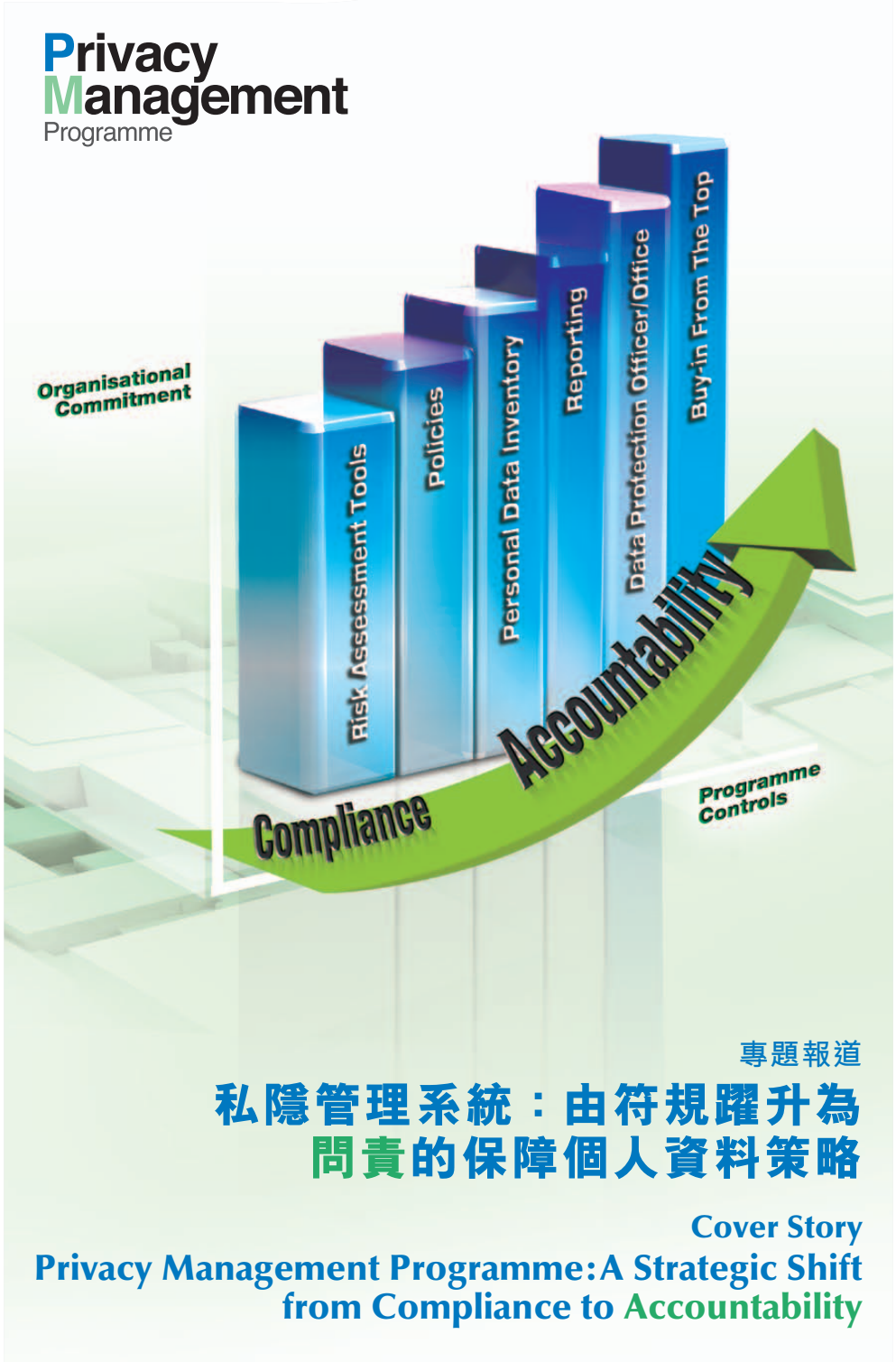
PCPD NEWS
私隱專員公署通訊
二零一四年四月 April 2014 | ISSUE NO. 29



專題報道

私隱管理系統：由符規躍升為問責的保障個人資料策略

Cover Story
Privacy Management Programme: A Strategic Shift from Compliance to Accountability

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data Hong Kong

www.pcpd.org.hk

私隱管理系統：由符規躍升為問責

Privacy Management Programmes: A Strategic Shift from Compliance to Accountability

私隱管理系統
Privacy Management Programme

面對公眾對保障個人資料私隱與日俱增的期望，以及大數據帶來更高的潛在私隱風險，個人資料私隱專員提倡機構把保障個人資料提升為良好管治必要的責任，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。

政府和本港39間保險業、電訊業及其他業界處理大量市民個人資料的機構響應公署的號召，承諾引入以問責為本的私隱管理系統。

In response to rising public expectations for privacy protection, along with increased privacy risks brought about by the era of Big Data, the Privacy Commissioner for Personal Data 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.

The government, together with 39 companies handling vast volumes of personal data from the insurance, telecommunications and other sectors, have made a pledge to implement an accountability-based privacy management programme ("PMP").

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）、25間保險公司、九間電訊公司和五間其他業界的公司承諾在機構內推行**私隱管理系統**。名單詳見www.pcpd.org.hk/pmp。

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。

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》下的規定，而是「資料使用者申報計劃」（見第4頁背景資料）的過渡期替代方案。

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。穩妥的私隱管理系統基建應具備以下特點：

- 有機構最高管理層的決心和支持，並成為機構管治架構不可或缺的一環；
- 待私隱和個人資料保障為跨部門的事宜，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；
- 參照私隱風險估的結果制訂適當的防範措施；
- 確保所有措舉、項目和服務都顧及保障私隱的考慮；
- 設立資料外洩或個人資料私隱事故的應變計劃；
- 設立內部的監督和檢討機制；
- 合時宜，能夠追隨私隱生態系統的迅速轉變，保持實用和有效；
- 有適當的資源配合和專責人員處理。

私隱管理系統的組件
Building Blocks of PMP

<table>
<tr><td colspan="3">機構的決心
Organisational Commitment</td><td colspan="4">系統監控
Programme Controls</td></tr>
<tr><td rowspan="2">最高層的支持
Buy-in from the top</td><td rowspan="2">保障資料主任／部門
Data protection officer/office</td><td rowspan="2">匯報機制
Reporting</td><td>個人資料庫存
Personal data inventory</td><td>保障個人資料的政策
Policies on data protection</td><td>風險評估工具
Risk-assessment tools</td></tr>
<tr><td>培訓及教育推廣
Training and education requirements</td><td>資料外洩事故的應變機制
Breach handling</td><td>對資料處理者的管理
Data-processing management</td><td>溝通
Communication</td></tr>
<tr><td colspan="6">持續評估及修訂
Ongoing Assessment and Revision Plan</td></tr>
<tr><td colspan="3">監督及檢討計劃
Oversight & Review Plan</td><td colspan="3">按需要評估和修訂系統監控
Access and Revise Programme Controls Where Necessary</td></tr>
</table>

推行得宜 加強競爭優勢

個人資料私隱專員蔣任宏在私隱管理系統推展儀式上指出：「從我們的規管經驗所見，若機構只視個人資料私隱保障為循規的法律事宜，而欠缺機構最高管理層的參與，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。全面的私隱管理系統不單可協助機構有效地遵從條例的規定，而且有助建立和推動尊重私隱的機構文化，有利於與客戶、僱員、股東及監管機構建立互信關係，提升機構的聲譽，從而加強其競爭優勢。」

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，資料外洩的代價亦相當大。

不少組織及機構持有大量的個人資料，資料的經濟價值日增，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。

蔣任宏希望承諾推行私隱管理系統的機構履行責任，為其他資料使用者樹立良好榜樣。

Over the 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 PMPs in the sectors concerned. As at 18 February 2014, the following organisations have pledged to implement **PMP**: the HKSAR Government (including all bureaux and departments), 25 insurance companies, nine telecommunications companies and five companies from other sectors. The list of pledging organisations is available at www.pcpd.org.hk/pmp.

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

What is a PMP?

A PMP is not a legal requirement provided in the Personal Data (Privacy) Ordinance (the "Ordinance"), but an interim substitute for the Data User Return Scheme ("DURS") (see backgrounder on page 4).

A PMP serves as a strategic framework to assist an organisation in complying with legal requirements of the Ordinance, as well as privacy risk management. A 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 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.

A PMP Can Create a Competitive Edge

Speaking at the PMP pledge ceremony, the **Privacy Commissioner for Personal Data, Mr Allan Chiang**, remarked, "Our Regulatory experience has shown time and again that privacy and data protection cannot be managed effectively if they are treated merely as a legal compliance issue, with little or no involvement of top management. 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,

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間來自保險業及其他行業的機構進行私隱管理系統。

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.

operational processes, product and service design, physical architecture and networked infrastructure. At the minimum, the outcome of this holistic approach is a demonstrable capacity to comply with the legal requirements of the Ordinance. 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."

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.

私隱專員寄語與會人士，在2014年把私隱管理系統變成各自機構內的熱門詞語。

Privacy Commissioner appeals to the Conference participants to make Privacy Management Programmes the buzz word in their organisations in 2014.

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.

Mr Chiang hopes these organisations will fulfill their pledges thus setting an example of responsible privacy management for other data users to follow.

背景資料：

「資料使用者申報計劃」vs「私隱管理系統」

根據《個人資料(私隱)條例》第IV部，私隱專員有權推行「資料使用者申報計劃」(Data User Return Scheme)，要求指定類別的資料使用者呈報所持有的個人資料詳情，例如資料類別和用途；私隱專員並可將申報資料匯編成資料使用者登記冊，供公眾查閱。

公署於2011年7月就實施「資料使用者申報計劃」諮詢公營機構、銀行、電訊和保險等四個界別(計劃實施第一階段受影響的行業)。有關業界的團體認同有需要提升保障個人資料私隱的水平，但呈報計劃的形式則有所保留。

本港的「資料使用者申報計劃」借鑑歐盟的資料保障制度，而歐盟於2012年起在這方面醞釀改革，考慮摒棄資料使用者呈報的安排，取而代之，是著重收集和使用個人資料須具問責性和透明度的改良制度。歐盟在商議中的建議包括強制規定(一)公營機構及(二)私營機構凡於任何連續12個月內處理超過五千名人士的個人資料，均須設立資料保障主任的職位。鑑於上述形勢，公署計劃暫緩在本港推行「資料使用者申報計劃」，直至歐盟改革完成為止，以便從中汲取經驗。

Backgrounder:

DURS vs PMP

Part IV of the Ordinance provides for a DURS, under which specified organisations are obliged to notify the Commissioner of "prescribed information", which includes the kinds of personal data they control and the purposes for which the data are held. The Commission may create a register of the returns and make it available to the public.

In July 2011, the PCPD consulted the banking, telecommunications, insurance and public sectors (those sectors to be covered in the initial phase of DURS implementation) on the operational framework and implementation plan of the DURS. There was no dispute over the objective of promoting a higher standard in the protection of personal data privacy, but the consultees had considerable scepticism about achieving this objective with the DURS scheme.

At the same time, the PCPD has learned that the European Union (EU) data protection system, upon which Hong Kong's DURS is modelled, is undergoing reform. Among other things, the EU is considering replacing the notification requirement with new and improved systems which emphasise accountability and transparency in the collection and use of personal data, including the mandatory appointment of a data protection officer in (a) public authorities and bodies, as well as (b) private enterprises that process data of more than 5,000 persons in any consecutive 12 months.

In light of the reform, the PCPD decided to put the project on hold until the reforms in the EU have been finalised, and useful lessons can be learnt from the exercise.

公署倡導私隱管理系統的工作
What Has the PCPD Done to Promote PMP?

2013

在2013年，私隱專員及他的團隊與政府、銀行業、保險業及電訊業舉行一連串的會議，尋求他們支持私隱管理系統。
Throughout 2013, the Privacy Commissioner and his team held a series of discussion meetings with the Government, the banks, the insurance companies and the telecommunication service providers to seek their buy-in of PMP.

12月17日－個人資料及私隱保障CEO專題早餐會議
17 December – CEO Breakfast Meeting on Privacy and Data Protection

前英國個人資料專員Richard Thomas來港分享個人資料保障對企業管治的重要性，有近70名行政總裁和高層行政人員、及至行政會議成員陳智思先生和立法會政制事務委員會主席譚耀宗先生出席。

Mr Richard Thomas, the former UK Information Commissioner, was invited to share his views on the importance of data protection from a corporate governance perspective. The talk was well attended by some 70 CEOs and senior executives of local organisations. Among the attendees were Executive Council member the Honourable Bernard Chan and Chairman of the Legislative Council Panel on Constitutional Affairs the Honourable Tam Yiu-chung.

2014

1月17日－向政府部門首長作簡報
17 January – Briefing to Department Heads of the HKSAR Government

私隱專員出席由政務司司長主持的部門首長會議簡介公署這方面的工作。

Privacy Commissioner was invited to a meeting of Department Heads chaired by the Chief Secretary.

2月11日－保障私隱與企業管治國際會議
11 February – International Conference on Privacy Protection in Corporate Governance

逾250名與會人士就如何在各自的機構內建立及推行私隱管理系統向本地和海外講者汲取實際經驗。

Over 250 participants picked up practical advice from local and overseas privacy professionals on how to build and maintain a PMP in their organisations.

2014

2月12日－私隱影響評估專業研習班
12 February – Professional Workshops on Privacy Impact Assessment

由個人資料私隱策略顧問、前任澳洲私隱專員Malcolm Crompton 講授兩節研習班，逾120人參加。

More than 120 people attended two workshops delivered by Mr Malcolm Crompton, a data privacy strategies consultant and former Australian Privacy Commissioner.

2月18日－出版《私隱管理系統最佳行事方式指引》
18 February – Release of Privacy Management Programme: A Best Practice Guide

公署出版《私隱管理系統最佳行事方式指引》，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，扼述私隱管理系統作為保障個人資料私隱策略框架的必需組件，提供原則性的建議。

The PCPD published the Privacy Management Progamme: Best Practice Guide to help organisations develop and improve privacy management programmes according to their specific circumstances, considering factors such as the organisation's size, the nature of its business, and the amount and sensitivity of the personal data it collects and manages. The Guide outlines the building blocks of PMPs and provides guidance.

下載「最佳行事方式指引」Download "Best Practice Guide"：
www.pcpd.org.hk/pmp/guide.html

2月18日－私隱管理系統推展儀式
18 February – Privacy Management Programme Pledge Ceremony

政制及內地事務局副局長劉江華為私隱管理系統推展儀式的主禮嘉賓。在特區政府、香港保險業協會和香港通訊業聯會的協力提倡下，香港特別行政區政府與25間保險公司、九間電訊公司及五間其他行業的機構，均承諾推行保障私隱系統。

Officiating at the pledge ceremony is Mr Lau Kong Wah, Under Secretary for Constitutional and Mainland Affairs. With the tremendous support of the HKSAR Government, the Hong Kong Federation of Insurers, and the Communications Association of Hong Kong, pledges to implement PMPs were made by the HKSAR Government bureaux and departments, 25 companies from the insurance sector, nine companies from the telecommunications sector, and five organisations from other sectors.

經驗之談：從良好企業管治中實踐私隱管理系統

Experience Sharing for Privacy Management Programmes in Good Corporate Governance

在公署於2014年2月18日舉行的保障私隱與企業管治國際會議上，多位講者從理論和實踐的層面，分享建立和推行私隱管理系統的經驗。《私隱專員公署通訊》為大家輯錄箇中精華。

An International Conference on Privacy Protection in Corporate Governance was organised on 18 February 2014. During the conference, speakers shared their views on the theory and practice of how to develop and maintain a sound PMP. PCPD News recaps some of the highlights here.

講者在國際會議上的簡佈：www.pcpd.org.hk/privacyconference2014

Presentation slides are available on the Conference webpage: www.pcpd.org.hk/privacyconference

Mr J Trevor Hughes

美國國際私隱專業人員協會（IAPP）主席及行政總裁

President and CEO, International Association of Privacy Professionals (IAPP), US

有效的私隱管理系統，必須建基於私隱意識和問責性之上。問責的機構在不同方面都要有良好的私隱管理，輔以相關的保障私隱知識和技能。不論是人力資源、財務、市場推廣等，所有範疇的人員都需要對私隱保障有所認識，才可在日常處理個人資料時作出明智的決定，這亦是新時代對私隱專業人員的要求。機構可能有最優秀的律師和專責私隱保障人員，但如果做決定的人不諳私隱，可足令機構陷入危機，因此機構不單要培訓核心的保障私隱團隊，還必須為員工就不同範疇的私隱事宜提供培訓。

The foundation of any effective privacy programme is privacy awareness and accountability. In an accountable organisation, good privacy programme management – with privacy knowledge and privacy skills – must be present in many different areas: human resources, finance, marketing, and so on. Professionals in these departments need to understand privacy issues so as to make good decisions every day when handling data. That is the definition of the new era of accountable privacy professionals. You may have the best lawyer and privacy officer, but if one person who makes a decision doesn't understand privacy issues and risks, then the whole organisation is at risk. Therefore, many organisations train not only a good core privacy team about privacy issues, but also many other staff from different departments.

鍾王穎婷女士

Mrs Elaine Chong

中華電力香港有公司

General Counsel, CLP Power Hong Kong Limited, Hong Kong

建立和推行私隱管理系統，可為企業和顧客創造雙贏局面。尊重顧客和建立超越符規的文化，是驅使中電追求完備的私隱管理系統的原動力。在建立有效的私隱管理系統的過程中，與前線人員保持雙向對話，以及善用科技處理網絡保安和預防資料外泄或損失，也相當重要。

另外，在推出新的服務或產品前，應進行資料影響評估，以確保機構公平使用相關的個人資料，同時找出對策減低潛在的私隱風險，諸如儘量減少使用個人資料和在傳輸前把資料加密。

在執行方面，強而有力的領導至為重要。發生事故時冷靜地建議如求補救的醫生；嚴厲執行私隱政策的「虎媽」；能夠洞悉各種潛在風險的偵探，抑或是滿腔熱誠，悉心培育尊重私隱文化的園丁，以上多個角色，得由個別的機構抉擇最合適的風格。

The development and implementation of a PMP can create a win-win situation for both the company and its customers. Respect for customers and fostering a "beyond compliance culture" have been the motivation for CLP to develop a comprehensive PMP. To establish an effective PMP, it is also important to establish two-way communication between the privacy team and front-line staff, and leverage technology tools for cyber security and data-loss prevention.

Conducting a data-impact assessment before putting out a new service or product can help ensure that the company uses the personal data involved fairly and effectively mitigates the potential privacy risks by, for example, using as little personal data as possible, and using encryption when transmitting data.

When implementing a PMP, strong leadership is essential. You have to be a doctor, calmly providing a remedy when an incident occurs, a 'tiger mum', enforcing privacy policy in the company, a detective, tracing all potential risks, and a passionate gardener, nurturing your creation on a daily basis so that the culture of respect for personal data in your organisation grows stronger and better. It is up to companies to distinguish which winning style they would like to use.

Ms Bojana Bellamy

英國Hunton & Williams
資訊政策領導中心主席

President, Centre for Information Policy Leadership at Hunton & Williams, UK

全球各地保障個人資料私隱的法例不斷發展，科技的演進和全球化，再加上電子數據為本的新經濟體系盛行，個人資料和私隱保障的法規和符規要求也相應出現新的模式。新模式不再單純以法律常規為依歸，而是著眼於機構在收集、使用和分享資料時的問責性。具問責性和負責任的個人資料私隱管理系統，已成為企業管理不可或缺的一環，對營商無往而不利，有助增加競爭優勢。

The proliferation of data privacy laws across the globe, the transformation and globalisation of technology, and the rise of a digital, data-based economy call for a new approach to data privacy regulation and compliance – one that is based not solely on legal norms, but on the accountability of organisations that collect, use and share data. The accountable and responsible management of data and privacy has become an integral part of corporate governance, a business enabler and a competitive differentiator.

鄭衛賓先生
Mr Chris Cheng

香港電訊集團高級法律顧問

Senior Group Legal Adviser HKT Group, Hong Kong

電訊業已邁進以客本的紀元，資料使用者與規管者和資料當事人保持溝通對話是十分重要的。香港電訊在符規方面的標準，有兩項基本要求：公平和透明度。在透明度方面，職員應按「有需要知道」的原則查取客戶的個人資料；機構應在儘早的階段告知客戶他們所提供的資料的用途，這樣才可以讓客戶真正明白和同意個人資料的使用。藉著參與私隱管理系統，我們向公眾傳達出的訊息是香港電訊時刻遵從法律，和公平地使用顧客的資料。

The telecommunications industry has moved into a "customer-centric" universe. Dialogue amongst regulators, data users and data subjects is of growing importance.

The standard of our compliance has always been based on two basic requirements: fairness and transparency. Regarding fairness, staff can access customer data only on a need-to-know basis, and regarding transparency, customers are informed about the use of their data at the earliest convenience, and they must genuinely consent to the use of their personal data. By implementing and following a PMP, we are sending a message to the public that HKT is a fair, law-abiding user of our customers' personal data.

Ms Karinna Neumann

加拿大Nymity認可
私隱保障專業人員

Certified Privacy Professional Nymity, Canada

私隱管理系統的基本組件是問責性，而達致問責性，機構須具備多項關鍵的條件，包括維繫一個有效私隱保障制度的責任，在處理個人資料過程中推行有利私隱保障的活動；機構內需要有視私隱管理系統為己任的人，對私隱管理活動的統籌和監督瞭如指掌的人。機構亦要需要在私隱管理活動完成後加以紀錄。

在這實行問責制度的框架之下，機構應首先訂立私隱管理活動作基準，然後規劃所需要的措施，根據已界定的範圍、業務個案、時序和資源把活動付諸實行。機構可參閱Nymity出版的書籍Practical Guide to Building Accountability through an Effective Privacy Programme。

The fundamental component for an effective privacy programme in an organisation is accountability. The key elements of accountability include responsibility for maintaining an effective privacy programme and activities that have a positive impact on the processing of personal data; ownership, in terms of individuals answerable for the management and monitoring of privacy management activities); and evidence of the completion of privacy management activities.

Under the framework for implementing accountability, organisations should, in the first place, set up a baseline for privacy management activities; plan which measures should be implemented in a privacy programme; and put the activities into place according to a determined scope, business situation, sequence and resources.

Organisations may refer to the Nymity publication Practical Guide to Building Accountability through an Effective Privacy Programme for more information.

張耀堂先生
Mr Sunny Cheung
八達通控股有限公司行政總裁
Chief Executive Officer
Octopus Holdings Limited, Hong Kong

不止於守法，要做對的事。如果你只是做合法的事，你的顧客難免會向你表示不滿，要求你做得更好。預防勝於治療，遇有疑問，最好是問顧客提供答案。

八達通近年引入了全面的企業管治框架，以回應個人資料、顧客保障和風險評估等方面的挑戰。保障個人資料私隱是產品及服務開發過程中必須考慮的因素。機構又採用職責劃分和雙重監控的制度，任何個人資料的提取和銷毀都需要起碼兩名專責人員核准。

機構的首席風險主任本身是管理層的一員，他兼顧個人資料私隱和保障顧客兩方面的工作。每當大家醞釀和討論新措施，新產品或程序，首席風險主任都會參與，即時探討和評估相關的潛在私隱風險。

在開發流動應用程式方面，收集個人資料面對的一大挑戰是處理透明度和可讀性兩者之間的予盾。八達通採用「可免則免」的原則去收集個人資料。以 OctoCheck 程式為例，程式並無收集可識別個人身份的資料或位置資料；用戶登記時只需提交部分的八達通帳戶資料。另一款獎賞程式亦沒有收集顧客的身份證明資料；只有在顧客同意的情況下才會收集位置資料，從而為顧客提供鄰近商舖的定位服務。

We need to do not just enough to satisfy the legal requirements, but what is right. Even 'legally right' does not protect a company from dissatisfied customers, as they always demand something more. Prevention is better than cure; in the case of doubt, it is good to ask your customers.

Octopus has responded to these challenges with an all-round corporate governance framework addressing the issues of personal data, customer protection and risk assessment. Octopus has embedded personal data privacy in its product and service development, and has adopted a programme of segregation of duties and dual control. The extraction and destruction of data require the approval of at least two designated persons.

The Chief Risk Officer [of the company], who looks after both data privacy and customer protection, is also a member of the management team. When we talk about new measures, products or procedures, the Chief Risk Officer is present to identify the potential risks so that we can do a risk assessment on the spot.

Regarding mobile app development, one of the main challenges is to deal with the paradox of transparency versus readability in data collection. Octopus has adopted the principle of "always collect the minimum". For the OctoCheck app, neither personally identifiable information nor location data are collected. Only a partial Octopus ID is used for registration. In the case of the rewards app, no personally identifiable data is collected from customers. Location data is collected only with the consent of customers for the provision of customer service, by helping them locate the nearest merchants.

Mr Mikko Niva
芬蘭諾基亞私隱保障總監
Director of Privacy, Nokia Corporation, Finland

全球科技環境變得愈來愈複雜，臨急抱佛腳式，欠缺協調的措舉難以妥善地保障個人資料私隱。法規、技術和標準、問責性和倡導保障私隱，才是回應當下這複雜環境的良策。

尊重個人私隱是諾基亞私隱管理系統的核心價值，問責、公平和合法地處理個人資料、採用貫徹私隱保障的設計、通知和取得當事人的同意、選擇和參與、收集和用途限制、資料管理，披露資料的限制和保安等等，這些都是機構每位員工恪守的原則。機構不容任何隱瞞式的，沒有監控或保安措施的或過度的個人資料處理活動。

在評估私隱影響時，單是著眼於產品是不夠的，還要看產品整個生命周期會涉及的個人資料。換言之，我們要仔細檢視個人資料如何經由用戶經應用程式或流動裝置流向支援的後勤系統，以及市場推廣、數據分析及廣告代理等第三方。如過程涉及數據流的分拆，資料由多個資料使用者操控，或個人資料遍佈廣泛的地區，事情就更加複雜。

The global technology environment is getting so complex that it is impossible to get it right through uncoordinated, ad hoc activities. Regulations, technology, standards, accountability and privacy engagement are some of the tools organisations can use to deal with the complexity.

At Nokia, respect for individuals' privacy is at the heart of our privacy management programme. Everyone observes the principles of accountability; the fair and lawful processing of personal data; Privacy-by-Design; notice procedures; customer consent, choice and participation; collection and purpose limitation; responsible data management; limited disclosures; and security safeguards. No hidden, uncontrolled, excessive or unsecure processing of personal data is allowed.

Regarding privacy impact assessment, it is not enough to look at the product alone, but at the complete life cycle of the associated personal data. This involves examination of the data flow from users, via an app or device, to the supporting backend systems and third parties, such as marketing, analytics and advertising agents. The data chain becomes more complex with the physical separation of the data flow components, with data being held by different controllers, and with the data spread over geographical regions.

Ms JoAnn Stonier

美國萬事達全球行政副總裁、首席資訊管治及私隱主任

Executive Vice President Chief Information Governance and Privacy Officer, MasterCard Worldwide, US

資訊管治，就是確保機構以統一和全面的方針，使用和保護公司各業務範疇的資訊資產，從而創造效益，以及為資料的使用制立常規和程序。在萬事達，資訊管治職能包括負責建立一套全面的程序，優化機構內數據主導的決策過程，在迎合客戶和市場期望的同時，在創新、資訊操守、私隱和法例規定之間取得平衡。

機構曾推出一個項目，涉及全球超過22個網站為提供優惠和市場推廣目的而收集顧客的個人資料。如何遵從不同地方的資料保障法規；如涉及跨境的推廣，如何處理更為複雜的符規要求；當機構擬把資料用於比客戶同意的範圍更廣的用途時，如何處理，這些都是機構需要照顧的。為此，萬事達創出MasterCard ID ，確保所有網站在收集個人資料方面推行一致的常規，以及容許用戶經中央系統管理他們的喜好。這系統更可以識別持咭人來自哪個國家，從而保證提供優惠的方式與用戶知悉的私隱政策聲明和已同意的細則脗合。隨著資料使用方式的演變，這系統更有助企業向客戶就新的情況徵求同意。

Information governance is the process of ensuring a consistent and comprehensive approach for the use and protection of the company's information assets across all business initiatives, in order to create better efficiencies, practices and processes for data use.

The Information Governance Department at MasterCard is responsible for establishing a comprehensive process to improve data-driven decisions across the enterprise, balancing innovation, information, ethics, privacy and regulatory requirements, while meeting customer and market expectations.

For example, there was a global campaign involving the operation of more than 22 websites around the world that collected personal data for offer fulfilment and marketing purposes. There were several issues to address: the challenges of complying with different data protection regulations, the additional complexity of legal compliance in the case of cross-border promotions, and the desired uses of data being broader than current scope of consent. MasterCard created a MasterCard ID to implement consistent data collection practices across all sites and enable users to manage their preferences through a centralised infrastructure. It is also able to recognise the cardholders' country of origin and thus provide offers in a manner which is consistent with the privacy notice given and consent the cardholders have given. The system will be used in the future to obtain additional consents from customers as the use of data evolves.

Mr Scott Taylor

美國惠普公司副總裁和首席私隱主任

Vice President and Chief Privacy Officer Hewlett-Packard Company, US

要實行有效的個人資料私隱管理，機構便需要作出根本的轉變，由關注「法律責任」轉為「問責」。換言之，機構在作出決定前，必須考慮相應的風險，以法律責任以外的一套道德和價值標準作為依歸。機構所有員工須責成管理他們掌管的個人資料。

問責的機構應具備完善的系統，藉以評估個人資料私隱方面的風險，減低風險和推行符規的項目，並持續評估推行的成效。此外，機構應向內部人員和外界的持份者展示它們有能力妥善管理私隱風險。

Effective data privacy management requires a fundamental shift from liability to accountability. This means that when decisions are made, they take into account the concurrent risks beyond strict liability using ethics- and value-based criteria. All employees in the organisation are accountable for the stewardship of the data under their charge.

Accountable organisations should have comprehensive programmes to assess and risk, implement compliance programmes, and continually evaluate the effectiveness of implementation. In addition, organisations should stand ready to demonstrate their privacy management capacity to both internal and external stakeholders and data subjects.

Mr Malcolm Crompton

會議主持、Information Integrity Solutions Pty Ltd董事總經理

Moderator of the conference discussions; Managing Director of Information Integrity Solutions Pty Ltd

個人資料可謂是新興的資本類別，用得愈多，其價值就愈高。不過，究竟個人資料的私隱和保安，兩者之間有何分別？簡而言之，資訊保安旨在確保機構妥善地掌管其持有的資產，資料從何處得來，打算怎樣使用資料，都一清二楚。至於個人資料私隱的保障，前提是上述各項已得到肯定，機構須多做一步，主動監控，確保機構盡責地處理個人資料。如果你的機構只做到資料保安的水平，那即是說在私隱管理之路才剛起步。

Personal information is the new asset class – the more you use it the more valuable it is. But what is the difference between privacy and security with regards to personal information? Security is about assuring the asset in your organisation is under your control. You must know where you obtain the information, and what you are going to do with it. Privacy of personal information assumes all of the above is achieved, plus the active exercise of control to ensure your organisation is handling the personal data responsibly. If you have only security, then your journey to privacy management has just begun.

海外代表團與本地私隱保障專家交流

Overseas Delegation Exchanges Views with Local Privacy Professionals

在保障私隱與企業管治國際會議(「國際會議」)舉行前，私隱專員蔣任宏於2014年2月10日接待本地私隱保障專家，及由資訊政策領導中心(CIPL)率領訪港的代表團，成員包括跨國企業私隱保障主管。

As a side programme to the International Conference on Privacy Protection in Corporate Governance ("International Conference"), Privacy Commissioner Mr Allan Chiang hosted a meeting on February 10, 2014 between local privacy professionals and a delegation of chief privacy officers from multinational corporations, led by the Centre for Information Policy Leadership ("CIPL").

私隱專員安排本地私隱保障專家及學者與CIPL的企業代表團會晤，就多個有關私隱議題(包括大數據分析)進行交流和討論。

Privacy Commissioner engages local privacy advocates and academia with the CIPL delegation in a privacy dialogue. Views were exchanged on a number of privacy issues, including Big Data and analytics.

在會上，海外的資料私隱保障專家與本地研究私隱保障的學者及持份者就不同有關私隱議題進行交流，包括大數據分析、個人資料匿名化、私隱風險管理，以及互聯網的使用。

香港大學社會科學研究中心總監及公署科技發展常務委員會成員白景崇教授在會上擔任主持人。

代表團成員**IBM首席私隱主任Christina Peters**指出，基於新的科技發展令資料極速流轉，以致法律難以追得上急速的科技發展。她解釋，現今的挑戰是協助機構了解它們在保障個人資料私隱方面的選擇，並向它們提供實際的業務解決方案，讓它們繼續遵從法律要求和尊重客戶的權利。她表示：「除非客戶信任我們，否則我們的業務難以蓬勃發展。」

芬蘭諾基亞私隱總監Mikko Niva將保障私隱比喻為一場有多重陣地的戰爭，他建議公司制訂一套依從私隱原則的全面計劃。「首要工具是法律及相關條例。接著是機構的問責性。一個有意義的框架可以令機構變得負責任。」

Mikko Niva強調，科技保障的標準化是需要注視的重要新範疇。他說：「如果基礎的科技不支持資料私隱保障，我們的努力便會白費。」

他預期私隱專業人員日後需要更多元化的技能：「私隱保障專業人員不再只是來自法律界，僅是提供指導和回答問題。例如，日後將會有私隱工程師的出現，因為我們需要大量的保安設計，以防止風險。」

代表團亦強調將公平原則付諸實行的重要性。**萬事達卡首席私隱主任JoAnn Stonier**認為機構內每個人都需要對個人資料私隱有一定程度的理解，而在處理資料的收集、分析及應用時，需要在整個機構貫徹道德準則。她補充，公平不只是限於向顧客發出通告。

白景崇教授和應JoAnn Stonier的說法，他以八達通事件為例，述說香港市民的個人資料如何被不公平地處理。

惠普的首席私隱主任Scott Taylor在講述如何為資料收集及保障創造一個健康的環境時，把大數據分析中的資料保障比喻為減少空氣污染。他表示，要保持環境盡量健康，是需要多項規例、企業負責任的回應，以及資料當事人的參與。「空氣不是時刻絕佳，但我們現在所做的，已比三十年前好。」他說。

與會者亦討論了目前法律能否滿足科技發展的需要。

白景崇教授指出，雖然目前的法律有缺點，但以原則為本的私隱法例本身是健全的。「我們要區別究竟是原則有弱點，還是在特定的法律框架中執行原則有弱點。」

他表示匿名化不再是私隱保障的有效解決方案。他舉例說，在敏感資料方面，我們必須區分不能改變的生物辨識資料(如DNA)與其他個人資料(如銀行記錄)。將某人的DNA資料匿名化並不能達到資料免除識別化的效果。最後，我們還是要透過審視有關原則或其執行方法，從而處理這些私隱風險。

Mikko Niva在分享處理私隱議題的經驗時，強調需要盡一切可能保障私隱。他笑說：「舉例來說，容易識別使用者的情況是有的，因為在芬蘭的細小服務區，可能只得一個人。但這是否意味我們不應把資料匿名化？當然不是。」

在討論接近尾聲時，**私隱專員蔣任宏**表示互聯網及先進科技的使用增加，對私隱保障帶來挑戰，而公署去年發表調查報告的「起你底」事件就是一例。他指出這個案在社會上引起不少討論。他總結，雖然法律永遠追不上具體情況，但我們的私隱法例以原則為本的取向仍是非常好。「再者，問責原則雖然不是香港資料保障法律的一部分，但它仍是有效的。」他說。「我們在處理私隱議題時，可以經常反問，有關資料的收集或使用是否公平。」

The event connected overseas experts in the data privacy field with local privacy academics and stakeholders on various privacy issues including Big Data and analytics, the de-identification of personal data, privacy risk management, and the Internet.

Professor John Bacon-Shone, Director of the Social Science Research Centre at the University of Hong Kong and a member of the PCPD's Standing Committee on Technological Developments, acted as moderator for the session.

Delegation member **Ms Christina Peters, Chief Privacy Officer of IBM**, pointed out that the law was having trouble keeping up with the rapid development of technology because new technological developments had created an unprecedented flow of data. She explained the challenge nowadays was to help organisations understand what their options were regarding the protection of personal data privacy and provide practical business solutions that allowed them to remain compliant with the law and respectful of the rights of their clients. "Our businesses cannot thrive unless people trust us," she said.

Mr Mikko Niva, Privacy Director of Finland's Nokia compared privacy protection to a war that needs to be fought on multiple fronts and suggested companies establish a comprehensive toolkit to comply with privacy principles. "The first tool is the law and related regulations. Then we focus on the accountability of the organisation. A meaningful framework helps organisations become accountable."

A new and important area to look at is the standardisation of technological safeguards, Mr Niva stressed. "If the underlying technology doesn't support data privacy protection, then our efforts will be wasted."

He said he anticipated a more diversified skill set among privacy professionals in the future. "Privacy protection professionals are no longer from just the legal field to provide guidance and answer questions. For example, we will see the emergence of privacy engineers, as we will need a huge amount of security design to prevent risks."

The delegation also reinforced the importance of putting the fairness principle into practice. **Ms JoAnn Stonier, Chief Privacy Officer at MasterCard**, said she believed that everyone in an organisation needed to have a certain level of savvy about personal data privacy and that an ethical code needed to be enforced throughout the organisation when dealing with the collection, analysis and application of data. She added that fairness was not limited to providing a notice to customers.

Professor Bacon-Shone echoed Ms Stonier, citing the Octopus incident as an example that showed the public in Hong Kong how unfairly personal data was being handled.

Mr Scott Taylor, Chief Privacy Officer at Hewlett-Packard, compared data protection in Big Data analysis to reducing air pollution, when he shared his views on how to create a healthy environment for data collection and protection. He said keeping the environment as healthy as possible required a mixture of regulations, responsible responses from companies, and participation by data subjects. "The air is not always perfect, but we are doing better than we did 30 years ago," he said.

The participants also discussed whether the current law was able to address the needs created by technological developments.

Professor Bacon-Shone pointed out that despite the weaknesses in the law in its current form, the principle-based privacy law was, in itself, sound. "We need to distinguish whether there is weakness in the principle, or there is a weakness in the implementation of the principle in a specific legal framework."

私隱專員與代表團、國際會議的講者及本地私隱保障專家合照。

Privacy Commissioner connects members of the delegation and speakers at the International Conference with local privacy experts.

He said the assumption that anonymisation was a solution for privacy protection was no longer valid. For example, in the case of sensitive data, he said we must distinguish between biometric data, like DNA, which cannot be changed, and other personal data, such as bank records. Anonymisation of one's DNA data does not serve the effect of de-identifying the data. "Yet ultimately, we have to frame and address these privacy risks – either by looking at the principles, or looking at the implementation (of the principles)," he said.

When sharing experiences in tackling privacy issues, Mr Niva stressed the need to do everything that can be done to protect data privacy. "For example, there are cases in which a user can be easily identified, as there may be only one person in a tiny service area in Finland," he grinned. "But does that mean we should not de-identify the data? Of course not."

As the discussion drew to close, **Privacy Commissioner, Mr Allan Chiang**, observed that the increased use of the Internet and advanced technologies posed challenges to privacy protection, and that the 'Do No Evil' case, which the PCPD released in an investigation report last year, was an illustrative example of this. He pointed out that the case had created a lot of discussion in the community. He concluded that although the law could never keep up with the specifics, the principle-based approach of our privacy law was still very good. "Further, the accountability principle, although not part of the Hong Kong data protection law, is still valid," he said. "We can always address a privacy issue by asking whether the collection or use of data in question is fair."

會議參與者
Participants of the Meeting

海外
Overseas

- Ms Bojana Bellamy, President, Centre for Information Policy Leadership, UK
- Mr Manuel Maisog, Partner, Hunton & Williams, UK
- Mr Mikko Niva, Director of Privacy, Nokia, Finland
- Ms Laura Juanes Micas, Director of International Privacy, Yahoo!, US
- Ms Christina Peters, Chief Privacy Officer, IBM, US
- Mr Luca Probst, Attorney, Asia Pacific Legal, UPS, US
- Ms JoAnn Stonier, Chief Information Governance & Privacy Officer, MasterCard, US
- Mr Huey Tan, APAC Privacy and Compliance, Accenture, UK
- Mr Scott Taylor, Vice President and Chief Privacy Officer, Hewlett-Packard, US

香港及澳門
Hong Kong and Macau

- 香港大學社會科學研究中心總監及公署科技發展常務委員會成員白景崇教授
  Prof John Bacon-Shone, Director, Social Sciences Research Centre, The University of Hong Kong, and Member of the Standing Committee on Technological Developments, the PCPD
- 公署資訊科技顧問張宗頤博士
  Dr Henry Chang, Information Technology Advisor, the PCPD
- 香港大學法律學院教授張善喻教授
  Prof Anne S Y Cheung, Professor, Faculty of Law, The University of Hong Kong
- 香港個人資料私隱專員蔣任宏先生
  Mr Allan Chiang, Privacy Commissioner for Personal Data, Hong Kong
- 香港大學計算機科學系副教授及公署科技發展常務委員會成員鄒錦沛博士
  Dr K P Chow, Associate Professor, Department of Computer Science, The University of Hong Kong, and Member of the Standing Committee on Technological Developments, the PCPD
- 香港中文大學法律學院助理教授Prof Stuart Hargreaves
  Prof Stuart Hargreaves, Assistant Professor, Faculty of Law, The Chinese University of Hong Kong
- 香港特別行政區政制及內地事務局首席助理秘書長梁何綺文女士
  Mrs Philomena Leung, Principal Assistant Secretary, Constitutional and Mainland Affairs Bureau, Hong Kong SAR Government
- 香港大學法律學院法律及資訊科技研究中心助理教授Dr Marcelo Thompson
  Dr Marcelo Thompson, Assistant Professor of Law, Deputy Director, Law and Technology Centre, Faculty of Law, The University of Hong Kong
- 孖士打律師行高級顧問黃錦山先生
  Mr Kenny Wong, Senior Consultant, Mayer Brown JSM
- 澳門特別行政區個人資料保護辦公室副主任楊崇蔚先生
  Mr Ken Yang, Deputy Coordinator of the Office for Personal Data Protection, Macau SAR Government

零售業保障個人資料私隱活動

Retail Industry Campaign for Protecting Consumers' Personal Information

「店鋪裝有感應器，可找到附近正開啟Wi-Fi功能以搜尋網絡的智能電話。店員憑手機的位置，從而追蹤機主的在店鋪裡的行動，考查他曾否光顧和買了哪些產品，這做法有問題嗎？」

「商戶可收集參加會員計劃人士的身份證號碼嗎？」

「零售商如何使用客戶的個人資料進行推廣活動？」

"A store has installed sensors that scan for smartphones with Wi-Fi turned on. The store uses the sensor to identify each phone's unique address, determining if the owners are repeat customers, and then tracking their movements around the store to record what they buy, etc. Is this lawful? "

"Are retailers permitted to collect identity card numbers from membership applicants?"

"Are there any restrictions on how retailers use their customers' personal data for promotional activities?"

零售商經常面對上述問題。本港目前約二十六萬人從事零售業，佔勞動人口一成。零售業前線人員在日常工作中經常接觸到客戶和員工的個人資料。有見及此，公署與香港零售管理協會自去年六月合作推展主題為「卓越零售，保障私隱」的行業保障私隱活動，目標是增進業界對《個人資料(私隱)條例》(「條例」)的認識，提倡良好行事方式。更成立了工作小組，分享零售商在營運上會涉及個人資料的業務範疇和業界關注的事項。參與是次工作小組的成員包括香港零售管理協會經理**樊麗儀女士**、利亞零售有限公司人才管理及發展高級經理**潘寶珍女士**、香港必勝客管理有限公司市務經理**廖婷英女士**及美心食品有限公司法律顧問**戴敬慈女士**。

零售商在許多情況下均會收集及處理個人資料(例如會員計劃、推廣活動等)，工作小組因而建議從這些實際運作為基礎，編制了「零售業保障私隱面面觀」講座。並為切合不同工作性質的需要，制定了一系列的培訓課程(見第18頁表)，務求提昇從業員對個人資料私隱保障的意識。

公署正著手製作一套網上評估工具，就零售業前線人員涉及處理個人資料的常見場景(即以下例子)，解釋條例的規定，並提供實用貼士，以助從業員在遵從條例要求的前提下，有效地完成相關工作。

All of the above are scenarios encountered by retailers every day. Currently, about 260,000 people in Hong Kong are engaged in retailing, making up 10% of the working population. Frontline workers are frequently required to handle the personal data of their customers and co-workers while carrying out their daily duties. In view of this, the PCPD collaborated with the Hong Kong Retail Management Association (HKRMA) last June to launch an industry-specific campaign called "Driving Retail Excellence through Privacy Assurance". The purpose of the event was to promote understanding of data-protection requirements under the Personal Data (Privacy) Ordinance and share good privacy practices among members of the industry. Also, a working group was set up for retailers to discuss compliance issues in various business environments and other concerns. Members of the working group included **Ms Veronica Fan**, Manager of the HKRMA; **Ms Carol Poon**, Senior Manager-Talent Management & Development of the HRA Division of Convenience Retail Asia Ltd.; **Ms Liane Liu**, Marketing Manager of Pizza Hut Hong Kong Management Ltd; and **Ms Rachel Dai**, Legal Counsel of Maxim's Caterers Ltd.

Since retailers in their business operations collect and handle personal data for various purposes (e.g. membership applications and promotional activities), the working group suggested focusing on these data practices. The collaborative effort has resulted in the formulation of a "Retail Operation Seminar". The working group has also planned a series of training programmes (see Table on page 18) to enhance compliance among the retail workers with different job types.

Aiming to help frontline staff in the retailing sector to do their job efficiently without violating the Ordinance, the PCPD is now developing an online assessment tool to explain the stipulations set out in the Ordinance, together with some useful tips, using the following common scenarios involving personal data processing by retailers.

公署為零售服務業界舉行不同課題的講座，令從事不同範疇工作的零售業從業員了解條例的規定。

The PCPD has organised a series of training programmes to enhance compliance among the retail workers with different job types.

場景 Scenario 1 積分獎賞／會員計劃 Reward Points for Purchases

零售商推出積分獎賞計劃，會員需提供身份證號碼及出生日期登記。會員每次購物可賺取積分，用積分換取現金券。會員亦享有購物折扣和推廣優惠。若會員報失會員咭，店員會要求會員出示身份證以核實會員的身份，才安排換領新會員咭及保留已賺取的積分。

A retail group has devised a customer-loyalty programme which requires the collection of ID card numbers and dates of birth of its members. Members can earn reward points for each purchase, and the reward points can be used to redeem cash coupons. Members are also entitled to take advantage of discount and promotional offers. If members lose their membership cards, they need to present their ID cards to obtain new cards and retain the reward points earned.

保障私隱錦囊

- 提供一般的消費優惠或獎賞，用顧客的姓名及電話號碼已足以核實身份，毋須收集身份證號碼或副本等私隱度高的資料。
- 在申請表格上提供「收集個人資料聲明」，述明收集資料的目的、資料用途、資料可能轉移給甚麼類別的人，及要求查閱及改正個人資料的方法等。
- 如要收集與參加積分獎賞／會員計劃無直接關係的資料（例如職業、喜好），以作市場分析，應讓客人自行選擇是否願意提供。
- 考慮侵犯私隱度較低的方法。舉例說，憑出生月份已足以提供生日優惠，不必要求顧客填報出生年月日；用年齡組別選項代替填寫具體歲數，避免收集「超乎適度」的個人資料而違反規定。
- 如為會員提供網上服務，應採取足夠的保安措施，以防資料外洩。勿用電話號碼或身份證號碼作為會員號碼或網上帳戶的密碼，減低被盜用的機會。

Tips for data privacy

- Name and telephone number are adequate for the purpose of identity authentication in the case of general offers and rewards. There is no need to collect highly private data such as ID card numbers or hard copies of ID cards.
- Provide a Personal Information Collection Statement ("PICS"), which states the purpose of collection, the intended use of the data, the types of parties the data will be transferred to, and how to make a request for data access or data correction.
- If any data not directly related to the reward programmes/membership programmes (for example, occupations or preferences) is to be collected for market research purposes, the members should be given the choice of whether or not to provide the data.
- Consider less privacy-intrusive alternatives. For example, collect only the month of birth for birthday offers; use age ranges instead of asking for the exact age. These alternatives would help avoid collecting excessive personal data.
- If online services are provided for members, take measures to ensure the security of their data. To reduce the risk of identity theft, never use the phone numbers or ID card numbers of members as default membership numbers or passwords for online user accounts.

場景 Scenario 2 抽獎活動 Lucky Draws

零售公司舉辦抽獎遊戲，要求參加者提供姓名、地址、電話號碼和身份證號碼登記。獎品價值達數萬元。

A retail company is holding a lucky draw. Participants are required to provide their names, addresses, telephone numbers and ID card numbers for registration. The prize is worth tens of thousands of dollars.

保障私隱錦囊

- 可考慮在抽獎券上印上序號，以防複製或偽造。領獎時，可要求得獎者出示身份證以核對其姓名和容貌。
- 除非關乎公司「超過輕微程度的損失」，否則不必收集顧客的身份證號碼作身份核實之用。
- 活動完結後，應將不再需要的資料銷毀，以免違規。

Tips for data privacy

- Consider printing the numbers on the draw ticket to prevent duplications or fakes. Check the name and photo on the ID card produced by the person who claims to be the winner.
- If the potential loss for the company is trivial, it is not necessary for the company to collect the ID card number of participants for identity-authentication purposes.
- Destroy all data which is no longer necessary after the event.

場景 Scenario 3 禮品換領 Gift Redemptions

商店向會員發出換領券，憑券到店舖領取禮品時，店員要求會員提供身份證號碼以核實其會員身份。

A store issues vouchers, which members can redeem for gifts. Upon redemption, members are requested to produce their ID card numbers for membership authentication.

保障私隱錦囊

- 可要求顧客出示有相片的身份證明文件以核實其身份，例如會員證、學生證或職員證。
- 足夠確認換領者身份便可，不應收集身份證號碼或副本。
- 如顧客授權他人代領，可要求代領者出示授權書及有關身份證明文件。

Tips for data privacy

- Ask the members to present identification documents with photos, such as membership cards, student cards or staff cards for identity authentication.
- Only collect the data necessary for identification. There is no reason to collect ID card numbers or hard copies of ID cards.
- If the members authorise someone else to redeem the gift for them, you can request the latter to produce an authorisation and identification document.

場景 Scenario 4 發放產品或服務推廣資訊 Sending Promotional Materials for Products or Services

電器店向會員寄出其姊妹公司的美容產品推廣資訊。

An electronics retailer sends promotional materials for beauty products from an associated company to its members.

保障私隱錦囊

- 利用顧客的聯絡資料進行直銷活動前－
  - > 須告知顧客你的機構擬使用他們的何種個人資料，以推廣機構的哪類產品或服務。
  - > 須先得到顧客的同意，才可向他們發送上述的廣告或宣傳資訊。
  - > 不回覆不代表同意。
- 如顧客以書面或口頭方式表示不欲再接受推廣資訊，須馬上停用他們的資料作直銷，以尊重他們的私隱。
- 確保使用中的「拒收直銷資訊名單」是最新版本，在寄發直銷資訊時剔除名單上的人士。

Tips for data privacy

- Before using the personal data of customers for direct marketing:
  - > the company must notify its customers of its intention and what kind of personal data it intends to use, as well as the classes of products and services it intends to promote;
  - > the company must obtain consent from its customers to use their personal data; and
  - > if their customers do not reply to their request for consent, the company must assume they do not agree to the use of their personal data for direct marketing.
- If their customers, either orally or in writing, ask the company to stop using their personal data, the company must stop using their personal data.
- The company should maintain a regularly updated opt-out list and make sure no one in the company uses the personal data of members who have indicated that they do not wish to receive further marketing materials.

場景 Scenario 5 使用閉路電視 Use of CCTV

某時裝店在商舖內安裝隱蔽式攝錄機，藉以監察可能出現的盜竊情況。

A boutique has installed a covert recording device to monitor the store for possible theft.

保障私隱錦囊

- 除非別無他選和有充分理由，否則不應安裝隱蔽式的攝錄機。
- 如用作防盜用途，應採用非隱閉式的閉路電視。
- 閉路電視監察範圍內及入口應有明顯告示，提醒顧客／員工會受到監察，及告知監察的目的等。
- 顧客和員工期望有較高私隱高的地方（例如休息室及更衣室），不應設置閉路電視監察。

續 continued 》》

Tips for data privacy

- Unless there is a strong justification, the company cannot install covert recording devices in its shop.
- Overt means such as CCTV may be used for purposes such as theft prevention.
- A prominent notice should be placed at the shop entrance and in the surveillance area to remind customers and staff that they are subject to surveillance, and inform them of the purpose of the monitoring.
- No CCTV surveillance can be installed in places where customers and staff expect a relatively high degree of privacy, such as in restrooms or changing rooms.

場景 Scenario 6 招聘及僱傭活動 Recruitment and Human Resources Activities

商店經理在招募售貨員的第一輪面試中，要求影印求職者的身份證，以作紀錄和辨識求職者身份。

A shop manager collects a copy of the ID card of a job applicant in the first round of interviews for the post of retail clerk for the purpose of recording and checking the identity of the candidate.

保障私隱錦囊

- 除非求職者已受聘，否則僱主不可過早收集求職人士的身份證副本。一般而言，僱主可收集僱員的身份證副本，作為已遵從《入境條例》（第115章）第17J的證明。
- 只向求職者收集足以遴選用的個人資料。
- 落選者的個人資料，保存時間不應超過兩年。
- 現職員工的個人資料，只可用於僱傭目的。

Tips for data privacy

- Employers should not collect ID card copies of job applicants during the recruitment process unless and until the candidate has accepted an offer of employment. Generally speaking, an employer may collect the ID card copy of an employee as proof of compliance by the employer with section 17J of the Immigration Ordinance (Cap 115).
- Employers should collect only the personal data which is necessary for recruitment selection.
- Employers should not keep longer than two years the personal data of candidates not employed.
- Employers should use the personal data of current employees only for employment purposes.

場景 Scenario 7 手機應用程式 Mobile Apps

某食肆推出外賣的智能電話應用程式，消費者用手機點選食品，然後輸入地址發送訂單，便可享用送遞上門的食品。

A restaurant has launched a food delivery mobile app, which allows customers to choose the food from a menu, key in their address, and have the food delivered.

保障私隱錦囊

- 在用戶安裝程式前提供清楚的個人資料收集聲明。
- 程式的讀取資料權限聲明，不能代替個人資料收集聲明或私隱政策聲明。
- 收集的資料只限用於處理外賣訂單，而不應用作其他目的。做好保安措施，防止訂單的個人資料外洩。
- 就目的而言不再需要的顧客資料，便應刪除。
- 如要用已收集的顧客資料發放宣傳推廣資訊，應事先取得顧客同意，和限於用作推銷顧客已同意的產品和服務類別。

Tips for data privacy

- The restaurant must clearly display its PICS to its customers before they install the app.
- The restaurant cannot substitute the declaration for data accessing rights of the app for its PICS or Privacy Policy Statement.
- The restaurant cannot use the data collected for any purpose other than processing orders for delivery, and it should have proper safety precautions in place to prevent data leakage.
- The restaurant should delete customers' details that are no longer necessary for the prescribed purposes.
- The restaurant must obtain its customers' consent before using the collected data in promotional activities, and ensure the products or services promoted are only those agreed to by its customers.

場景 Scenario 8 社交網絡市場推廣 Social Network Marketing

食品公司在社交網站上推出有獎遊戲活動，分享相片，有機會贏得獎品。社交網站用戶須「讚好」該遊戲專頁才可參加，並且要同意專頁內含的程式閱取其張貼在社交網絡的公開帖子。

A food company has launched a prize-winning game on a social networking site, whereby participants can win a prize by sharing their personal photos. The social network users must "like" the fan page of the food company to join the game. Participants are then required to allow the company to access their posts.

保障私隱錦囊

- 招募會員、攝影比賽、抽獎、投票等活動涉及明確地收集及使用個人資料，於收集資料前須提供相應的收集個人資料聲明。
- 在社交網絡上監察任何人的帖子內容和活動，可構成收集和使用個人資料，你需要告知當事人你如此使用他們在社交網絡上的個人資料。
- 利用程式查閱某人帳戶的個人資料前，應先徵求用戶的允許。
- 如在社交網絡上利用用戶的「讚好」，或追蹤個人的網上行蹤，以作產品和活動推廣用途，應通知當事人及給予他拒絕參與的選擇。
- 機構委託公司進行網上推廣活動，應採用合約規範或其他方式要求承辦商採取切實可行的措施，確保個人資料的收集、處理和轉移遵從條例規定。

Tips for data privacy

- When the company collects personal data through member recruitment, competitions, lucky draws or voting, it must provide a PICS to its customers.
- If the company intends to monitor participants' social network activities, it must inform the participants.
- The company must obtain the consent of the participants before accessing their social network accounts to view their personal data.
- When making use of "likes" on social networks or conducting on-line tracking to promote products or services, companies should inform the people concerned and give them the choice to opt-out.
- If a company engages an agent to conduct online promotional activities, the company is required to adopt contractual or other means to ensure the agent complies with the Ordinance in relation to the collection and processing of personal data.

表：零售服務業保障私隱活動培訓系列
Table: Training Programmes under Privacy Campaign for Retail Industry

日期 Date	活動 Activities
2013.06.25	開展儀式暨研討會 Inaugural ceremony cum Seminar
講座 Seminar	
2013.10.03	直接促銷新規管簡介 New Direct Marketing Regime
2013.12.17	《個人資料(私隱)條例》簡介 Introductory to the Personal Data (Privacy) Ordinance
2014.01.28	如何擬備「收集個人資料聲明」及私隱政策 How to prepare Personal Information Collection Statement and Privacy Policy Statement
2014.02.19	善用資訊及通訊科技 Use Information and Communications Technology Smartly
2014.02.26 2014.04.28 2014.05.29 2014.06.23	「零售業保障私隱面觀」 Retail Operation
2014.03-06	個人資料(私隱)條例簡介(會員公司包班) In-house seminar on Personal Data (Privacy) Ordinance
2014.06	個人資料(私隱)條例簡介(中小企零售商) Introduction to Personal Data (Privacy) Ordinance for SME Retailers
專業研習班 Professional Workshop	
2013.10.29	人力資源管理的資料保障 Data Protection in Human Resource Management
2013.11.22	直接促銷活動的資料保障 Data Protection in Direct Marketing Activities
2014.03.31	資料保障法律研習班 Legal Workshop on Data Protection

詳情 Details：www.pcpd.org.hk/retail

以電郵寄出課程資訊，是否受條例的直接促銷規管機制管限?

Does Sending Course Information via Email Fall under the Direct Marketing Regulatory Regime under the Ordinance?

一間教育機構查詢，透過電郵網絡向其學生及職員發出課程資料，是否構成條例所指的「直接促銷」。如果是的話，可否視之為「一般的通訊」而免受條例第VIA部的直接促銷規管機制所規管。

公署回覆

條例把直接促銷定義為，用「直接促銷方法」提供或宣傳推廣貨品、設施或服務，而「直接促銷方法」包括以電子郵件方式向特定的具名人士寄出資訊或貨品。

若該教育機構寄出的電郵涉及該機構提供的新課程，便屬於直接促銷活動，該機構須遵從條例中有關規管為直接促銷用途而使用個人資料和提供該資料予他人作直銷用途的規定。

機構須在使用學生和職員的個人資料進行促銷前，先取得他們的同意。在首次使用他們的個人資料作直接促銷時，須告知當事人機構會應要求停止把有關個人資料用於直接促銷，而且不收費用。如機構的學生／職員提出拒絕直接促銷的要求，機構必須依從。

條例並沒有就資料當事人和資料使用者之間的「一般通訊」提供豁免。惟有關告知當事人擬使用其個人資料的目的和取得當事人同意的規定，不適用於一些在條文生效前（即2013年4月1日）已由該資料使用者控制，並符合以下條件的個人資料。

- 資料當事人已獲資料使用者以易於理解及閱讀（如以書面方式告知）的方式明確告知，其個人資料被用作或將會被用作促銷某類別的產品／服務；
- 資料使用者曾經使用當事人的個人資料進行上述的促銷活動；
- 當事人不曾要求資料使用者停止使用其任何個人資料；及
- 資料使用者使用該等個人資料時，沒有違反當時的條例規定。

了解更多：請參閱《直接促銷新指引》
www.pcpd.org.hk/chinese/files/publications/GN_DM_c.pdf

An educational institution enquired about whether sending course information to its students and staff members by email would constitute "direct marketing" under the Ordinance, and if so, whether it could be regarded as "general communications", thereby being exempted from the requirements under the direct marketing regime (Part VIA) of the Ordinance.

PCPD Reply

Direct marketing, as defined in the Ordinance, includes offering or advertising the availability of goods, facilities or services through direct means, including sending information or goods addressed to individual by name through email.

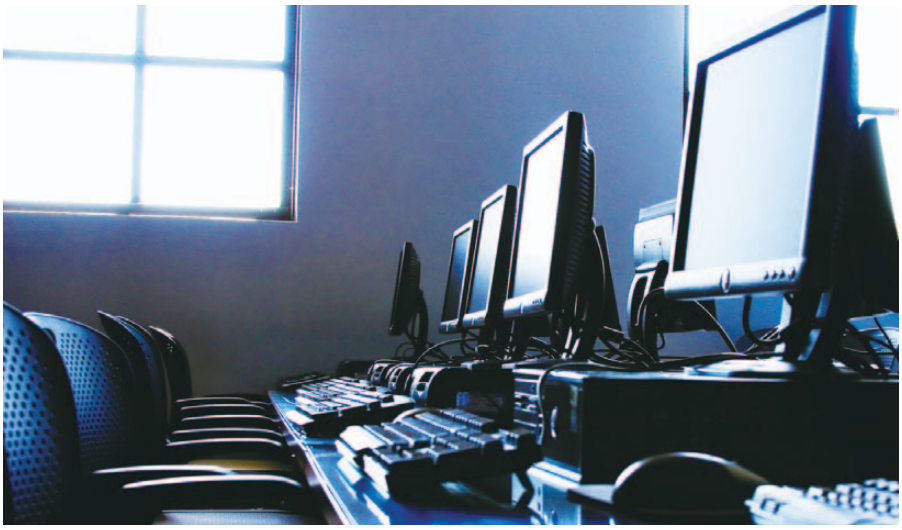
If the email content offers new courses organised by the institution, it would constitute direct marketing and the institution would need to observe the requirements which regulate the use of personal data for its use in direct marketing and the transfer of such data to third parties for their use in direct marketing.

The institution should obtain the consent of its students and staff members before using their personal data in direct marketing. When using their personal data in direct marketing for the first time, the institution needs to inform them that it will, without charge, cease to use their data in direct marketing if they do no wish to receive it. The institution should comply with any opt-out requests made by its students and staff members.

The Ordinance does not contain any exemption in relation to "general communications" between a data user and a data subject. However, the requirements for notification of use and consent do not apply for personal data used by the data user before the effective date of these new legal requirements (i.e. 1 April 2013) if–

- the data subject had been explicitly informed by the data user, in a manner which was understandable and readable (if in writing), of the intended use of the data subject's personal data in direct marketing in relation to the class of products or services;
- the data user had used the data of the data subject for the above mentioned activities;
- the data subject had not required the data user to stop using any of the data; and
- the data user had not, in relation to such use, contravened any provision of the Ordinance in force at the time of such use.

Learn more: Read New Guidance on Direct Marketing (www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf).



加緊規管個人資料的跨境轉移
Push for Regulation on the Transfer of Personal Data Outside Hong Kong

私隱條例第33條對轉移個人資料至香港以外地區的安排具非常嚴謹和全面的規管。該條文明確禁止持有資料的資料使用者把個人資料轉移至香港以外的地區，除非符合指定的條件，例如：

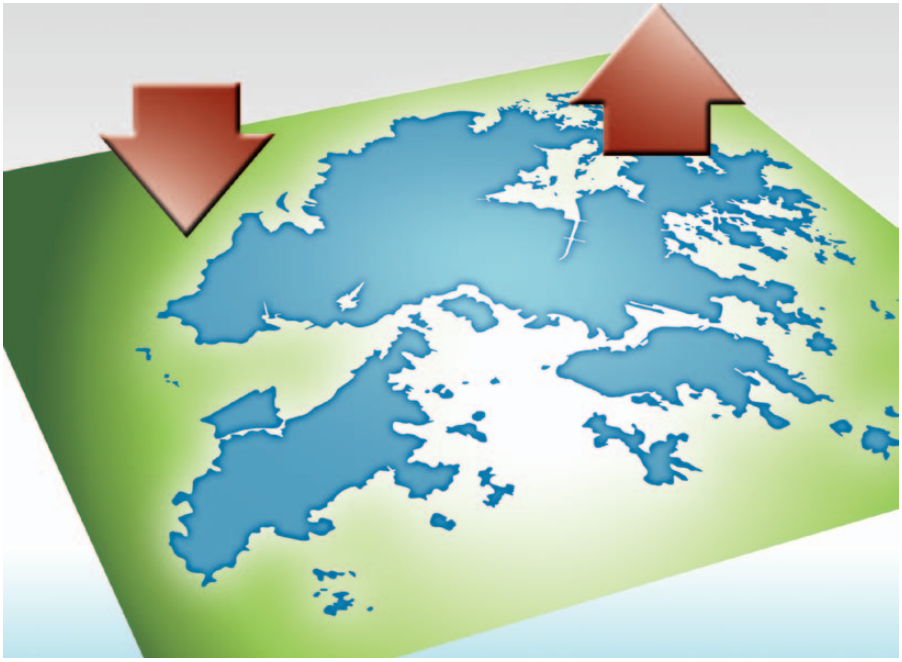
(1) 該地區是在專員制訂的「白名單」內，即這些地區實施的有關個人資料保障的法律，與本港私隱條例大體上相似，或其目的與私隱條例的目的相同[第33(2)(a)條]；及

(2) 資料使用者已採取所有合理的預防措施及已作出所有應作出的努力，以確保資料轉移該地區後被處理的方式不違反私隱條例規定[第33(2)(f)條]。

但是，私隱條例自1995年實施以來，第33條遲遲未生效，而政府當局亦未有訂立落實該條文的時間表。換言之，現時香港有關個人資料由香港轉移海外的保護相當薄弱，有欠全面。

私隱專員蔣任宏指出：「私隱條例於九十年代制定，時至今天，全球數據流動的模式已大大不同。科技進步，加上機構的業務模式和行事方式演變，個人資料的轉移已變成個人資料的數據流。數據跨境，連綿不絕和大規模地流動。政府是時候正視私隱條例第33條相關的議題，確保香港維持國際金融中心和數據樞紐的地位。」

為此，公署在2013年對香港以外50個司法管轄區的個人資料保障法例進行研究，結果擬備了一份『白名單』，臚列出正實施大體上近似本港私隱條例或達致相同目的之法律的地方。研究報告和『白名單』已交給政府考慮。



Section 33 of the Ordinance provides a very stringent and comprehensive regulation of the transfer of data outside Hong Kong. It expressly prohibits all transfers of personal data 'to a place outside Hong Kong' except in specified circumstances such as:–

(1) the place is specified by the Commissioner as one which has in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance [section 33(2)(a)]; and

(2) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be handled in a manner tantamount to a contravention of a requirement under the Ordinance [section 33(2)(f)].

The only problem is that section 33 has not been brought into force since its enactment in 1995 and the Government has no timetable for its implementation in future. As a result, the current protection for personal data transferred overseas is weak and far from comprehensive.

Privacy Commissioner Mr Allan Chiang commented, "Advances in technology, along with changes in organisation's business models and practices have turned personal data transfers into personal data flows. Data is moving across borders, continuously and in greater scales. It is high time for the Government to have a renewed focus on section 33 of the Ordinance to ensure that the international status of Hong Kong as a financial centre and a data hub will be preserved."

To assist the Government in this area, the PCPD completed in 2013 a survey of 50 jurisdictions and come up with a white list of places which has in force a data protection law substantially similar to, or serves the same purpose as the Ordinance. A copy of the report has been forwarded to the Government.

行政上訴委員會確立雜誌偷拍藝人案屬不公平收集個人資料

AAB Affirms the Decision on the Clandestine Photo-taking of Artistes Cases

行政上訴委員會駁回《忽然一週》和《FACE》週刊就偷拍藝人案提出的上訴，確立兩雜誌偷拍藝人的行為是以不公平手法收集個人資料，並違反條例的保障資料原則第1(2)條的規定。行政上訴委員會裁定公署的決定是正確的，維持私隱專員發出執行通知的決定，並作出以下的重要裁定：—

公眾利益是衡量新聞機構採用有系統的監察，和望遠鏡鏡頭來偷拍相片是否公平。而該兩宗個案並不涉及公眾利益的情況。

裁決亦確立了專員向兩間雜誌發出的執行通知，指令它們制訂就有系統的隱蔽監察及／或遠距離攝影拍攝照片的方式收集個人資料的私隱指引；以及為員工提供相關培訓，確保他們遵從條例的規定。

兩家雜誌社的律師知會公署，已經將涉事的相片，永久從雜誌社的資料庫和網站移除。兩雜誌社於三月向高等法院提出司法覆核許可的申請。

了解更多：

行政上訴委員會的裁決

www.pcpd.org.hk/english/files/casenotes/AAB_5_2012.pdf
www.pcpd.org.hk/english/files/casenotes/AAB_6_2012.pdf

Administrative Appeal Board ("AAB") has dismissed the appeals from Sudden Weekly and Face Magazine against the Privacy Commissioner's decision in two cases relating to the clandestine photo-taking of artistes, and confirmed the Privacy Commissioner's decision that the two magazines' had collected their personal data by unfair means and amounted to contravention of Data Protection Principle ("DPP")1(2).

In its decision made on 6 January 2014, the AAB ruled that public interest is one of the factors to consider as to whether or not the taking of clandestine photographs by news organisations using systematic surveillance and telescopic lens is fair. The two cases did not involve public interest.

The AAB also confirmed the enforcement notice directing the two magazines to take measures to remedy the contravention, including in these cases, to draw up privacy guidelines on the collection of personal data by systematic covert surveillance and/or long distance photograph shooting, and to provide relevant training to their staff.

The solicitors of the magazines informed the Commissioner that the photographs had already been permanently deleted from the magazines' database and websites.

The two magazines applied to the High Court for leave to judicial review in regard to the AAB's and PCPD's decisions in March.

Learn more:

Decisions of the AAB

www.pcpd.org.hk/english/files/casenotes/AAB_5_2012.pdf
www.pcpd.org.hk/english/files/casenotes/AAB_6_2012.pdf

California Fitness違規向會籍申請人收集過度的個人資料

California Fitness Collected Excessive Personal Data from Membership Applicants

公署認為California Fitness收集超乎適度的個人資料，包括香港身份證副本，違反了條例的規定。
California Fitness was found in breach of the Ordinance by collecting excessive personal data, including copies of Hong Kong Identity Card.

連鎖健身中心California Fitness（簡稱「CF」）向申請入會或續會的人士收集超乎適度的個人資料，包括香港身份證副本，侵犯顧客的個人資料私隱。

私隱專員於2013年12月公佈調查結果前發出執行通知，指令CF糾正和防止違規情況發生，而CF已向行政上訴提出上訴，反對該執行通知。該公司堅稱需要收集會員的身份證副本以配合職員的銷售獎賞制度，作為防止銷售員遞交虛假會籍申請。

調查源於兩名市民投訴CF在處理其會籍申請及續會申請時收集其完整出生日期（包括年月日）、身份證號碼及身份證副本（或以回鄉證副本替代）。

私隱專員蔣任宏批評CF並沒有從八達通事件汲取教訓，重犯錯誤收集超乎適度的身份證明資料以核實客戶身份。

「機構在收集個人資料方面傾向寧濫莫缺，未有認真考慮收集得的個人資料，可達致的實際目的為何。再者，機構流於偏重行政及運作的方便，而犧牲了資料當事人的私隱及資料保障。在核證方面，機構不理會交易的性質而追求最嚴密的核證程序，過份依賴用身份證號碼及身份證副本去核證個人身份的做法普遍，實在有必要糾正過來。」

他提醒機構在身份核實程序的設計和執行上應尊重私隱，核實的嚴密程度（如為核實而收集多少個人資料），應與交易的性質和價值相稱，並應考慮相關的個人資料的敏感度。

網上閱覽調查報告全文：
www.pcpd.org.hk/chinese/publications/files/R13_12828_c.pdf

California Fitness, a fitness centre chain, has breached data protection principle under the Ordinance by collecting excessive personal data, including copies of Hong Kong Identity Card ("HKID Card"), from its customers who applied for or renewed memberships.

California Fitness lodged an appeal to the Administrative Appeals Board against the enforcement notice served by the Privacy Commissioner following the release of the investigation report in December 2013. The company held that HKID Card copies had to be collected to support its staff remuneration system for reward of achievement of sales targets. These documents served to data submission of bogus membership applications by the sales staff.

The investigation stemmed from two complaints by its members against California Fitness's collection of their full dates of birth; HKID Card numbers; and copies of HKID Card or alternatively, Home Visit Permit.

Privacy Commissioner, Mr Allan Chiang criticised California Fitness for not having learnt from the infamous Octopus incident and repeating the mistake of excessive collection of customers' personally identifiable information for authentication purposes.

"Corporate data users tend to collect personal data without giving serious thought to what real purposes the data collected could serve. Further, they tend to over-emphasise their administrative and operational convenience, at the expense of data subjects' privacy and data protection, and adopt the strongest level of identity authentication regardless of the nature of the transaction. The over-reliance of production of HKID Card number and HKID Card copy for identity authentication amounts to overkill and the trend must be reversed."

He advised organisations should respect privacy and ensure data protection at every stage of the process of design and operation of an authentication process. The level of authentication (such as the amount of personal data collected for that authentication process) should be in proportion to the nature and value of the transaction, and take into account the sensitivity of the personal data involved.

Read the Investigation Report online:
www.pcpd.org.hk/english/publications/files/R13_12828_e.pdf

警務處接連遺失載有敏感個人資料的記事冊

The Police Force Warned after Repeated Incidents of Loss of Notebooks containing Sensitive Personal Data

公署的調查指出，香港警務處在兩宗分別遺失警察記事冊和「定額罰款單」的資料外洩事故中，未有妥善保護文件中的個人資料和避免資料意外遺失，違反條例的資料保安規定（保障資料第4原則），逐發出執行通知，指令警務處訂立額外的保安程序堵塞漏洞，以及加強監督有關文件的處理過程。

是次調查的範圍是11宗警務人員遺失記事冊和定額罰單的事故，共涉及 285名罪案受害人、證人及疑犯等的個人資料。

私隱專員認為，不論是否涉及違規，這些事故中的警務人員都有疏忽大意。儘管人為錯誤不可杜絕，但考慮到涉案的個人資料性質非常敏感，以及這類事故接連發生，他建議警務處全面檢討盛載或運送警方文件用的器材及制服，以防止個人資料受未經准許的查閱或意外的遺失；並應加強培訓並設獎勵和紀律制度，以督促警務人員遵從保障私隱及個人資料的政策及程序。

他指出：「即使是完備的私隱政策和嚴格的保安措施，都有可能被個別員工的鹵莽或粗心大意拖跨。機構應為員工提供全面的內部培訓，提高保障私隱的意識。推動整個機構建立一個尊重私隱文化是至為重要。」

調查報告：www.pcpd.org.hk/chinese/publications/files/R13_0407_c.pdf

The Hong Kong Police Force ("HKPF") was found to have breached the requirement of the Ordinance relating to protection of personal data against accidental loss (Data Protection Principle 4) in two incidents which involved the loss of police notebooks and a copy of fixed penalty tickets ("FPT"). The PCPD has served an enforcement notice on the HKPF, directing it to establish supplementary security procedures to plug the loopholes identified, and tighten up its supervision.

The investigation covered 11 incidents involving the loss of notebooks and copies of FPTs by different police officers, involving the personal data of 285 persons including crime victims, witnesses and suspects.

Most of the incidents involved negligence or carelessness on the part of the police officers concerned. Mr Allan Chiang, Privacy Commissioner agreed that human error could not be totally ruled out, but taking into account the sensitive nature of the data involved and the frequency of the incidents, he advised the HKPF should take the matter seriously and review HKPF's equipment and uniform used for carrying and transporting police documents in order to prevent personal data from unauthorised access or accidental loss. He also urged the HKPF to step up its training, incentive and disciplinary programmes to promote compliance with its privacy policies and procedures.

"Recklessness or carelessness of a single employee can undermine sound privacy policies and robust security practices. It is of utter importance that organisations institute comprehensive internal training and awareness programmes for their staff.

"The HKPF should commit to building a culture respecting privacy and data security," he said.

Investigation Report： www.pcpd.org.hk/english/publications/files/R13_0407_e.pdf

資料經Foxy外洩後患無窮

Use of Foxy Culminated in Data Leakage which Got Out of Control

公署跟進傳媒報道，調查警務處兩宗涉嫌經Foxy共享軟件洩漏個人資料的事故，調查結果確定事件屬於人為錯失，警務處未有違反條例規定。

但鑑於外洩文件載有重要和敏感的個人資料，私隱專員敦請警務處採取預防措施，避免同類事件再次發生。例如：(i) 加強宣傳，鼓勵警務人員使用部門提供的「個人電腦清洗」程式。(ii) 設立諮詢熱線，為有需要的人員以不記名方式提供支援。(iii) 促進警務人員之間的個案分享及經驗交流，以增進對保障個人資料的認知和明白網上資訊外洩的嚴重後果等。

私隱專員提醒公眾人士：「檔案一旦經過Foxy 網絡外洩，基本上無法把資料挽回。雖然Foxy 的開發商經已結業，但全球至少有40萬人的電腦仍啟動著Foxy軟件，用家需了解其Foxy版本如何運作，並加以適當的設定，以保護資料檔案。」他忠告市民，下載這軟件，是非常危險的事，因為在非官方渠道下載的版本有機會是惡意程式或遭加工，可能招致無法控制的資料外洩事故。

調查報告：www.pcpd.org.hk/chinese/publications/files/R13_15218_c.pdf

The PCPD has probed into two incidents of alleged leakage of internal documents by the Hong Kong Police Force ("HKPF") via Foxy after they were reported in the press. The investigation concluded that the two incidents were attributed to human error, and found no contravention on the part of the HKPF.

Considering the importance and sensitivity of the personal data contained in the police documents, Privacy Commissioner has urged the HKPF to take preventative measures to (i) promote the use of the HKPF's personal computer cleaning programme for checking and deleting personal data/confidential data on personal computers, (ii) set up an enquiry hotline to support police officers on an anonymous basis, and (iii) promote case and experience sharing among police officers to enhance the awareness of personal data protection and the serious consequences that may result from data leakages on the Internet.

Privacy Commissioner has warned the public that there is practically no effective recovery means once a data file is 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.

Investigation Report： www.pcpd.org.hk/english/publications/files/R13_15218_e.pdf

學生資助辦事處個人資料系統視察報告

Inspection Report of the Personal Data System of Student Financial Assistance Schemes

公署視察過學生資助辦事處用作處理四項中小學生資助計劃的個人資料系統，包括學校書簿津貼計劃、學生車船津貼計劃、上網費津貼計劃和考試費減免計劃。結果顯示該系統的資料保障措施大致令人滿意，惟某些方面，例如沒有明文指引規範職員向電話查詢者披露有關申請的個人資料，仍需檢討和改善。

視察報告：www.pcpd.org.hk/chinese/publications/files/R14_3771_c.pdf

The PCPD has conducted an inspection on the Student Financial Assistance Agency's personal data system in respect of four of its financial assistance schemes for primary and secondary students. The schemes include the School Textbook Assistance Scheme, Student Travel Subsidy Scheme, Subsidy Scheme for Internet Access Charges and Examination Fee Remission Scheme. The inspection concluded that the data protection measures in the personal data system inspected were reasonably satisfactory. However, certain areas such as the lack of written guidelines as to which information in application records may or may not be disclosed to callers require review and improvement.

Inspection Report: www.pcpd.org.hk/english/publications/files/R14_3771_e.pdf

不妥善地棄置載有病人紀錄的醫院廢料

Data Breach: Improper Disposal of Hospital Wastes Containing Patient Records

公署指醫院管理局(「醫管局」)處理載有病人紀錄的醫院廢料失當，違反保障資料第4原則(資料保安)，逐指令醫管局採取糾正措施，並加強保障病人的個人資料私隱 。

傳媒於2012年6月和9月分別報道有市民在密件處理服務有限公司(下稱「密件處理公司」)的粉嶺碎紙廠外，發現博愛醫院的一卷用過的打印用碳帶，及聖母醫院一批病人預約回條紙碎遭棄置街頭。該批廢料載有病人的姓名、性別、年齡／出生日期及身份證號碼等個人資料。

密件處理公司由2009年起承辦醫管局的廢料處理服務。

私隱專員在條例之下無權直接規管分判的資料處理者(承辦商)的行為，而只能靠資料使用者用合約或其他規範方式，促使承辦商遵從條例相關規定。公署在是次主動調查中發現兩大問題：

1. 合約在碳帶處理上存有疏漏，沒有列明需要點算裝有碳帶的回收袋，以防在運送過程中遺失；亦沒有訂明碳帶應切碎的程度以保證當中的個人資料不能被識別或還原。

2. 醫管局及其轄下的醫院沒有執行合約條款有效地監察密件處理公司的碎紙過程。醫管局總部否認他們有責任統籌監督轄下醫院的視察工序；醫管局亦從未檢視各醫院的視察報告，或透過審計途徑更全面和深入檢核醫院廢料處理的工序。

私隱專員已發出執行通知，指令醫管局(1)取回在事故中的棄置醫院廢料，並予以銷毀；(2)檢討和修訂醫院廢料棄置程序。

蔣任宏強調：「這事故帶出一個訊息：經常保障個人資料的重要。即使機構持有的個人資料在機構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，處理病人資料的表現極不理想。而醫管局在合約和程序方面對密件處理公司的監督不力，實地監察的表現亦強差人意。」

閱覽調查報告：www.pcpd.org.hk/english/publications/files/R13_6740_e.pdf

The Hospital Authority ("HA") has been served an enforcement notice following a breach of the Data Protection Principle 4 (data security) for improper disposal of hospital wastes containing the personal data of patients.

It was reported in the press in June and September 2012 respectively that a roll of used printer ribbon from Pok Oi Hospital and shredded strips of medical appointment slips from Our Lady of Maryknoll Hospital were found abandoned on the street outside a shredding factory of Confidential Materials Destruction Limited ("CMDS") in Fanling. The wastes contain personal data of patients such as their names, genders, ages/dates of birth and identity card numbers.

CMDS has been appointed as the waste disposal service provider of the HA since 2009.

Under the Ordinance, where a data user outsources the work of data processing, Privacy Commissioner has no authority to regulate directly the work of a data processor (contractor). The onus is on the data user to use contractual or other means to secure its contractor's compliance with the Ordinance.

The PCPD's self-initiated investigation into the two incidents have revealed two key issues:

1. Contractual omission. There is no contractual requirement that the number of bags of thermal ribbon waste is checked to prevent accidental loss during transit, or that the waste is shredded to the extent that the personal data contained therein could not be readily recognised or recovered.

2. Inadequate supervision of contractor. Neither HA Head Office nor the hospitals had exercised the right provided by the contract to effectively inspect the shredding process at CMDS' factory. HA Head Office denied its responsibilities for centrally monitoring the inspections and had never reviewed the hospitals' inspection reports. Moreover, HA had not carried out any audit to which it is entitled under the Contract to review compliance throughout the whole handling process of hospital wastes.

Privacy Commissioner has served an enforcement notice on HA, directing it to: (1) endeavour to retrieve and destroy the abandoned hospital wastes identified in the two incidents, and (2) review and revise the hospital wastes disposal process, and implement specified improvement measures.

Privacy Commissioner stressed that the breach illustrates 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 HA's contractor in the treatment of hospital wastes containing personal data is unacceptable, and the HA's oversight of CMDS' performance, in terms of contractual and procedural rigour as well as physical supervision, is also far from satisfactory.

Read the Investigation Report: www.pcpd.org.hk/english/publications/files/R13_6740_e.pdf

就「2014數碼21資訊科技策略公眾諮詢」表達意見
Response to the Public Consultation on 2014 Digital 21 Strategy

公署於2013年11月回應了政府發出的「2014數碼21資訊科技策略公眾諮詢」文件，提倡在設計和運用資訊及通訊科技方面採納「貫徹私隱保障」的方針。

公署指出文件裡提及的四項新技術，包括運用雲端運算、大數據分析、物聯網及無線及多平台技術，各有其潛在的私隱問題：

在推動自由使用公共資訊方面，政府應留意存在於公共領域，包括公共登記冊的個人資料，依然受條例的規管。而匿名化和去除身份識別元素的技術，有助機構延長對資料的保留，重訂使用目的和進行分析，同時可保障私隱。

對於政府提議把所有向公眾發佈的資訊預設為「機器可讀」，公署有所保留，因為該做法會便利資料的整合、重整和配對，令其後的資料使用產生新的目的，可能違反有關資料用途的保障資料原則。

在私隱保障教育方面，政府應要求資訊及通訊科技專業人員備有私隱管理和個人資料保障的技能和能力，並考慮在大學及專上院校的課程納入私隱和個人資料保障單元。

意見書：www.pcpd.org.hk/english/infocentre/sub_pub_con.html
（只有英文版）

The PCPD advocates the "Privacy by Design" approach for the design and use of information and communication technologies ("ICTs") in a paper submitted in November 2013 to the Government in response to the public consultation on the 2014 Digital 21 Strategy.

The PCPD points out that the four enabling technologies namely cloud computing, big data analytics, Internet of Things, wireless and multi-platform technologies mentioned in the strategy have privacy concerns of their own.

In promoting public sector information for free re-use, the Government should take note that personal data available in the public domain, including those in public registers, are still subject to regulation under the Ordinance. Anonymisation and de-identification techniques may be adopted as means to enable prolonged retention, repurposing and analytics of personal data in the public domain, while at the same time preserving privacy.

The PCPD has grave reservations for the proposal to make all Government information released to the public machine-readable by default, as it facilitates aggregation, re-arranging and matching of such data which could lead to a function creep, that is, use of the data by subsequent data users for a new purpose in contravention of the data protection principle on use of personal data.

On privacy education, the Government should include privacy management and data protection as part of the required skills and capabilities for ICT professionals, and consider to incorporate privacy and data protection modules in the academic programmes of universities and other tertiary institutions.

Submissions: www.pcpd.org.hk/english/infocentre/sub_pub_con.html

就驗毒助康復計劃諮詢文件提交意見
PCPD's Submissions in Response to Public Consultation on Drug Testing Scheme

公署回應政府提出的驗毒助康復計劃公眾諮詢，公署今年一月提交意見書，申明驗毒測試本身高度侵犯個人私隱，敦請政府當局審視計劃對個人資料私隱方面的影響，考慮採取侵擾程度較低的替代方案和提供實質證據支持有必要推行計劃。

禁毒常務委員會發出諮詢文件，邀請公眾討論應否及如何立法，至使在有強烈環境因素合理懷疑某人曾吸食危險毒物的情況下授權執法人員進行驗毒測試。

意見書：www.pcpd.org.hk/english/files/infocentre/resue_drugtest.pdf

In response to the public consultation on the Government proposed RESCUE Drug Testing Scheme, the PCPD made submissions in January asserting that drug testing is extremely intrusive to one's privacy right, and calls upon the Government to consider its impact on individual's personal data privacy, the availability of other less privacy intrusive alternatives, and to provide more substantial evidence to justify the proposal.

The consultation paper prepared by the Action Committee Against Narcotics invited views on whether and, if so, how legislation should be introduced to authorise drug testing on a person who is suspected to have taken dangerous drugs when there are reasonable grounds, based on circumstantial conditions.

Submissions: www.pcpd.org.hk/english/files/infocentre/resue_drugtest.pdf

公眾教育巡迴展覽
Public Education Roadshow

公署於去年12月至今年3月於港九新界七個地點舉辦公眾教育巡迴展覽，推廣保障個人資料和私隱的重要性。巡迴展覽旨在協助市民認識條例所保障的個人資料私隱權，以及了解條例去年經修訂後對日常生活的影響。公署於巡迴展覽期間派發新出版的《個人資料私隱，自己作主話事》小冊子。

A public education roadshow was launched in seven locations from December 2013 to March 2014 to promote the importance of personal data and privacy protection. The roadshow aimed to enhance public awareness and understanding of individuals' privacy rights under the Ordinance and how the recent amendments to the Ordinance impact on everyday life. Copies of a newly-published handbook *'Have My Say on Personal Data Privacy'* were distributed during the roadshow.

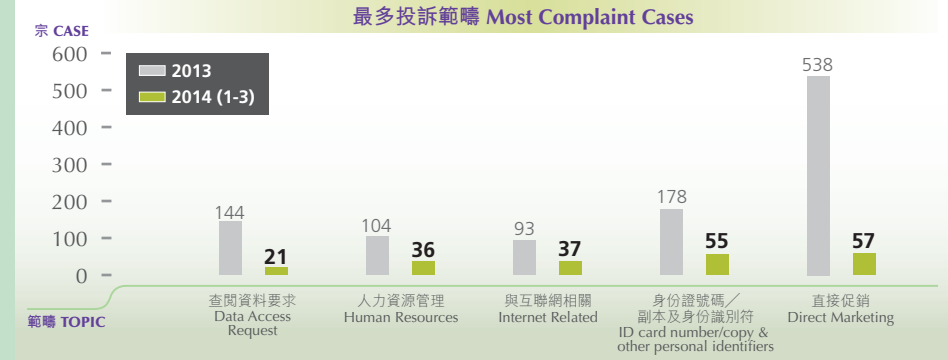
大學保障私隱活動
University Privacy Campaign

以大學生為對象的校園推廣私隱活動於去年10月展開，公署走訪本港十間大專院校，舉行巡迴講座及有獎攤位遊戲，以互動形式介紹條例如何保障個人資料私隱，以及分享使用智能電話保障私隱的實用資訊。公署亦藉此機會向教職員講解資料使用者在條例下應履行的責任，妥善處理學生和員工的個人資料。

The PCPD embarked on its educational programmes for university students in October 2013 with campus tours across ten local universities. The campaign introduced how the Ordinance protects the personal data privacy of individuals and shared practical tips on data protection while using smartphone through a series of talks and interactive booth games. The PCPD also explained to university staff the kind of obligations they have as data users under the Ordinance, and how they should handle the personal data of students and staff.

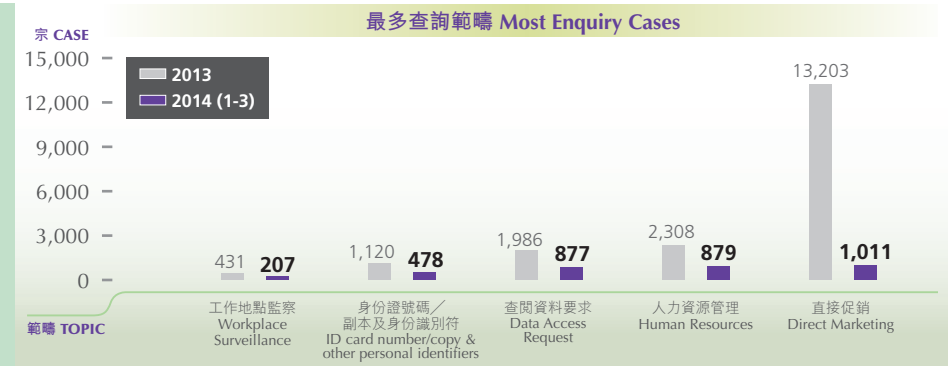
接獲投訴個案
(2014年1月至3月)：
394 宗

Number of complaint cases received
(January – March 2014):
394 cases



接獲查詢數目
(2014年1月至3月)：
4,635 宗

Number of enquiry cases
(January – March 2014):
4,635 cases



詞彙
Glossary

私隱影響評估 Privacy Impact Assessment

私隱影響評估是機構決策過程有用的系統性評估工具，有助機構充分考慮計劃或項目對個人資料私隱的影響。

《個人資料(私隱)條例》沒有明確規定資料使用者必須進行私隱影響評估，但公署建議機構在推行可能對個人資料私隱有重大影響的業務項目或計劃前，應考慮進行私隱影響評估，以審視對個人資料私隱的影響和識別潛在的私隱問題，進而在設計階段提供解決方案或措施，避免或減低不利的影響。私隱影響評估亦可為日後的循規審查和監控提供基準。

所謂對個人私隱有重大影響是指涉及處理或儲存大量個人資料；使用影響廣泛和私隱侵犯程度高的技術；或機構擬在措施方面作出重大改變，引致收集、處理或共用個人資料的數量和範圍擴大。

香港特區政府引入智能身份證之前，曾四度作私隱影響評估。

私隱評估過程一般包括：

- 個人資料的處理周期分析，涵蓋資料的收集、保留、準確性、使用(包括披露和轉移)、保安、政策透明度、查閱和改正
- 私隱風險分析
- 避免或減低私隱風險
- 評估報告

為免與規管角色有衝突，私隱專員不會認可或批核私隱影響評估報告。

詳情可參考公署出版的私隱影響評估資料單張：www.pcpd.org.hk/chinese/publications/files/PIAleaflet_c.pdf

A Privacy Impact Assessment ("PIA") is a systematic risk assessment tool that can be integrated into the decision-making process to evaluate the impact of a proposal on personal data privacy.

Although PIAs are not explicitly provided for under the Personal Data (Privacy) Ordinance, the PCPD recommends data users undertake a PIA before the launch of any new business initiative or project that might have a significant impact on personal data privacy. The objective is to identify privacy risks so that data users can use a privacy-by-design approach and privacy-enhancement measures at the design stage of a personal data system, in order to avoid or mitigate any potential negative impact. A PIA can also provide a benchmark for future privacy compliance audits and control.

A PIA should address significant processing or collection of massive personal data; the implementation of privacy intrusive technologies that might affect a large number of individuals; or a major change in organisational practices that may result in expanding the amount and scope of personal data to be collected, processed or shared.

For instance, before the HKSAR Governmant introduced the SMART identity card, four PIAs were undertaken.

The PIA process should generally include:

- Data processing cycle analysis, covering collection, accuracy, retention, use (including disclosure and transfer), security, policy transparency, access, and correction of personal data;
- Privacy-risk analysis;
- Measures to avoid or mitigate potential privacy risks; and
- PIA reporting.

To avoid any potential conflict with its regulatory role, Privacy Commissioner neither endorses nor approves the PIA reports of organisations.

To learn more, please read the PCPD information leaflet "Privacy Impact Assessment": www.pcpd.org.hk/chinese/publications/files/PIAleaflet_c.pdf

網上私隱要自保　公司機構篇
Be Smart Online Resources for Businesses

對企業和機構來說，儲存在其電腦系統的資料，包括客戶、員工、商業合作夥伴等個人資料，都是有用的數據和重要的資產；加上不少機構順應潮流而紛紛開拓網上業務，要妥善地管理這些網上和電腦上的資料，有效的私隱政策及常規至為重要。

除了資料保安，機構亦須履行《個人資料(私隱)條例》下的責任，保障個人資料私隱。

機構疏於個人資料保障，而在事後才採取補救措施，不但費時失事，更有可能會賠上機構的聲譽和顧客的信任。

以本港消費者為對象的調查研究指出：

- 市民對資料保安的關注有增加之勢，互聯網資料保安的關注度升幅最大。(1)
- 84%受訪者擔心別人取得或使用自己的信用咭及信貸資料；以及擔心個人資料未經授權而被讀取或誤用。(1)
- 56%表示擔心網上購物和網上理財的保安 (1)
- 81%表示，若機構因資訊保安問題而損害其個人資料私隱，他們不會再跟有關機構交易。(2)

另外，外國研究指出，容許員工使用流動裝置的機構，半數機構曾經因為員工不慎地使用流動裝置而外洩資料。(3)

公署在「網上私隱要自保」專題網站為企業和機構而設的專區（www.pcpd.org.hk/besmartonline/business.html），提醒機構在應用互聯網和通訊科技時如何妥善保障個人資料和私隱，並提供的指引、單張或刊物以供參考：

For many businesses and organisations, the data stored on their IT systems, including the personal data of customers, employees, business partners and so on, is a useful and valuable asset. As more businesses are operating online, it is essential for organisations to put in place an effective data privacy policy and practice to properly manage the data on computers and on the Internet

Apart from data security concern, they should also note that there are legal obligations under the Personal Data (Privacy) Ordinance which govern how businesses should manage personal data to ensure privacy. Not protecting your customer information could have a negative impact on the reputation of your business and customer relationship. It is also costly for the organisation to arrange a remedy.

The findings of studies on local consumers show that:

- The concern about security, in particular Internet security was on the rise. (1)
- 84% of the respondents were extremely or very concerned about other people obtaining or using their credit/debit card details; and about unauthorised access to or misuse of their personal information. (1)
- 56% were concerned about the security of online shopping and online banking. (1)
- 81% said they would stop dealing with an organisation, such as closing their accounts, if their personal information had been breached. (2)

Furthermore, according to an overseas study report, 51 % of the organisations which allowed their employees to bring their own devices to work had experienced data loss resulting from employee use of insecure mobile devices. (3)

To support organisations, the PCPD provides a range of resources on its "Be Smart Online" mini-website (www.pcpd.org.hk/besmartonline/en/business.html). Tips for compliance when doing business online and using Information and Communication Technologies, as well as guidelines and information leaflets, are available.

資料來源 Sources：
1. Unisys Security Index Report Hong Kong – May 2013
www.unisyssecurityindex.com.hk
2. Hong Kong customer actions after unauthorised access of personal information held by an organisation – Nov 2011
www.unisyssecurityindex.com/usi/hong-kong/additional_research
3. Research Report: Global Study on Mobility Risks by Ponemon Institute
www.websense.com/content/ponemon-institute-research-report-2012.aspx?cmpid=prnr2.29.12

工作間的自携電子裝置政策 Bring-Your-Own-Device Policy at workplace	如你的機構容許員工使用私人流動裝置或便携裝置處理公務，你必須明白這些裝置所帶來的私隱風險，例如裝置是否符合機構的資訊安全標準，機構是否有方法追蹤流動裝置的使用情況和監察資料外洩事故。 If your organisation allows the use of private mobile or portable devices, you should realise that the risk of using such device – whether they meet the organisation's security standards, whether it is possible to track the uses and monitor data breach incidents.
慎防經網站洩露資料 Data breach through website	在互聯網上設有網站的機構，必須有在系統設計和管理、密碼設定、權限控制、網址和員工培訓等各方面採取保安措施，把網站意外洩露資料的風險減至最低。 If your organisation has a website on the Internet, make sure that you take security measures in relation to the system design and maintenance, password setting, access control, access parameters in the web address so as to minimise the risk of data breach.
使用雲端運算 Cloud computing	在決定使用雲端運算處理個人資料前，必須明白有何個人資料私隱和保安風險或是否已詳細考慮公署的建議以規範雲端服務供應商。 Before you decide to use Cloud computing to handle your organisation's data, ensure that you are clear about the risks you would encounter, and consider the PCPD's recommendations on how to ensure their compliance with the Ordinance.
網上營商 Doing business online	機構在網上收集及處理個人資料；用社交媒體進行市場推廣；在社交網絡上提供客戶服務、人力資源管理，以致分析目標顧客的資料以提升銷售效益等，這些活動都涉及個人資料的處理，應遵從條例規定。另外，如機構使用取自公共領域的個人資料作新的用途，有機會違反資料用途方面的保障資料原則。 If your organisation engages in online activities from collecting and handling of personal data; social media marketing, social network customer services, human resources management, to analysing the data of potential customers, you will need to adhere to the requirement of the Ordinance. If you organisation uses personal data obtained from public domain for new purposes, you should be aware of the risk of violating the data protection principle on data use.
培訓及資源 Training & resources	你的機構必須有為員工，特別是內部資訊科技人員提供合適的培訓。委託應用程式開發商和其他服務承辦商時應作相應的考慮和安排以確保個人資料私隱。 Make sure you provide suitable training for your staff, in particular internal IT staff. When you commission an app developer or a service provider, make sure you have considered the relevant factors and make the appropriate arrangement for data protection.

網站 Website

1 私隱管理系統網站
Privacy Management Programme website
www.pcpd.org.hk/pmp

2 關注私隱運動網站
Privacy Awareness Week website
www.pcpd.org.hk/paw

最佳行事方式指引 Best Practice Guide

3 私隱管理系統最佳行事方式指引
Privacy Management Programme: A Best Practice Guide

小冊子 Leaflet

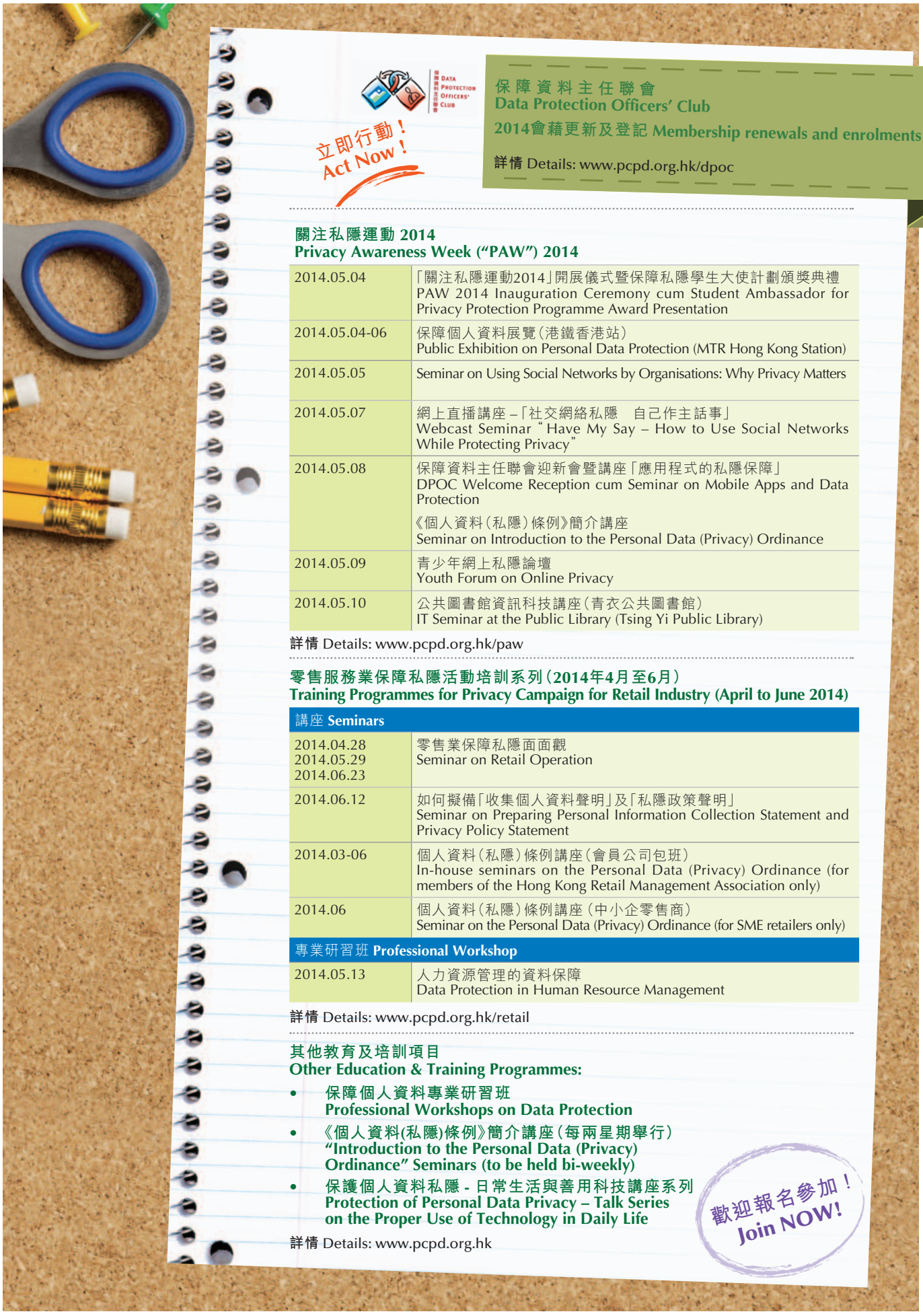
4 個人資料私隱，自己作主話事
Have My Say on Personal Data Privacy

有意訂閱電子版的《私隱專員公署通訊》，請以電郵與我們聯絡：
newsletter@pcpd.org.hk

We recommend you subscribe to PCPD News online at newsletter@pcpd.org.hk

電話 tel 2827 2827
傳真 fax 2877 7026
電郵 e-mail enquiry@pcpd.org.hk

瀏覽電子版 View e-version:
www.pcpd.org.hk > 出版刊物及錄影帶　或歡迎到公署辦事處索取。
www.pcpd.org.hk > Publications & Videos, or obtain a copy at PCPD office



立即行動！
Act Now！

保障資料主任聯會
Data Protection Officers' Club
2014會藉更新及登記 Membership renewals and enrolments

詳情 Details: www.pcpd.org.hk/dpoc

關注私隱運動 2014
Privacy Awareness Week ("PAW") 2014

2014.05.04	「關注私隱運動2014」開展儀式暨保障私隱學生大使計劃頒獎典禮 PAW 2014 Inauguration Ceremony cum Student Ambassador for Privacy Protection Programme Award Presentation
2014.05.04-06	保障個人資料展覽（港鐵香港站） Public Exhibition on Personal Data Protection (MTR Hong Kong Station)
2014.05.05	Seminar on Using Social Networks by Organisations: Why Privacy Matters
2014.05.07	網上直播講座 –「社交網絡私隱　自己作主話事」 Webcast Seminar "Have My Say – How to Use Social Networks While Protecting Privacy"
2014.05.08	保障資料主任聯會迎新會暨講座「應用程式的私隱保障」 DPOC Welcome Reception cum Seminar on Mobile Apps and Data Protection 《個人資料（私隱）條例》簡介講座 Seminar on Introduction to the Personal Data (Privacy) Ordinance
2014.05.09	青少年網上私隱論壇 Youth Forum on Online Privacy
2014.05.10	公共圖書館資訊科技講座（青衣公共圖書館） IT Seminar at the Public Library (Tsing Yi Public Library)

詳情 Details: www.pcpd.org.hk/paw

零售服務業保障私隱活動培訓系列（2014年4月至6月）
Training Programmes for Privacy Campaign for Retail Industry (April to June 2014)

講座 **Seminars**	
2014.04.28 2014.05.29 2014.06.23	零售業保障私隱面面觀 Seminar on Retail Operation
2014.06.12	如何擬備「收集個人資料聲明」及「私隱政策聲明」 Seminar on Preparing Personal Information Collection Statement and Privacy Policy Statement
2014.03-06	個人資料（私隱）條例講座（會員公司包班） In-house seminars on the Personal Data (Privacy) Ordinance (for members of the Hong Kong Retail Management Association only)
2014.06	個人資料（私隱）條例講座（中小企零售商） Seminar on the Personal Data (Privacy) Ordinance (for SME retailers only)
專業研習班 Professional Workshop	
2014.05.13	人力資源管理的資料保障 Data Protection in Human Resource Management

詳情 Details: www.pcpd.org.hk/retail

其他教育及培訓項目
Other Education & Training Programmes:

- 保障個人資料專業研習班
  Professional Workshops on Data Protection
- 《個人資料(私隱)條例》簡介講座（每兩星期舉行）
  "Introduction to the Personal Data (Privacy) Ordinance" Seminars (to be held bi-weekly)
- 保護個人資料私隱 - 日常生活與善用科技講座系列
  Protection of Personal Data Privacy – Talk Series on the Proper Use of Technology in Daily Life

詳情 Details: www.pcpd.org.hk

歡迎報名參加！
Join NOW!