong and China Gas Company Limited
The Hongkong Electric Company, Limited
Hospital Authority
Octopus Holdings Limited

在 2014 年 2 月 18 日舉行的推展儀式上，香港特別行政區政府與 39 間來自保險業、電訊業及其他行業的機構承諾推行私隱管理系統。
The HKSAR Government and 39 organisations from the insurance, telecommunications and other sectors pledged to implement PMP at the Pledge Ceremony held on 18 February 2014.

私隱管理系統 Privacy Management Programme

何謂私隱管理系統？

私隱管理系統本身並不是《個人資料（私隱）條例》（「條例」）下的規定。最低限度，私隱管理系統的策略框架有助機構達致符合法律要求和管理私隱風險的目標。更廣義來說，穩妥的私隱管理系統基建應具備以下特點：

- 得到機構最高管理層的決心支持，並成為機構管治架構不可或缺的一環；
- 視私隱和個人資料保障為跨部門的事務，並特別著眼於尊重客戶的需要、要求，權利和期望；
- 制定政策、程序和常規，以符合條例規定；
- 參照私隱風險評估的結果來制訂適當的防範措施；
- 確保所有措施、項目和服務都顧及保障私隱；
- 設立資料外洩或個人資料私隱事故的應變機制；
- 設立內部的監督和檢討機制；
- 能夠有效地回應私隱生態系統的迅速變化，保持實用，與時並進；及
- 有適當的資源配合和專責人員管理。

What is PMP?

PMP is not a legal requirement under the Personal Data (Privacy) Ordinance ("the Ordinance"). At the minimum, PMP serves as a strategic framework to assist an organisation in complying with legal requirements of the Ordinance, as well as privacy risk management. In a broader sense, PMP should be a robust privacy infrastructure that:–

- has top management commitment and is integrated into the organisation's governance structure;
- treats privacy and data protection as a multi-disciplinary issue, with a special focus on respect for customer or client needs, wants, rights and expectations;
- establishes policies, procedures and practices giving effect to the legal requirements under the Ordinance;
- provides for appropriate safeguards based on privacy risk assessment;
- ensures that privacy is built into all initiatives, programmes and services;
- includes contingency plans for responding to breaches and other incidents;
- includes internal oversight and review mechanisms;
- is kept current and relevant, and remains practical and effective in a rapidly changing privacy eco-system; and
- is appropriately resourced and managed by dedicated staff.

私隱管理系統最佳行事方式指引

公署於 2014 年 2 月出版《私隱管理系統最佳行事方式指引》（「指引」）。指引扼述私隱管理系統的必需組件，並提供原則性及指導性的建議，協助機構因應各自的規模、業務性質，收集及處理個人資料的數量和敏感程度等，建立和優化其私隱管理系統。

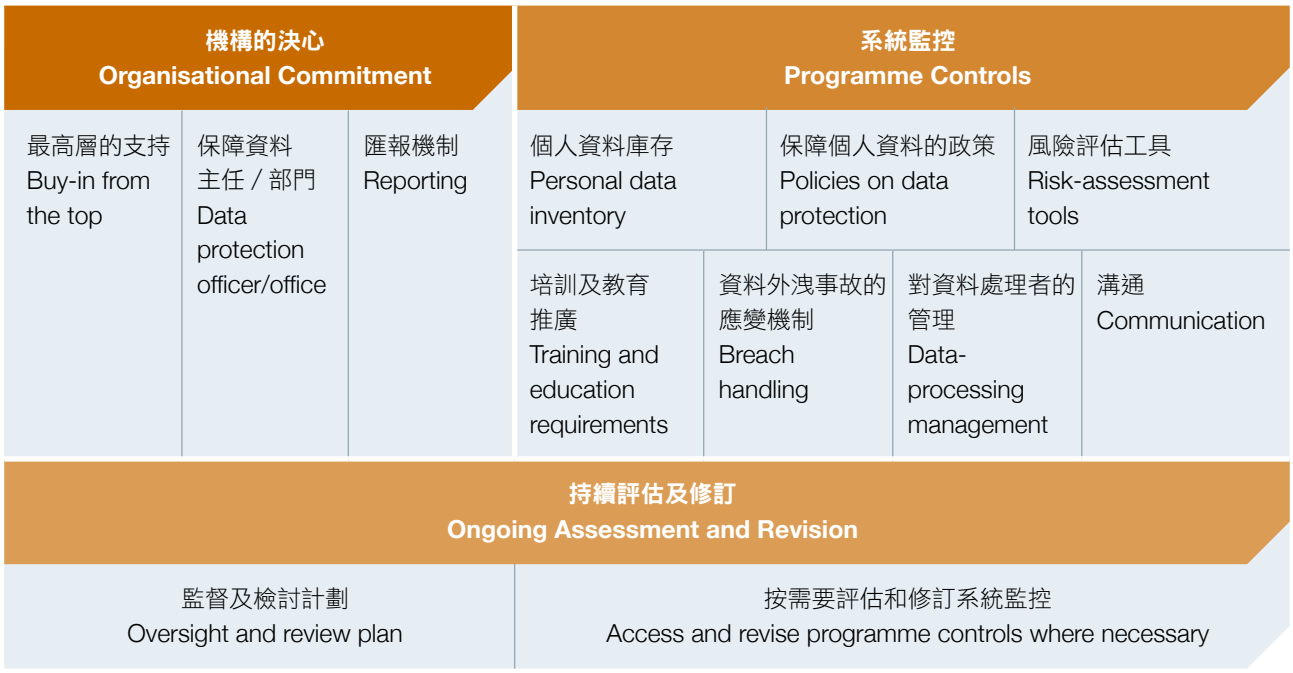
這份指引扼述如何建立私隱專員所提倡的穩健私隱管理系統。機構的決心和系統監控都是必備元素。指引亦討論如何維繫及持續地改進私隱管理系統。機構不應視建立私隱管理系統為一勞永逸的工作；系統需要持續的評估及調整，以確保有效及與時並進。機構應定期監察、評估及更新系統的組件，以配合機構內外諸如科技、業務模式、法例及最佳行事方式等各方面的轉變。

PMP: A Best Practice Guide

In February 2014, the PCPD released a guide entitled *Privacy Management Programme*: *A Best Practice Guide* ("the Guide"). The Guide outlines the building blocks of a PMP. It provides guidance to organisations for developing and improving their own programmes according to their specific circumstances, such as organisation size, nature of business, and the amount and sensitivity of the personal data they collect and manage.

The Guide outlines what the Commissioner advocates as good approaches for developing a sound PMP, emphasising the importance of elements such as organisational commitment and programme controls. It also discusses how to maintain and improve a PMP on an ongoing basis. A PMP should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The components should be regularly monitored, assessed and updated as necessary to keep pace with changes both within and outside the organisation. This may encompass changes in such areas as technology, business models, law and best practices.

私隱管理系統的組件
Building blocks of PMP



在機構建立私隱管理系統，需要慎密的策劃和跨部門、跨職能的考慮。員工應知悉和瞭解適用於其機構的私隱管理系統；機構應告知客戶及業務夥伴其私隱管理系統中有哪些部分與他們相關，並保證會付諸實行。機構在推出新產品或服務前，往往要制定業務模式及擬備技術和業務常規，過程中應確立和適當地考慮保障私隱方面的責任及風險。機構應設法減低資料外洩的可能；一旦外洩資料的事故發生，應把事故的影響減至最低。

Constructing a PMP within an organisation takes careful planning and consideration across all disciplines and job functions. Employees should be aware of and understand the applicable parts of the organisation's PMP. Customers and business partners should likewise be made aware of and given assurance, where appropriate, about the relevant aspects of the PMP. Privacy-related obligations and risks should be correctly identified and appropriately taken into account when developing business models, related technologies and business practices before new products or services are launched. Risks of data breaches should be minimised and the effects of any data breaches should be mitigated.

推行得宜　加強競爭優勢

若機構只視個人資料私隱保障為循規的法律事宜，是不足夠的。面對大數據年代和公眾對私隱保障的期望與日俱增，機構應該採取積極進取及防患未然的措施，而非被動的回應或亡羊補牢。機構應把個人資料和私隱保障納入為企業管治責任不可或缺的一環，並且由上而下貫徹地在機構中執行。私隱保障策略必須由「符規」躍升為「問責」。

機構要做到問責，推動整體全面的私隱管理系統至為重要，確保機構有穩妥的政策和程序，應用在所有業務常規、操作程序、產品／服務設計、實體建築和基建網絡等各方面。機構積極推行私隱管理系統的好處，最起碼是展示機構有能力依從條例的法律規定。但好處不止於此，它有助在機構內培養尊重私隱的文化。如果執行得宜，系統有助機構與客戶／市民、員工、股東和規管者等建立互信的關係，提升機構的聲譽，從而加強其競爭優勢。

事實上，建立和維持客戶的信任是企業競爭優勢的基石。大眾逐漸意識到個人資料的價值；沒有妥善處理個人資料的機構會失去客戶的信任，甚至其惠顧。因此，很多大企業均積極採取尊重私隱的業務措施。坐言起行，實施健全的私隱管理系統，可贏取持份者（包括客戶）對機構的信任。穩健的私隱管理系統亦可提升機構的聲譽，加強競爭優勢。

有時失誤是難以避免的。但穩妥的私隱管理系統有助機構辨識己方在保障個人資料方面的弱點，從而鞏固良好的行事方式，展示機構作出應盡的最大努力，甚至提升保障個人資料的水平，而不是僅僅符合法律的最基本要求。

A PMP can create a competitive edge

Privacy and data protection cannot be managed effectively if they are treated merely as a legal compliance issue. A more effective response in this era of Big Data and rising public expectations for privacy protection is to be proactive and preventative, rather than reactive and remedial. Organisations should embrace personal data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business imperative throughout the organisation. A strategic shift from compliance to accountability is required.

To achieve accountability, it is of paramount importance for organisations to adopt a holistic and encompassing PMP that ensures robust privacy policies and procedures are in place and implemented for all business practices, operational processes, product and service design, physical architecture and networked infrastructure. At the minimum, the outcome of this holistic approach should be a demonstrable capacity to comply with the legal requirements of the Ordinance. But it is more than that. It helps foster a privacy respectful culture throughout an organisation. When executed well, a PMP is conducive to building trustful relationships with customers or citizens, employees, shareholders and regulators, creating a competitive edge in the industry.

Indeed, building and maintaining customers' trust is the cornerstone of a business' competitive advantage. People are waking up to the value of their personal data, and organisations which fail to handle people's personal information properly will lose their trust and even their business. For this reason, many leading companies are proactively adopting privacy-friendly business practices. When an organisation "walks the talk" by implementing a robust PMP, enhanced trust from stakeholders, including customers, to engage with that organisation should follow. An organisation that has a strong PMP should enjoy an enhanced reputation that gives it a competitive edge.

There may be times when mistakes are made. However, with a solid PMP, organisations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal data that they hold to a higher level than the bare minimum needed to meet the legal requirements.

相反，若機構沒有周全地保障個人資料，會損害機構的信譽。機構一旦發生個人資料外洩事故，不論在善後及修補聲譽方面都可能要付上非常沉重的代價。對受影響的個人而言，資料外洩的代價可能亦相當大。

Conversely, without strong personal data protection, trust may erode to an organisation's detriment. Personal data breaches can be expensive for organisations – both in terms of "clean up" and reputation repair. Breaches may also prove expensive for the affected individuals.

現時不少機構均持有大量的個人資料，資料的經濟價值又日增，公眾亦更為留意及關注侵犯私隱的事故，因此機構有必要採取步驟去制定及維持完善的私隱管理系統，以減低這類事故發生的風險，同時提高機構處理根本問題的能力，把事故所造成的損害減至最低。

Given the vast amounts of personal data held by organisations and institutions, the increasing economic value of the data, and the heightened attention and concern regarding privacy breaches, it makes business sense for organisations to take steps to put in place and maintain a PMP to minimise the risks of such breaches, maximise the organisation's ability to address any underlying problems, and minimise the damage arising from breaches.

私隱專員寄語把私隱管理系統成為機構內的熱門詞語。
The Commissioner appeals to make Privacy Management Programmes the buzz word in all organisations.

回響
Feedback

「雖然遵從該指引（私隱管理系統最佳行事方式指引）所列的建議及意見並不是《個人資料（私隱）條例》的規定，但該指引就了解條例的保障資料責任提供了有用的建議。

該指引清楚顯示公署決心改變企業保障個人資料的文化。」

"Whilst it is not a legal requirement under the Personal Data (Privacy) Ordinance (PDPO) to comply with the recommendations and advice set out in the Guide (PMP: A Best Practice Guide), it provides useful recommendations for understanding how data protection obligations arise under the PDPO.

The release of the Guide is a clear signal of the PCPD's determination to change the corporate culture on personal data protection."

Ms Michelle CHAN, Ms Clarice YUE and Mr Wilfred NG
Partner, Senior Associate and Associate respectively at Herbert Smith Freehills

摘自 *Quote: Privacy This Week, Cecile Park Publishing Ltd. (2014.03.03)*

「公署推廣在機構內建立私隱管理系統作為策略性架構，實在令人鼓舞。」

"It is particularly encouraging that the PCPD is promoting the adoption of PMPs within organisations as a strategic framework."

劉嘉敏工程師，JP, 香港電腦學會副會長（執行）
Ir Stephen LAU, JP, Vice President (Executive), Hong Kong Computer Society

摘自 *Quote: Computer World (2014.02.24)*

「……積極的規管者、違規者被點名的政策，及公眾日漸關注資料私隱事宜，這些都清楚顯示遵從《個人資料（私隱）條例》是香港企業的首要項目。」

"With... an activist regulator, a policy of "naming and shaming" those who fail to comply, and growing public interest in data privacy issues, it is clear that PDPO compliance has to be a priority for Hong Kong businesses."

Hogan Lovells

「恭賀（公署）完成全面的私隱管理系統指引……六年前，問責是被大多數人忘記的經濟合作及發展組織的（私隱保障）原則。現在它有真正的牽引力……這是基金會的挑戰，同時是香港的挑戰。多謝……在香港所做的工作。」

"Congratulations on your (PCPD's) comprehensive privacy program guidance... Six years ago accountability was a mostly forgotten OECD (privacy protection) principle. It now has real traction... That is the Foundation's challenge, as well as (that) in Hong Kong. Thanks so much for the work... done in Hong Kong."

Mr Martin ABRAMS, Executive Director and Chief Strategist, Information Accountability Foundation

諮詢工作

本年度，運輸署為回應審計處處長就改善現時執法攝錄系統效能的建議，設計了一套在交通燈旁加設前置鏡頭以記錄衝紅燈的車輛及駕駛者面貌的系統（「該系統」），並徵詢公署的意見。

首先，公署建議運輸署對該擬議系統進行私隱影響評估，以識別及減少在個人資料保障私隱方面任何實際及潛在的影響。

公署建議運輸署按照條例附表 1 的保障資料原則考慮下述事宜：個人資料的收集、準確性及保留、使用、保安，以及個人資料政策及措施的透明度。

保障資料第 1 原則：該系統似乎會影響所有駕駛者，甚至其他道路使用者。攝錄其他人士，例如有關車輛內前座乘客或其他道路使用者的影像，會被視為過度收集個人資料。公署建議運輸署考慮及尋找其他侵犯私隱程度較低的方法，以達致同樣或類似目的。

保障資料第 2 原則：由於這些資料會用來對有關人士作刑事檢控，運輸署必須採取所有切實可行的步驟，以確保資料的準確性。運輸署應制定資料保留政策，以確保在達致收集目的後，適時刪除個人資料。

CONSULTATION

During the year, the Transport Department sought our view on the proposed installation of additional front cameras beside the traffic lamps to record the images of vehicles and the faces of drivers jumping red lights ("the System"), which was designed to address the recommendation of the Director of Audit to improve the effectiveness of the present enforcement camera system.

First and foremost, the PCPD advised the Transport Department to conduct a Privacy Impact Assessment on the proposed System to identify and reduce any actual and potential privacy impact on personal data protection.

The PCPD recommended the Transport Department to consider the following issues in light of the Data Protection Principles ("DPP") in Schedule 1 of the Ordinance, in dealing with the collection, accuracy, retention, use and security of personal data, as well as the transparency of the System, in both policy and practice.

DPP1: It appeared that the System would affect all drivers and even other road users. The capturing of the images of other individuals, such as front seat passengers inside the relevant vehicle or even other road users, would be considered excessive collection of personal data. The Transport Department was advised to consider and explore other less privacy intrusive alternatives to achieve the same or similar purpose.

DPP2: All practicable steps must be taken to ensure data accuracy, since such data would be used for the purpose of assisting criminal prosecution against the individuals. A data-retention policy should be devised to ensure the timely erasure of personal data after the purpose of collection has been fulfilled.

保障資料第 3 原則：公署建議運輸署制定清晰的政策及指引，規管查閱及使用該系統所收集的個人資料，以防止「改變用途」的情況，即所收集的個人資料可能被用來追蹤有關人士的活動，與違反交通規則無關。

DPP3: A clear policy and guidelines should be devised to govern access to and use of the personal data collected by the System to prevent “function creep”, i.e. the personal data collected may be used to track the activities of individuals for purposes other than the traffic offence.

保障資料第 4 原則：在開發該系統時，應採取「貫徹私隱的設計」。查閱個人資料的權限須以「有需要知道」原則為規限，並須保存適當的審核追蹤記錄，以監察遵從內部政策、指引及程序的情況。

DPP4: A privacy-by-design approach should be adopted in developing the System. Access to personal data must be on a need-to-know basis and a proper audit trail must be kept to monitor compliance with internal policies, guidelines and procedures.

保障資料第 5 原則：公署建議運輸署在政府網站或以其他途徑公佈其私隱政策聲明，以增加該系統的個人資料政策及措施的透明度。在該系統實施初期，相信亦有需要舉行傳媒簡介會及進行其他宣傳工作，以回應公眾在私隱方面的關注。

DPP5: To make the personal data policy and practice of the System as transparent as possible, a Privacy Policy Statement should be published on the relevant Government website(s) or otherwise be made available to the public. A media briefing and other publicity work would be necessary to address any privacy concerns the public might have during the initial stage of implementation of the System.

處理查詢

公署在本年度共處理 23,459 宗查詢個案，比上年度增加 18 %； 平均每個工作天處理 95 宗查詢（圖 2.2）。

HANDLING ENQUIRIES

A total of 23,459 enquiry cases were handled during the year, up 18 % from the number of the previous year. On average, 95 enquiry cases were handled per working day (Figure 2.2).

圖 2.2：全年查詢個案

Figure 2.2: Annual enquiry caseload

18%
較上年度增長
up from the number of the previous year

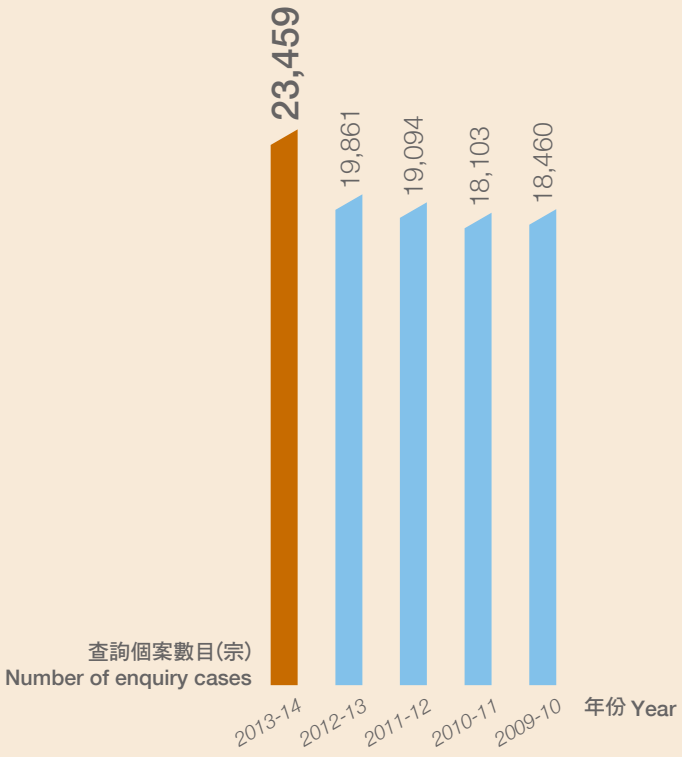
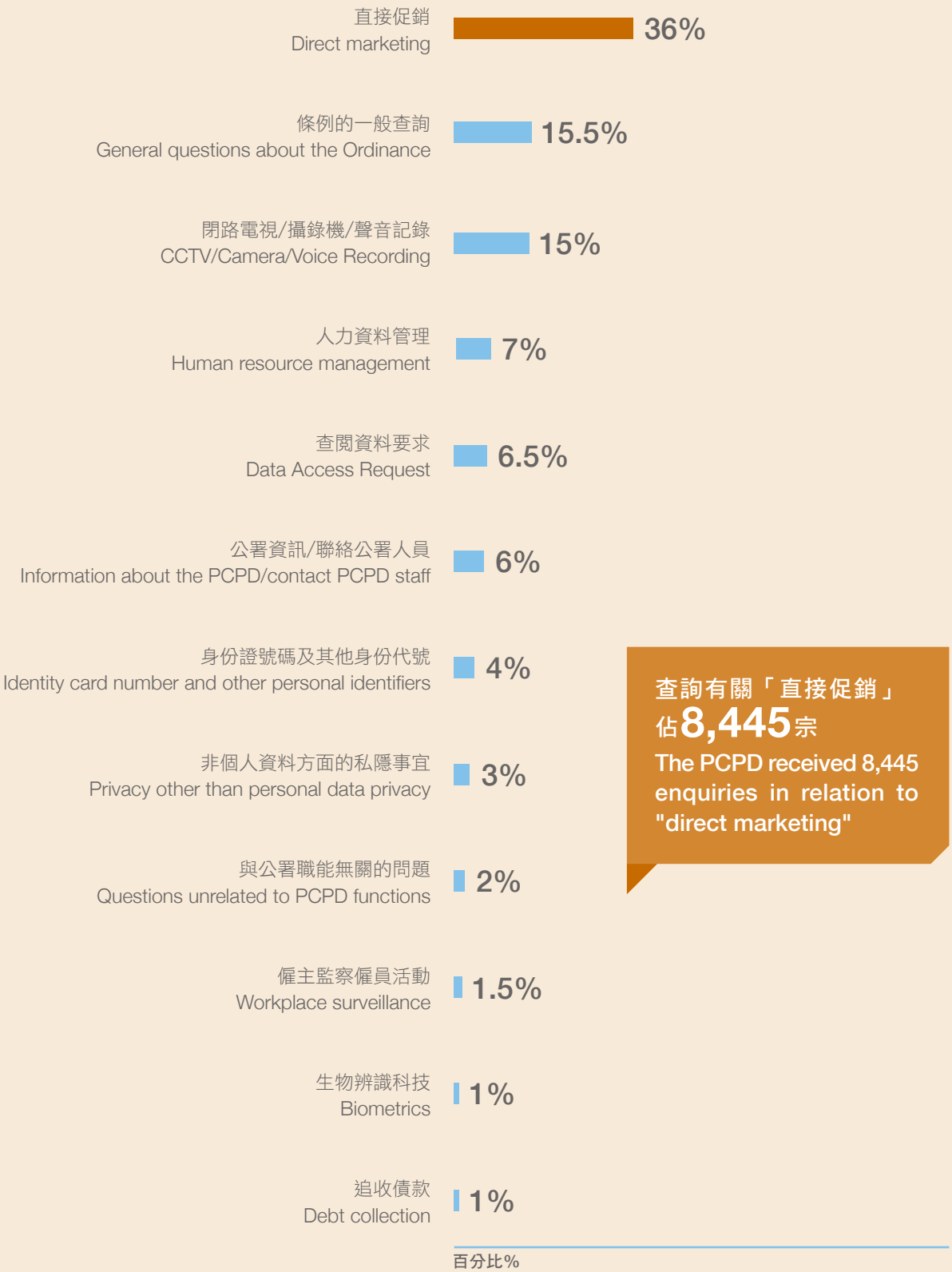


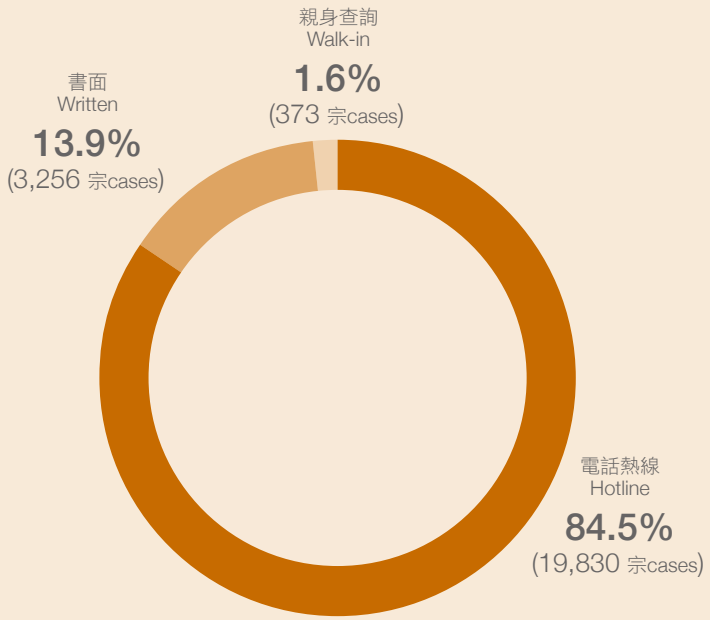
圖 2.3：查詢個案的性質　　Figure 2.3: Nature of enquiry cases



查詢有關「直接促銷」佔**8,445**宗
The PCPD received 8,445 enquiries in relation to "direct marketing"

大部分（84.5%）查詢經由公署的電話熱線（2827 2827）提出（圖 2.4）。
The majority of the enquiries (84.5%) were made via the PCPD hotline (2827 2827). (Figure 2.4)

圖2.4：提出查詢的途徑 **Figure 2.4: Means by which enquiries were made**



我是負責處理公眾查詢及機構循規審查工作的。查詢者一般都會很迫切希望公署可幫忙解決他們各自遇到有關私隱的問題，而我和部門的同事都會盡力解答；當得到他們的讚賞時，我們都會感到很鼓舞。雖然我入職的時間很短，但感謝公署給我機會，於執行部至審查及政策部輪換工作，擴闊工作經驗，我亦期望為公署作出更多貢獻。

My duties are to handle enquiries from the general public and conduct compliance checks against organisations. The enquirers generally would be very eager to have their various privacy-related problems solved with the help of the PCPD, and my colleagues and I would strive to meet their expectations. We are greatly encouraged should we receive enquirers' compliments. Although I have joined this office only for a short period of time, I am thankful for the opportunities offered to broaden my work experience through job rotation from Operations Division to Compliance & Policy Division. I am looking forward to contribute more to this office.

霍靜怡 個人資料助理
Phoebe FOK Personal Data Assistant

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 181 次循規審查行動。49% 的循規審查對象為私營機構，其餘 51% 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。

巴士車廂安裝閉路電視

公署獲悉某巴士公司（「該巴士公司」）其中一個巴士車廂所安裝的閉路電視拍下視頻片段，並可以透過一個視像分享網站讓公眾查看，於是對該巴士公司展開循規審查。

該巴士公司在回應事件時解釋，有關視頻片段是一名巴士車長未經授權在車廂內安裝閉路電視拍攝及上載的。在事發後，該巴士公司已因該車長違反公司政策而對他採取紀律行動。此外，該巴士公司已向所有車長發出通告，重申不得未經授權在巴士車廂內安裝任何攝錄器材。車站主管及督察則會定期上車檢查情況。

COMPLIANCE CHECKS

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

During the year, the Commissioner carried out 181 compliance checks. Of these, 49% were conducted on private sector organisations, while the remaining 51% 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.

CCTV installation in bus compartments

It was brought to PCPD's attention that a video clip captured by a closed-circuit television ("CCTV") camera installed inside a bus compartment of a bus company (the "Bus Company") was found to be publicly accessible through a video-sharing website. The PCPD then initiated a compliance check on the Bus Company to look into the matter.

In response to the incident, the Bus Company explained that the video clip in question had been taken and uploaded by a bus captain who had installed the CCTV camera inside the bus compartment without authorisation. After the incident, the Bus Company took disciplinary action against the bus captain for having contravened the company's policy. Further, a notice was issued to all bus captains reminding them of the company's policy prohibiting the unauthorised installation of any recording equipment inside bus compartments. Also, terminus supervisors and inspectors were required to check regularly on board the buses to monitor the situation.

公署在查詢期間得悉該巴士公司為了保安及調查事件而正式在部分巴士車廂安裝閉路電視。為了確定有關安裝是否符合條例的規定，公署在該巴士公司的車廠進行視察，並留意到：

During the course of our inquiries, it was revealed that the Bus Company had officially installed CCTV cameras in some of their bus compartments for security and incident investigations. To ascertain whether the installation of the CCTV was in compliance with the requirements under the Ordinance, the PCPD conducted an inspection at the depot of the Bus Company and noticed that:-

(a) 閉路電視的鏡頭是瞄準巴士的前方、前門、駕駛盤、後門及上層；

(a) CCTV cameras had been installed showing the driver's forward view, the entrance door, the steering wheel, the exit door, and the upper deck;

(b) 司機位上方安裝了顯示屏，為車長提供實時影像；

(b) A monitor screen had been installed above the driver seat providing the bus captain with real time images;

(c) 該公司有政策及程序，規管查閱及保留由閉路電視所拍攝影像的事宜；

(c) The Bus Company had policy and procedures governing the access to and retention of the images captured by the CCTV cameras;

(d) 閉路電視只會在引擎開動時操作，並鎖於巴士上的一個櫃內。只有獲授權人士才可開啟。因此巴士車長不能改動閉路電視的任何設定，亦不能存取任何記錄；及

(d) The CCTV would operate only when the engine was on, and the CCTV was locked in a cabinet inside the bus. Only authorised persons had access to it, so the bus captains were unable to alter any of its settings or retrieve any of the recordings; and

(e) 在巴士車廂內已張貼告示，通知乘客受閉路電視監察，但沒有提及可以向其提出個人資料私隱事宜的聯絡人。

(e) Notices were posted in the bus compartment informing the passengers that they were under CCTV surveillance, but there was no mention of a contact person with whom matters relating to personal data privacy issues could be raised.

循規審查結果認為，雖然該巴士公司可以合理地解釋，安裝閉路電視是為了保安及調查事件，但他們應加強與乘客及僱員的溝通，以減低有關使用閉路電視監察的疑慮或關注。在這方面，該巴士公司接納公署的建議，並採取下述改善措施：

The compliance check concluded that although the Bus Company could reasonably justify that the installation of the CCTV was for security and incident investigations, it should strengthen communication with passengers and employees to eliminate any doubt or concerns relating to the use of the CCTV surveillance recordings. In this regard, the Bus Company took the PCPD's advice and made the following improvements:-

(a) 表明安裝閉路電視系統是為了保安及調查事件，而不是為了監察僱員；及

(a) It indicated explicitly its policy that the CCTV system was installed for security and incident investigation purposes, not for employee monitoring; and

(b) 修訂閉路電視的告示，加上客戶服務熱線，讓乘客可透過熱線提出有關個人資料私隱的事宜。

(b) It revised the CCTV notices to include a customer service hotline that passengers could call for matters relating to personal data privacy.

載有 64,786 名人士個人資料的網站遭黑客入侵

一間環保機構（「該機構」）向公署通報發現其網站遭黑客入侵，因此懷疑約 64,786 名捐款者及參與活動者的個人資料已外洩。有關的個人資料涉及姓名、香港身份證號碼、性別、電話號碼、地址、電郵地址、出生日期、密碼、碳排放資料、捐贈 / 贊助的款額，及家庭成員資料。

該機構在回應公署的查詢時解釋，事件是因黑客利用其網站伺服器及網絡應用程式的漏洞，入侵並控制了該機構載有個人資料的資料庫。該機構補充，沒有證據顯示其網站內的個人資料受損。

該機構已在事發後立即採取多項加強系統措施，包括強化伺服器、重設密碼、提升軟件、伺服器修補及漏洞掃描。

在今次事件後，該機構又在技術及行政上實施連串補救行動，防止日後再發生類似事件，包括：

(1) 提供防火牆保障，把資料庫伺服器與網絡伺服器分開，加強儲存的個人資料的保安；

(2) 採用漏洞掃描軟件，定期識別及修補系統的保安漏洞；及

(3) 向全體職員公佈政策，提高他們在建立網站及電子應用程式的私隱意識。

Websites containing personal data of 64,786 individuals hacked

An environmental protection organisation (the "Organisation") reported to the PCPD that its websites were found to have been hacked, and as a result, the personal data of approximately 64,786 donors and participants of its campaign was suspected to have been leaked. The personal data involved names, Hong Kong identity card numbers, gender, telephone numbers, addresses, email addresses, date of birth, passwords, carbon footprint data, donation/sponsorship amount and family members' information.

In response to PCPD's enquiries, the Organisation explained that the incident had been caused by a hacker's exploitation of vulnerabilities in their web server and web application programmes, which allowed the hacker to gain control over their database containing the personal data. The Organisation added that there was no evidence showing that personal data contained in their website had been compromised.

Immediately after the incident, the Organisation took various steps to strengthen its systems, which included server hardening, password reset, software upgrade, server patching and vulnerability scanning.

The Organisation also subsequently implemented a series of remedial actions, both technically and administratively, to prevent recurrence of similar incidents in the future, which included:-

(1) Separating its database server from the web server by implementing firewall protection to strengthen the security of the personal data stored therein;

(2) Deploying vulnerability scanning software to identify and fix the security vulnerabilities of its systems periodically; and

(3) Disseminating a policy to all staff members to enhance their privacy awareness related to website building and digital applications.

371 名酒店客戶的資料經電郵外洩

一間酒店（「該酒店」）向公署通報，一名職員向 333 名客戶發出電郵提醒他們提取訂購的月餅時，不小心夾附一個載有 371 名客戶個人資料的試算表檔案（「該試算表檔案」）。該試算表檔案並沒有加密或以密碼保護。事件中外洩的個人資料包括客戶的姓名、地址、電郵地址、電話號碼、流動電話號碼、傳真號碼、付款方法、部分信用卡號碼及付款額（「該等資料」）。

該酒店在回應公署的查詢時解釋，一名僱員從銷售訂購軟件（「該軟件」）滙出該等資料到一個試算表，然後以電郵發給一名合約職員，以便該職員以電郵提醒客戶提取月餅。當該職員向客戶發信時，不小心夾附了該試算表檔案，因此該等資料被錯誤地披露予客戶。

該酒店因應事件採取了下述補救行動，防止日後再發生類似事件：

(a) 檢討客戶資料的查閱權，規定所有合約或兼職員工不得查閱客戶資料，查閱權只授予經理級職員；

(b) 只容許兩名高級職員有權從該軟件摘取／滙出客戶資料；

(c) 把所有客戶資料檔案加密，並把儲存於共用驅動器的客戶資料檔案加上密碼保護；

(d) 成立私隱小組制定政策及程序、監察培訓進度及循規事宜，並建議最佳行事方式；及

(e) 向所有職員提供強制性的保障資料私隱培訓。

Data leakage via email involving 371 customers of a hotel

A hotel (the "Hotel") reported to the PCPD that a staff member had inadvertently attached an Excel file (the "Excel File") containing the data of 371 customers in an email to 333 customers reminding them to collect mooncakes they had ordered. The Excel File was neither encrypted nor password protected. The personal data leaked in the incident included customers' names, addresses, email addresses, telephone numbers, mobile telephone numbers, facsimile numbers, payment methods, partial credit card numbers and payment amounts (the "Data").

In response to the PCPD's enquiries, the Hotel explained that an employee had exported the Data from their sales ordering software (the "Software") into an Excel spreadsheet and passed this by email to a contract staff member for sending a reminder email to customers to collect their mooncakes. When sending the reminder to the customers on the list, the contract staff member inadvertently attached the Excel File. As a result, the Data was wrongfully disclosed to the customers.

The Hotel subsequently took the following remedial action to prevent similar incidents in the future:-

(a) It reviewed the access right to its customers' data, denied access to all contract or part-time staff, and granted access to managerial staff only;

(b) It allowed only two senior staff members to have the user right to extract/export customer data from the Software;

(c) It encrypted all customer data files and added passwords to protect the customer data files stored in the common drive;

(d) It set up a data privacy team to define policies and procedures, monitor training progress and compliance issues, recommend best practices, etc.; and

(e) It provided compulsory data privacy protection training for all staff members.

主動調查

保障資料第 4 原則規定，資料使用者須採取所有合理地切實可行的步驟，以確保病人的個人資料受保障而免受未經准許或意外的查閱、遺失或使用所影響。

市民的個人資料若被不恰當使用，不論起因是意外遺失、被外洩或被偷竊，後果都可以很嚴重。特別是以下所載列牽涉市民病歷及警方文件的個案。

PCPD-INITIATED INVESTIGATIONS

Data Protection Principle 4 ("DPP4") requires data users to take all reasonably practicable steps to ensure personal data is protected against unauthorised or accidental access, loss or use.

The potential harm to individuals arising from the misuse of their personal data, whether accidentally lost, leaked or purposely stolen, could be significant, particularly in the cases described below which involve patients' medical records and police documents.

醫管局—處理棄用病人紀錄失當

載有病人資料的醫院廢料，包括用過的打印帶及病人預約回條，被發現棄置在密件處理服務有限公司（「密件處理公司」）的碎紙廠外。該公司是醫院管理局 （「醫管局」）以合約（「該合約」）聘用的廢料處理服務供應商。

根據調查結果，私隱專員裁定醫管局違反條例的保障資料第 4 原則，理由如下：

該合約在打印帶處理上的疏漏 — 在該合約中，列明了對載有個人資料的廢紙的保安措施（如回收廢料袋須用有序列編號的安全裝置或規定廢紙應切碎成多闊），但對同樣地載有病人個人資料的棄置打印帶，卻沒有說明處理方法。該合約沒有列明由醫院運送資料往碎紙廠途中，需要點算裝有打印帶的

Hospital Authority – Improper disposal of hospital waste containing patient records

Hospital waste containing patients' data, namely a used printer ribbon and shredded strips of medical appointment slips, were found abandoned outside the shredding factory of Confidential Materials Destruction Service Limited ("CMDS"), the waste disposal service provider of the Hospital Authority ("HA"), appointed under a contract (the "Contract").

Based on the investigation findings, the Commissioner determined that HA had contravened DPP4 for the following reasons:

Contractual omission in the treatment of printer ribbons – Security measures (such as the use of a serialised sealing safety device or specifying the maximum width of shredding) were found in the Contract in relation to paper waste containing patients' personal data, but not in relation to printer ribbon waste, which also contains patients' personal data. There was no contractual requirement that the number of bags of printer ribbon waste be checked (during transit from the hospitals

回收袋數目，以防遺失；亦沒有訂明切碎至那個程度以保證當中的個人資料不能被識別或還原；及

to the shredding factory) to prevent accidental loss; and no guarantee that the waste would be shredded to the extent that the personal data contained therein could not be readily recognised or recovered; and

密件處理公司監管不力 — 根據該合約，醫管局及其轄下的醫院均有權對密件處理公司的碎紙過程進行視察。視察行動若得以妥善協調和執行，並恰當地跟進，應可有效地監控資料處理者的表現，以及發現操作中的問題，適時作出改善。然而，醫管局總部否認他們有責任統籌監督轄下醫院進行視察。醫管局與轄下醫院之間就視察承辦商的次數、範圍或匯報全無指引和協調。再者，醫管局從未履行其權利進行審計，檢討或核實密件處理公司有否遵從該合約訂明的責任及條款。

Inadequate supervision of CMDS – Under the Contract, the HA and its hospitals were entitled to inspect the shredding process at the CMDS factory. If the inspections were coordinated well, conducted thoroughly, and followed up properly, they would be an effective tool to check the performance of the shredding contractor and identify irregular practices for prompt rectification. However, the HA Head Office denied responsibility for centrally monitoring the inspections carried out by hospitals. There were no guidelines or coordination between the HA and its hospitals to define the frequency, scope or reporting requirement for such inspections. Furthermore, the HA did not carry out the audits it is entitled to under the Contract to review or verify if CMDS had complied with its obligations under the Contract and the requirements under the Ordinance.

私隱專員因而向醫管局發出執行通知，指令醫管局：(1) 採取合理的行動，取回在事故中棄置的醫院廢料，並予以銷毀；(2) 檢討和修訂醫院的廢料棄置程序，並實施改善措施。

The Commissioner therefore served an Enforcement Notice on the HA, directing it to: (i) make a reasonable endeavour to retrieve and destroy the abandoned hospital waste identified in the two incidents; and (ii) review and revise the hospital waste-disposal process, and implement improvement measures.

私隱專員強調今次的違規事故帶出一個訊息：恒常保障個人資料是很重要的。即使機構持有的個人資料在機構範疇以外的地方或外判予第三者處理，機構保障個人資料的責任依然存在。密件處理公司作為醫管局的承辦商，處理載有病人個人資料的醫院廢料，表現實在是極不理想。醫管局在合約和程序層面對密件處理公司的監督，及醫管局人員對該公司實地的監察，表現都強差人意。

The Commissioner stressed that the breach illustrated the importance of keeping personal data secure at all times. An organisation's responsibility to keep personal data secure does not end when it is taken out of the building or outsourced. The unsatisfactory performance of CMDS, as the HA's contractor, in the treatment of hospital waste containing personal data was unacceptable, and the HA's oversight of its contractor's performance, in terms of contractual and procedural rigour, as well as physical supervision, was also far from satisfactory.

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R13_6740_c.pdf

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_6740_e.pdf

香港警務處—資料經 Foxy 外洩後患無窮

在 2008 至 09 年度完成對香港警務處（「警務處」）有關經 Foxy 外洩資料的調查後，前任私隱專員曾發出執行通知指令警務處予以糾正。警務處其後在 2009 年 8 月實施改善措施，包括 (i) 警隊電腦的 USB 接頭只容許使用經認可的 USB 記憶體；(ii) 制定資訊保安的規定及指引；(iii) 加強安全設施及支援，及 (iv) 提高警隊成員對資訊保安的認識。

傳媒在 2011 年 8 月及 2012 年 9 月先後報道兩宗懷疑警務處經 Foxy 外洩內部文件的事件後，私隱專員主動展開調查。

事故 1：有多份載有個人資料的警務處文件發現經 Foxy，於互聯網上可以搜尋得到；當中大部分文件在 2008 至 09 年度的調查中已涵蓋，今次只有一份外洩文件是新發現的，就是屬於警員職位申請者的回條，上面載有一名投考人士的姓名及身份證號碼等個人資料。外洩的原因相信是由於該投考人士在他的私人電腦安裝了 Foxy。換言之，在今次事件中警方並非洩密一方。

事故 2：多份證人口供、警務處內部備忘錄、表格及書信文件，涉及證人及被逮捕人士的姓名、香港身份證號碼、地址及檢控的內容等個人資料，經 Foxy 於互聯網上外洩。調查發現，事故中的警員從 2007 年起在未經上級批准的情況下，偶爾使用其私人 USB 記憶體從警隊電腦中下載文件至其私人電腦，並用該電腦處理公務。由於有關警員並沒有把其電腦連上互聯網，而且警務處確實沒有在該部門的電腦系統安裝任何分享軟件包括 Foxy，警務處認為有可能有人從該出售的電腦，把硬磁碟機內已清除的文件復原，令個人資料從而外洩。私隱專員裁定這宗事故起因在於有警務人員在未經授權的情況下，下載警方的文件，又在出售其電腦前未有用核准的軟件清除內裏載有的相關資料。而鑑於保障資料第 4 原則要求資料使用者確保個人資料保安並非一項絕對義務，私隱專員沒有發現警務處違反規定。

Hong Kong Police Force – The use of Foxy culminated in data leakage which got out of control

Upon the conclusion of a 2008-09 investigation of the Hong Kong Police Force (the "HKPF") for data leakage via Foxy, the then Commissioner served an enforcement notice on the HKPF which led to the adoption in August 2009 of a series of improvement measures to safeguard personal data, which included: (i) configuring the USB ports of the HKPF's computers to accept only approved USB thumb drives; (ii) the formulation of information security instructions and guidelines; (iii) the strengthening of security measures and support; and (iv) the enhancement of police officers' knowledge of information security.

The Commissioner initiated an investigation into two incidents of alleged leakage of internal documents by the HKPF via Foxy after they were reported in the press in August 2011 and September 2012 respectively.

Incident 1: A reply slip containing the name and identity card number of an applicant for a position in the HKPF, together with other police documents covered by the 2008-09 investigation, was searchable by the general public via Foxy. It was found that Foxy was installed in the applicant's personal computer, which led to the leakage of the reply slip. The HKPF was not responsible for the leakage in this case.

Incident 2: A number of police documents, including witness statements, internal memoranda, forms and correspondence, were leaked on the internet via Foxy. It was revealed that a police officer, without the HKPF's approval, had occasionally transferred documents from the HKPF's computer system to his own computer via his private USB thumb drive for work purposes since 2007. Given that the police officer had not used his computer to connect to the internet, and that the HKPF had not installed any file-sharing software, including Foxy, in its computer system, the HKPF concluded that the leaked documents could have been recovered from the hard disk after the sale of the computer, and that the data was subsequently leaked. The Commissioner determined that this incident was attributed to the unauthorised downloading of Police documents by the police officer and his failure to use approved software to erase the data before sale of his computer. He found no contravention on the part of the HKPF as DPP4 does not impose an absolute obligation on data users to safeguard personal data.

考慮到該些文件所載的個人資料的重要性及敏感性，專員敦促警務處採取預防措施，(i) 向警務人員推廣使用警務處的電腦程式來檢查及清除其個人電腦所載有的個人資料／機密資料；(ii) 設立諮詢熱線，讓有需要的警務人員以不記名方式得到支援；(iii) 促進警務人員之間的個案分享及經驗交流，藉以加深警務人員對個人資料保護的認知，及警覺網上資訊外洩可能造成的嚴重後果等。

Considering the importance and sensitivity of the personal data contained in the police documents, the Commissioner urged the HKPF to take preventative measures to (i) promote the use of HKPF's computer programme by police officers to check and delete personal data/confidential data on their personal computers; (ii) set up an enquiry hotline so that police officers could seek assistance on IT-related matters on an anonymous basis; and (iii) promote case- and experience-sharing among police officers to enhance their awareness of personal data protection and the potentially serious consequences of data leakage on the Internet.

私隱專員警告，一旦資料檔案經過 Foxy 網絡外洩，基本上並無有效的方法可以將資料挽回。雖然 Foxy 的開發商經已結業，但迄今全球至少有 40 萬人的電腦仍啟動著 Foxy 軟件。任何人若需要下載這軟件，只能到非官方渠道下載，這是非常冒險的，因所得的版本有可能載有惡意程式，或遭改裝而招致無法控制的資料外洩事故。

The Commissioner warned the public that there was practically no effective recovery means once a data file was leaked through the Foxy network. Though the developer of Foxy has ceased business, Foxy is still operating on 400,000 or more computers around the world. Whoever wants to download this software for use will have to resort to unofficial channels and may thus obtain a copy which contains malware or which has been altered, thus running the risk of uncontrollable data sharing.

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R13_15218_c.pdf

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_15218_e.pdf

加入公署的資訊科技部門，有別於我過往工作的範疇。於部門內日常接觸到的工作都與資訊科技有關，除了令我加深了對資訊科技的認識，更了解到在現今資訊科技急速發展的社會中，資訊科技與個人資料私隱有著密切的關係，例如安裝應用程式後，手機上的資料有機會在機主不知情下被讀取等，從而令我懂得保護個人資料私隱的重要性！

The work in the Information Technology (IT) Department of the PCPD is different from my past jobs. The daily routine in my department relates to IT. In addition to enhancing my IT knowledge, my work enables me to understand that IT has a close relationship with personal data privacy, e.g. after installation of an app, the data in the smartphone may be accessed without the user's knowledge. I have learnt of the importance of protecting personal data privacy from my work.

陳詩麗 資訊科技部 行政助理
Karmen CHAN
Administrative Assistant, Information Technology Division

香港警務處—接連遺失載有敏感個人資料的記事冊

私隱專員得悉發生了 11 宗警務人員遺失記事冊及定額罰款單的資料外洩事故後，主動展開調查。事故涉及的遺失物品共載有 285 名人士的個人資料，當中包括罪案受害人、證人及疑犯。

警務處在這兩類事故中違反了保障資料第 4 原則。警務處沒有採取所有切實可行的步驟，包括設立全面的程序及有效施行監督及監察制度，以確保載有個人資料的警方文件受保護。

私隱專員因此向警務處送達執行通知，指令警務處（a）訂立額外保安程序堵塞漏洞及（b）加強監督。

事故亦揭示 (i) 警務處有需要檢討警方的器材及制服設計，以及 (ii) 相關警務人員普遍對個人資料的保安風險意識不足，以致未能妥善保護載有個人資料的文件。私隱專員因此建議警務處 (i) 全面檢討用以盛載或運送警方記事冊及告票的器材及制服，以防止個人資料受未經准許的查閱或意外的遺失；及 (ii) 加強培訓、獎勵及紀律處分的項目，以促進警務人員遵從警務處保障私隱及個人資料的政策及程序。

私隱專員補充：「無可置疑，很多資料保安的事故，都是由人為錯失釀成，難以完全避免。即使是完備的私隱政策和嚴格的保安措施，都有可能因為個別員工的鹵莽或粗心大意而被削弱功效。機構應為員工提供全面的內部培訓和提高保障私隱的意識，這是至為重要的。建立一個尊重私隱的機構文化，則可確保推動機構整體投入，致力實踐保障私隱。」

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R13_0407_c.pdf

Hong Kong Police Force – Repeated incidents of loss of notebooks containing sensitive personal data

The Commissioner initiated this investigation upon noticing 11 data-breach incidents concerning the loss of police notebooks or fixed penalty tickets by different police officers. The lost items contained the personal data of a total of 285 persons, including crime victims, witnesses and suspects.

The HKPF was found to have breached DPP4 in these two types of incidents. The HKPF failed to take all practicable steps, including putting in place a set of comprehensive procedures, as well as ensuring the effective implementation of its supervision and monitoring system, to safeguard the security of police documents containing personal data.

The Commissioner accordingly served an enforcement notice on the HKPF directing it to: (i) establish supplementary security procedures to plug the loopholes which were identified; and (ii) tighten up its supervision.

The incidents also revealed: (i) the need to review the police equipment and uniform design; and (ii) a general lack of awareness of the security risks associated with personal data among the police officers concerned. The Commissioner therefore advised the HKPF: (i) to undertake a general review of the HKPF's equipment and uniform used for holding or conveying police notebooks and fixed penalty tickets in order to safeguard personal data from unauthorised access or accidental loss; and (ii) to step up its training, incentive and disciplinary programmes to promote compliance with the HKPF's policies and procedures in relation to privacy and data protection.

The Commissioner added: “Admittedly, many security breaches are simply the result of human error, which cannot be totally eliminated. Recklessness or simple carelessness of a single employee can undermine sound privacy policies and robust security practices. This underlies the importance for organisations to institute comprehensive internal training and awareness programmes for their staff. To ensure an organisation-wide commitment, the building of a privacy-respectful and data-secure culture is imperative.”

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_0407_e.pdf

視察行動

公署於 2013 年 4 至 8 月依據條例第 36 條，對學生資助辦事處（「學資處」）用作處理四項學生資助計劃的個人資料系統進行視察。

學資處是港府執行學生資助政策的機構。學資處於 2010 至 13 年三個學年內，每學年平均接獲逾 956,000 宗各項資助計劃的申請。

學資處為了處理申請而收集、持有及使用多種個人資料，包括申請人及其家庭成員的姓名、身份證號碼、出生日期、聯絡資料、就業狀況詳情、全年收入、銀行戶口資料及教育背景資料等。

視察結果認為，該系統的資料保障措施大致上令人滿意，惟某些方面仍需檢討和改善，例如：

(1) 學資處目前永久保留的資料有 35 類，包括可識別個人身份的個人資料，例如所有申請人及其家庭成員的英文姓名、身份證號碼及出生日期。私隱專員建議檢討這種做法，並應適當地將存檔的資料匿名化。

(2) 對於自稱為申請人的電話查詢者，學資處沒有向職員提供書面指引訂明可向來電者披露哪類有關申請的個人資料，職員只要求來電者提供其姓名及身份證號碼以核實其申請人身份。私隱專員建議學資處向職員提供清晰指引，並實施更嚴格的身份核實程序。

(3) 學資處會把所有資訊科技系統的資料備份磁帶從一個辦事處送往另一個辦事處作保存。不過，這些磁帶所記錄的資料並無加密處理。專員建議學資處把備份磁帶送離辦公大樓往儲存地點前，先把磁帶資料加密。

(4) 私隱專員建議學資處規定指定職位的職員，接受資訊科技保安意識的培訓（目前職員以自願性質參加）。

INSPECTION

The PCPD conducted an inspection of the personal data system of the Student Financial Assistance Agency ("SFAA") in respect of four of its financial assistance schemes for primary and secondary students, pursuant to section 36 of the Ordinance, in the period from April to August 2013.

The SFAA is the government agency responsible for the execution of the Hong Kong Government's policies on student financial assistance. It received on average some 956,000 applications for various financial assistance schemes in each of the three academic years from 2010 to 2013.

The SFAA collects, holds and uses a wide range of personal data, including the name, Hong Kong Identity Card (HKID Card) number, date of birth, contact information, employment details, annual income, bank account details and education background of applicants and their family members for the purpose of processing applications.

The inspection concluded that the data protection measures in the personal data system inspected were reasonably satisfactory. However, certain areas such as the following required review and improvement:

(1) The SFAA retained permanently 35 types of data, including personally identifiable data, such as the name, HKID Card number and date of birth of all applicants and their family members. The Commissioner recommended a review of this practice and anonymisation of the retained data, where appropriate.

(2) The SFAA provided no written guidelines for its staff as to which personal data in applications may be disclosed to callers representing themselves as applicants. Callers needed only to provide their full names and HKID Card Numbers for verification of their identity as applicants. The Commissioner recommended the promulgation of clear guidelines and implementation of a more stringent identity-verification procedure.

(3) Backup tapes of all IT systems were regularly transported from one SFAA office to another for safe-keeping. However, the data on the tapes were not encrypted. The Commissioner recommended encryption of the data on all backup tapes required to be transported to offsite storage.

(4) Staff attended IT security-awareness training on a voluntary basis. The Commissioner recommended that the SFAA provide mandatory IT security training for SFAA staff of designated posts.

(5) 學資處聘用承辦商將紙張形式的資料抄錄至光碟。學資處曾於 2010 年 3 月至 2013 年 3 月期間兩次視察資料準備承辦商的處所，但視察過程並無資訊科技技術人員提供支援。此外，學資處並無記錄視察結果，亦沒有檢查該承辦商完成抄錄過程後是否徹底刪除電腦系統上的資料。私隱專員建議學資處：(i) 日後的視察應加入資訊科技的技術人員；(ii) 記錄視察的結果；(iii) 隨機檢查以確保承辦商不會保留資料多於所需的時間；(iv) 制定政策訂明視察次數，以及 (v) 規定視察結果應由高級管理人員檢核。

(5) The SFAA engaged a contractor to transcribe the data provided in the application forms onto CDs. The SFAA conducted two inspections of the contractor's premises in the period from March 2010 to March 2013, without the involvement of staff from its IT technical support department. Moreover, the inspection results were not documented, and no check was conducted on whether the contractor had completely erased the electronic data after the transcription process. The Commissioner recommended: (i) that the SFAA involves IT technical support staff in future inspections; (ii) that the SFAA documents the inspection results; (iii) that it performs random checks to ensure data is not retained longer than necessary; (iv) that it establishes a policy on the frequency of inspections; and (v) that it requires a review of the inspection results by management staff of sufficient seniority.

視察報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/inspection_reports/files/R14_3771_c.pdf

Inspection Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/inspection_reports/files/R14_3771_e.pdf

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. After 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 DBN 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，公署共接獲 76 宗資料外洩事故通報（54 宗來自公營機構；22 宗來自私營機構，牽涉 114,275 人的個人資料。公署對肇事機構展開 76 項循規審查行動。）

During the year, the PCPD received 76 Data-Breach Notifications (54 from the public sector and 22 from the private sector), affecting 114,275 individuals. In response, the PCPD conducted 76 compliance checks.

個人資料的核對程序

在本年度，私隱專員共收到 28 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 27 宗申請。截至 2014 年 3 月 31 日，私隱專員在考慮餘下的一宗申請。

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 28 applications for approval to carry out matching procedures. All of the applications came from government departments and public sector organisations.

Upon examination, 27 applications were approved, subject to conditions imposed by the Commissioner. As at 31 March 2014, one remaining application was under consideration by the Commissioner.

The following is 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
社會福利署 Social Welfare Department	把綜合社會保障援助計劃租金津貼受助人的個人資料，與房屋署收集的公營房屋租賃人的資料互相比較，以避免向福利受助人提供超額津貼。 Comparing the personal data collected by the Social Welfare Department from the beneficiaries of rent allowance under the Comprehensive Social Security Assistance Scheme with the personal data collected by the Housing Department from public rental housing tenants, in order to prevent overpayments to welfare recipients.
民政事務局 Home Affairs Department	把民政事務局從村代表選舉參選人及選民登記申請人收集的個人資料，與選舉事務處從地方選區選民登記收集的個人資料互相比較，以確定申請人在村代表選舉的投票及被提名資格。 Comparing the personal data collected by the Home Affairs Department from applicants for elector and voter registration for the Village Representative Election with the personal data collected by the Registration and Electoral Office for voter registration for Geographical Constituencies, in order to determine the applicants' eligibility to vote and be nominated as candidates in the Village Representative Election.
香港房屋協會 Hong Kong Housing Society	把香港房屋協會從樓宇更新大行動長者自住業主津貼申請人收集的個人資料，與市區重建局從各類津貼及免息貸款計劃收集的個人資料互相比較，以避免有人獲得雙重津貼。 Comparing the personal data collected by the Hong Kong Housing Society from applicants of the scheme for Operation Building Bright Grant for Elderly Owner-Occupiers with the personal data collected by the Urban Renewal Authority from the applicants of various grant and interest-free loan schemes, in order to prevent double subsidies to applicants.
政府資訊科技總監辦公室 Office of the Government Chief Information Officer	把政府資訊科技總監辦公室從上網學習支援計劃申請人收集的個人資料，與社會福利署綜合社會保障援助計劃受助人的個人資料互相比較，以確定申請人的資格及避免公共資源遭濫用。 Comparing the personal data collected by the Office of the Government Chief Information Officer from applicants of the Internet Learning Support Programme with the personal data collected by the Social Welfare Department from the beneficiaries of the Comprehensive Social Security Assistance Scheme, in order to ascertain the eligibility of the applicants and prevent the abuse of public resources.

「全球私隱執法機關網絡」的聯合行動 - 本地 60 款智能手機應用程式的抽查結果

公署檢視本港智能手機程式的私隱政策透明度

2013 年 5 月，公署抽查了 60 款由本港開發的智能手機應用程式，結果顯示它們的私隱政策透明度普遍不足。

抽查的 60 個樣本（54 個為免費程式）當中，來自 Apple App Store 和 Google Play Store 的各佔一半 ，並分屬 16 個類別。

私隱政策透明度不足

智能手機用戶常於手機儲存多種私人資料，即使未必所有資料均符合條例下「個人資料」的定義，開發商宜採納公署就擬備私隱政策聲明所建議的良好行事方式，向用戶說明如何處理個人資料和 / 或保障私隱的安排。程式開發商 / 供應者如要收集和使用程式用戶的個人資料，須依從私隱政策透明度的原則，為用戶提供方便瀏覽、易於閱讀和易於明白的收集個人資料聲明。

在抽查中，僅六成程式在其網站備有私隱政策聲明，但絕大部分都沒有解釋程式讀取手機上哪些資料以及目的。其他出現的問題，包括中文程式卻只提供英文版的聲明；有私隱政策聲明長達 292 行，但只能以每次八行的形式瀏覽。

INTERNET PRIVACY SWEEP EXERCISE – LOCAL SURVEY RESULTS OF 60 SMARTPHONE APPS

The PCPD Examined Privacy Policy Transparency for Local Smartphone Applications

In May 2013, the PCPD conducted a survey of the 60 most popular smartphone applications ("apps") developed by Hong Kong entities and found that their privacy policy transparency was generally inadequate.

The 60 apps, 54 of which were free, were evenly selected from the Apple App Store and Google Play Store and covered 16 app categories.

Inadequate transparency in privacy policy

Smartphone users often store private data on their smartphones. Even though not all such data may come under the meaning of "personal data" under the Ordinance, app developers are advised to adopt the PCPD's recommended practices on preparing a Privacy Policy Statement ("PPS") and state how they handle personal data and/or protect their users' privacy. If app developers/providers collect and/or use personal data, they should comply with the principle of transparency and make their relevant Personal Information Collection Statement ("PICS") available to their data subjects in a manner that is easily accessible, readable and understandable.

In the survey, only 60% of the apps were found to have provided a PPS on their websites, but most of these did not explain what smartphone data they would access and the purpose of the access. Other issues included providing an English-only PPS even for Chinese apps or showing a 292-line PPS in an eight-line window on the website.

手機應用程式私隱政策聲明出現的問題
Issues found in PPS of smartphone apps

私隱政策聲明出現的問題 Issues in PPSs	程式數目 No. of apps 總數 Total：36（百分比 %）
沒有解釋程式讀取每項資料的目的 No explanation of the purpose for accessing each type of data	35 (97)
並非為該程式而編寫 Not tailored for the specific app	33 (92)
與應用程式採用的語言不一致，或編排非易於閱讀 Couched in a language different from that used for the app, or not easily readable	4 (11)

潛在的私隱風險

結果亦發現，應用程式會查閱手機的私人資料種類各有不同，被抽查的 60 個程式，可查閱一至八項私人資料不等。可讀取不同種類資料的程式數目如下：

Potential privacy risks

The types of private data accessed by apps also varied, ranging from one to eight different types of private data. The number of apps accessing each type of data was as follows:

讀取資料種類 Types of data accessed	**程式數目 No. of apps** 總數 Total：60（百分比 %）
手機獨特識別碼 Unique phone identifier	44 (73)
定位位置 Location data	34 (57)
用戶登入不同程式的帳號 Account information stored on the phone	21 (35)
手機正在執行的應用程式 List of apps running on the phone	13 (22)
使用手機攝影功能或麥克風 Camera/microphone function	10 (17)
SMS/MMS 訊息 SMS/MMS messages	8 (13)
通話紀錄 Call logs	6 (10)
通訊錄 Address book	6 (10)
日誌內容 Calendar details	1 (2)

雖然有些人會認為讓程式讀取上述的資料無傷大雅，但用戶應留意，不同程式讀取零碎的資料後，資料可能會被整合，而經整合後的資料對個人私隱造成風險。舉例說，程式甲收集了某君的手機獨特識別碼和定位位置，程式乙則讀取了其手機獨特識別碼和手機內儲存某君的社交網帳號。即使某君沒有在社交網「打卡」，若兩個程式收集的資料經過整合和串連，便可得知其社交網帳號的行蹤。

While some smartphone users may consider access to the data mentioned above harmless, they should be aware that bits and pieces of private data gathered by different apps may give rise to privacy concerns. For example, App A collects User X's unique phone identifier (IMEI number) and location data from X's smartphone, while App B collects the same IMEI number and X's social network account stored on the phone. If the data collected by the two apps is combined and correlated using the IMEI number, the location data of X's social network account may become trackable by parties who have access to the data collected by both apps. This is done even if X has not "checked in" his/her social network account.

公署的建議

應用程式開發商應參閱公署發出的《保障個人資料私隱：流動應用程式開發商及其委託人須知》資料單張。他們只應讀取程式所需的資料種類，並確保其《收集個人資料聲明》是按其特定的程式而編寫。他們應清楚表明其程式會否讀取智能電話的資料；如會，會讀取哪類資料及其原因，以及如何進行，以便用戶就是否使用該程式作出知情決定。

智能電話用戶應在安裝程式前閱讀其私隱政策。他們應定期檢視權限設定（如其電話的操作系統有提供此項設定），以防止程式讀取不必要的資料，例如定位位置資料。他們亦應把可疑程式及不再需要的程式卸載，以減低資料外洩的風險。更多相關保障資料的建議，可瀏覽公署的專題網站「網上私隱要自保」www.pcpd.org.hk/besmartonline。

The PCPD's recommendations

App developers should refer to *"Personal Data Privacy Protection: What Mobile Apps Developers and Their Clients Should Know"* issued by the PCPD. They should only access the types of data necessary for the app, and ensure that their PPSs are tailored for their particular apps. They should state clearly whether the apps would access data on the smartphones and what types of data would be accessed, why and how such access would be carried out so that users may make an informed decision whether or not to use the app.

Smartphone users are recommended to read the privacy policy of an app before installing it. They should regularly review their permission settings, if available on their smartphone operating system, to prevent the app from accessing unnecessary data such as location data. They should also uninstall dubious apps and those no longer needed to minimise the risk of data leakage. They may visit the PCPD's thematic website www.pcpd.org.hk/besmartonline for more advice on this.