

執法 保障資料 Enforcing Data Protection

調查不偏不倚

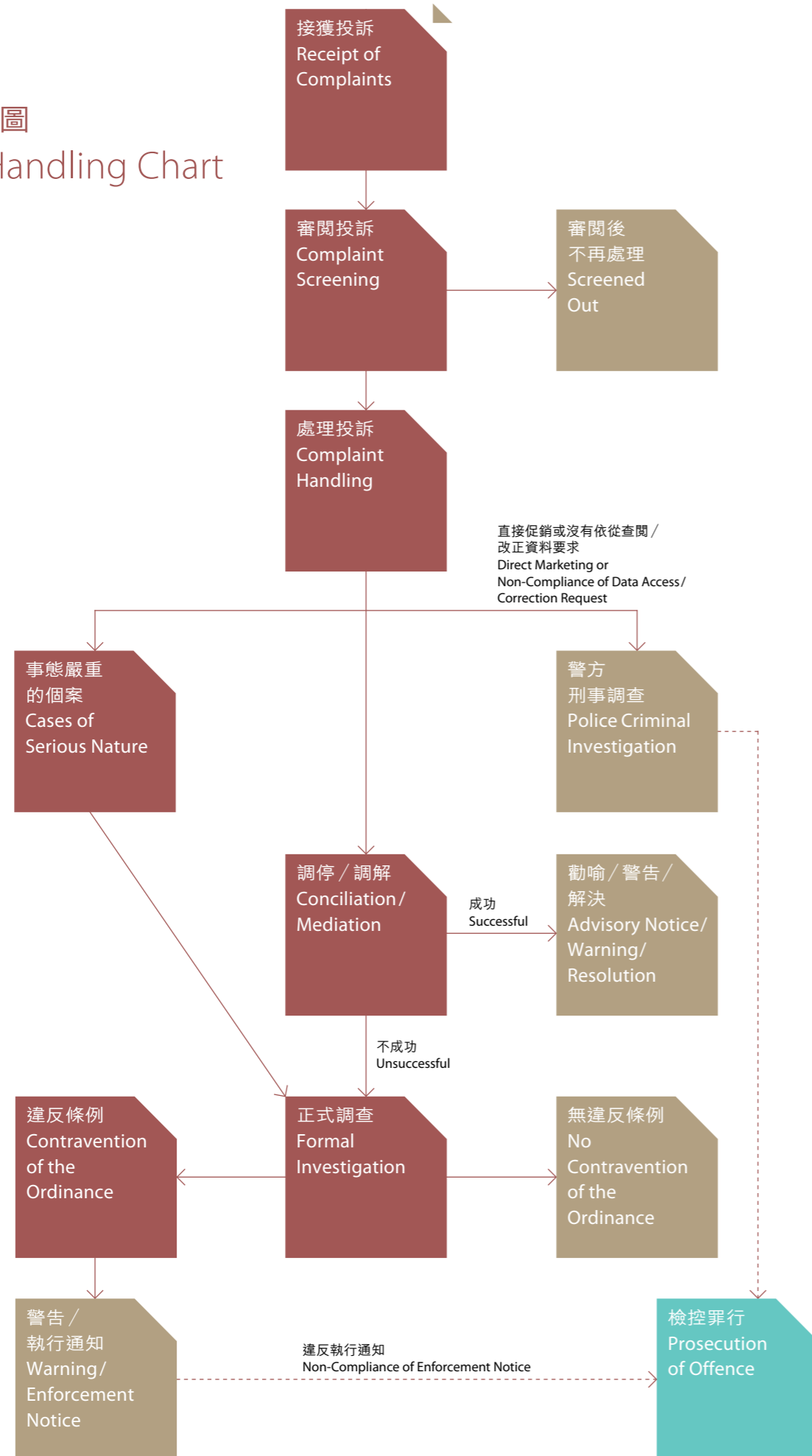
對於市民的投訴，執法及投訴科會作出具效率、公平公正的調查及處理。若發現有顯著私隱風險的情況存在，我們更會主動作出調查。

Thorough and Impartial Investigations

The Enforcement & Complaints Section investigates and resolves complaints effectively and in a manner that is fair to all parties concerned, and proactively investigates areas where privacy risks are significant.



處理投訴程序圖
Complaint Handling Chart



調查投訴

接獲有關個人資料私隱的投訴

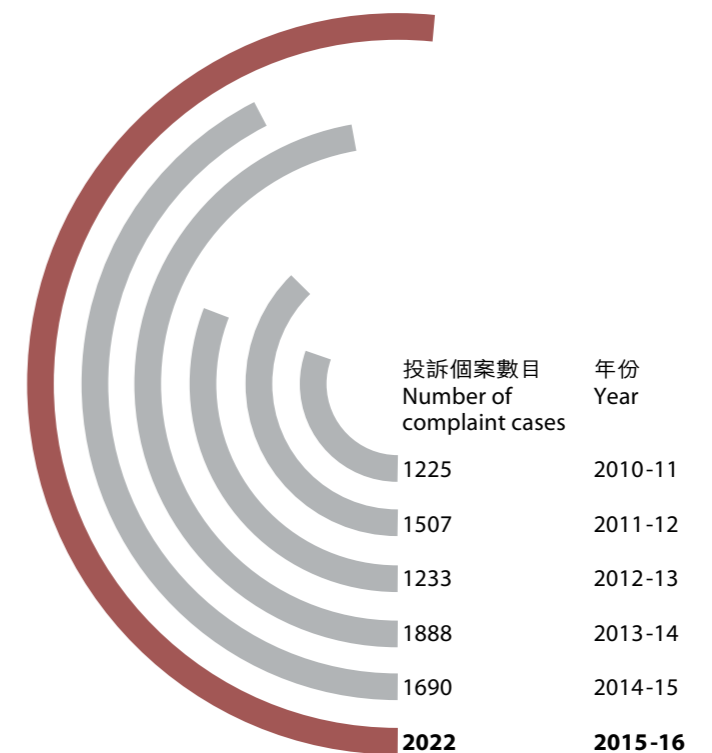
公署在2015至16年度共接獲2,022宗投訴個案，為歷年最多，較上年度上升了20%。(圖3.1)

COMPLAINT INVESTIGATION

Data Privacy Complaints Received

A record high 2,022 complaint cases were received in 2015-16, a 20% increase from that of the previous year. (Figure 3.1)

圖Figure 3.1 投訴個案數字
Number of complaint cases received



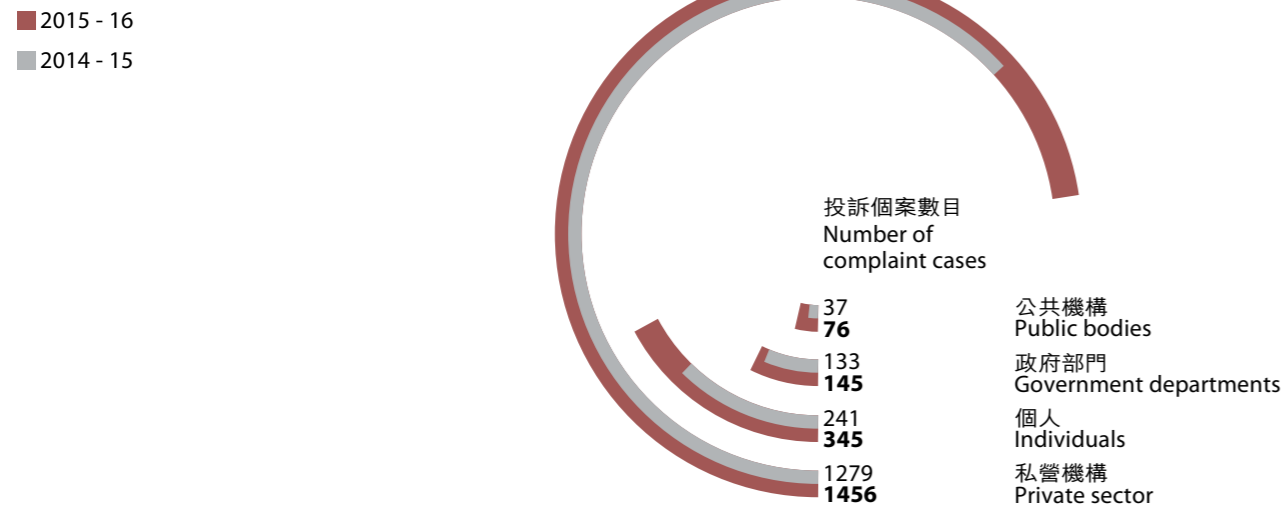
本年度所接獲的2,022宗投訴個案包括：

- 72% (1,456宗) 投訴私營機構；
- 17% (345宗) 投訴個人；及
- 11% (221宗) 投訴公營機構（即政府部門及公共機構）。（圖3.2）

Among 2,022 cases received during the year :

- 72% (1,456 cases) were against private-sector organisations;
- 17% (345 cases) were against individuals; and
- 11% (221 cases) were against public-sector organisations. (Figure 3.2)

圖 Figure 3.2 被投訴者類別
Types of parties complained against



私營機構的包括：

- 25% (367宗) 投訴銀行及財務機構；
- 14% (199宗) 投訴物業管理公司；及
- 7% (101宗) 投訴電訊公司。（圖3.3）

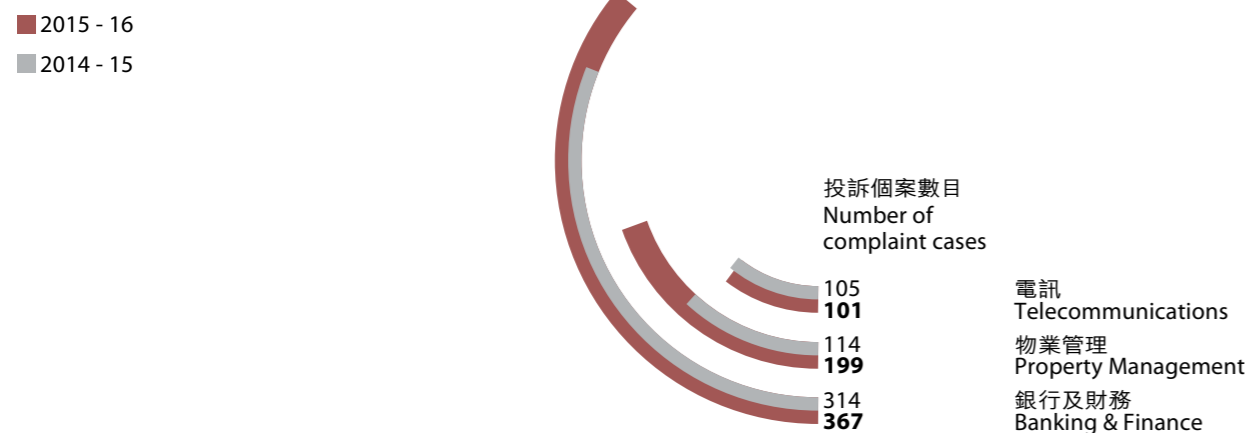
For the private-sector organisations :

- 25% (367 cases) were against the banking and financial sector;
- 14% (199 cases) were against the property management; and
- 7% (101 cases) were against the telecommunications sector. (Figure 3.3)

針對電訊及財務機構的投訴個案，大部分都是涉及收集個人資料和違反條例有關直接促銷的新條文。

The majority of the complaints against companies in the telecommunications and financial sectors related to the collection of personal data and breaches of the new direct marketing provisions of the Ordinance.

圖 Figure 3.3 對私營機構的投訴
Complaints against private-sector organisations



投訴公營機構的個案中，大部分涉及：

- 不符收集目的，及未取得當事人同意而使用或披露個人資料（34%）；
- 過度或不公平收集個人資料（26%）；
- 未能遵守查閱資料要求或改正資料要求（16%）；或
- 欠缺保障個人資料的保安措施（15%）。

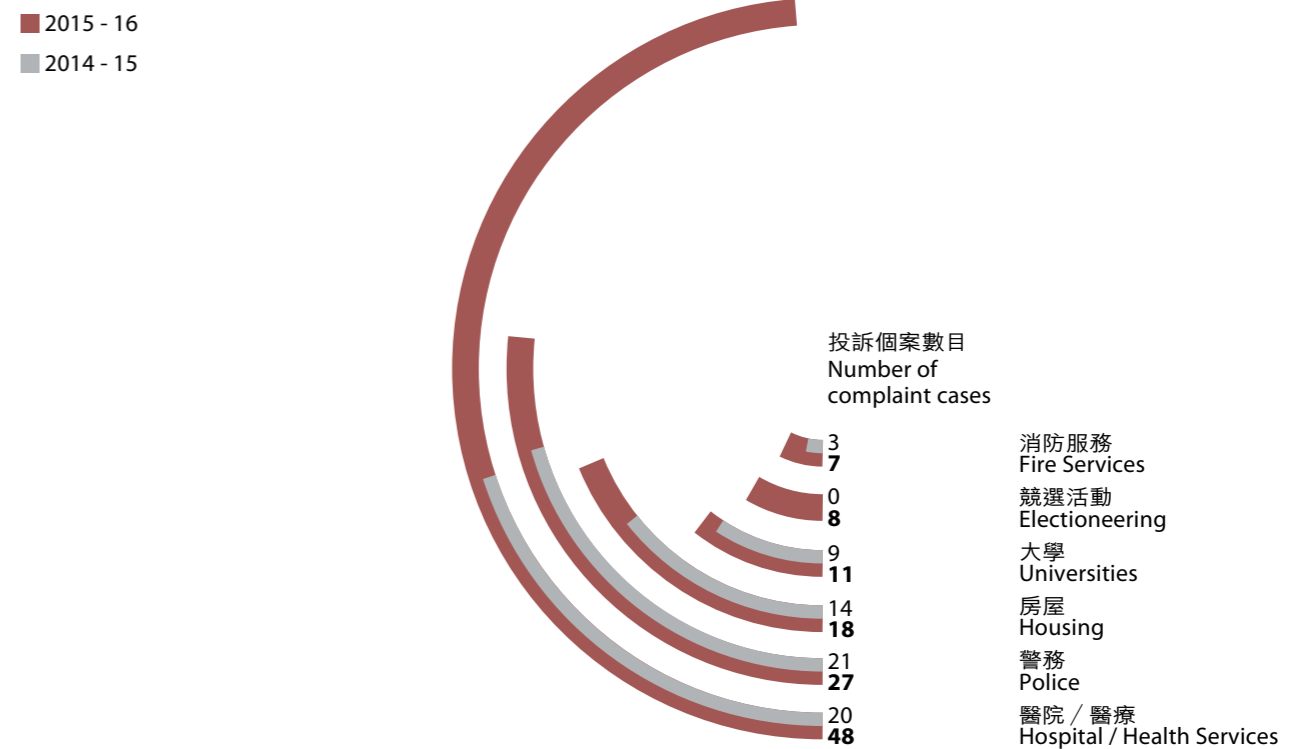
The majority of complaints against public-sector organisations involved :

- the use or disclosure of personal data beyond the scope of the collection purpose and without the consent of the individual (34%);
- the excessive or unfair collection of personal data (26%);
- non-compliance with data access or correction requests (16%); or
- lack of security measures to protect personal data (15%).

涉及醫院／醫療服務、警務，以及房屋的投訴最多。（圖3.4）

The hospital/health service organisations, police force, and housing generated most of the complaints. (Figure 3.4)

圖 Figure 3.4 對公營機構的投訴
Complaints against public-sector organisations



公署於2015至16年度接獲的2,022宗投訴個案，涉及2,585項違反條例規定的指稱包括：

- 2,091項 (81%) 指稱違反保障資料原則 (本身不構成刑事罪行)；及
- 494項 (19%) 則指稱違反條例的條文。

投訴指稱的性質如下 (圖3.5)：

- 862項與收集資料的目的及方式有關；
- 835項與個人資料在未經同意的情況下被使用有關；
- 321項與直接促銷有關；
- 237項與資料的保安有關；
- 165項與依從查閱或改正資料要求有關；
- 149項與資料的準確性及保留期有關；及
- 8項與資料政策的公開度有關。

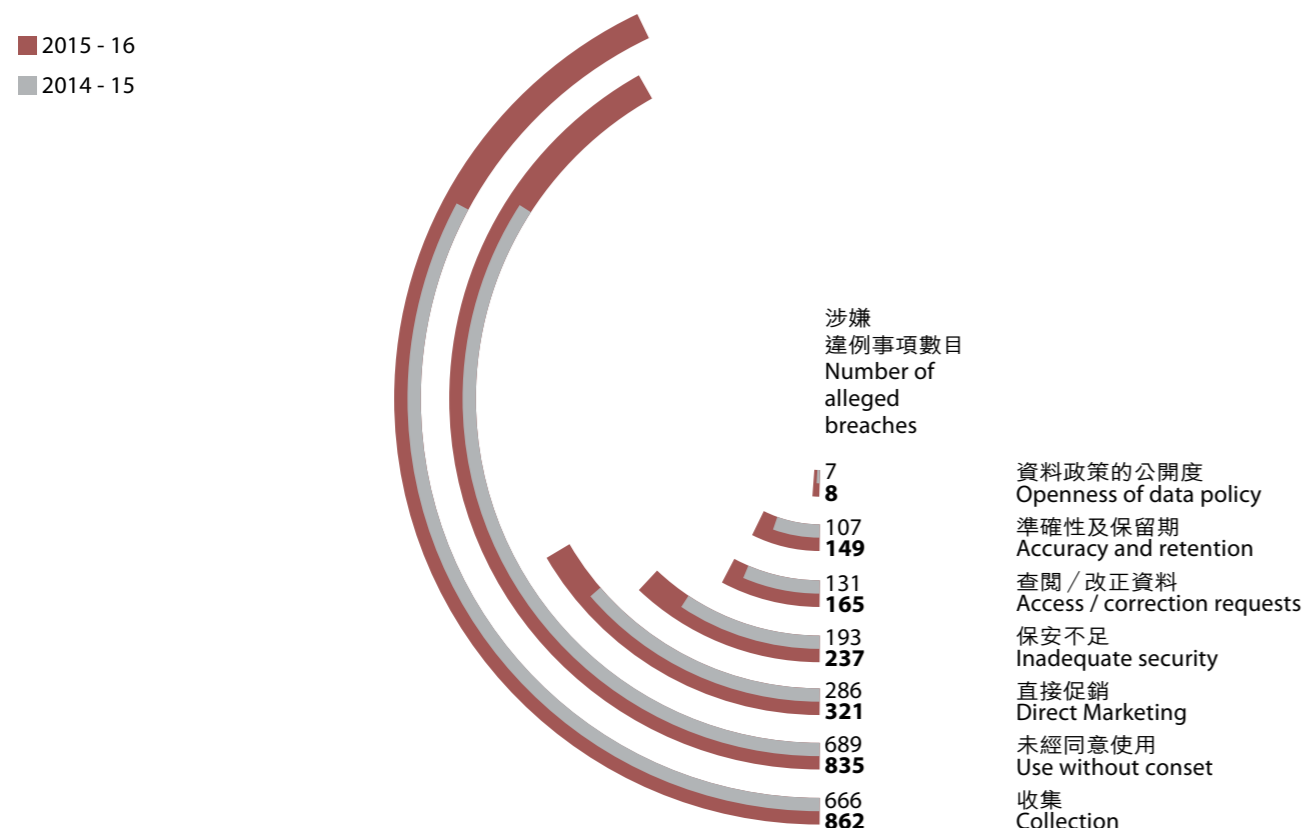
Of the 2,022 complaints received in 2015-16, a total of 2,585 alleged breaches of the requirements under the Ordinance were involved:

- 2,091 (81%) were alleged breaches of the data-protection principles (not a criminal offence per se); and
- 494 (19%) were alleged contraventions of the provisions of the Ordinance.

Nature of the complaint allegations was as follows (Figure 3.5):

- 862 related to the purpose and manner of data collection;
- 835 related to the use of personal data without the consent of the individual concerned;
- 321 related to direct marketing;
- 237 related to data security;
- 165 related to compliance with data access or correction requests;
- 149 related to accuracy and period of retention; and
- 8 related to openness of data policy.

圖 Figure 3.5 投訴的性質
Nature of complaints



值得注意的是，公署於2015至16年度接獲127宗與競選活動有關的投訴，當中大部分 (106宗) 是於2015至16年度第三季錄得並與2015年區議會選舉有關。大多數投訴是關於個人資料在未取得同意下被用於選舉活動。公署於2015年8月更新了《競選活動指引》，就候選人及其選舉代理人如何遵從條例的規定提供實務性指引。

圖3.6顯示投訴涉及的範疇。2015至16年度有關資訊及通訊科技的投訴達239宗，較上年度上升7%。投訴數字上升的主要原因是智能電話和互聯網的使用日益普遍。有關資訊及通訊科技的投訴涉及：

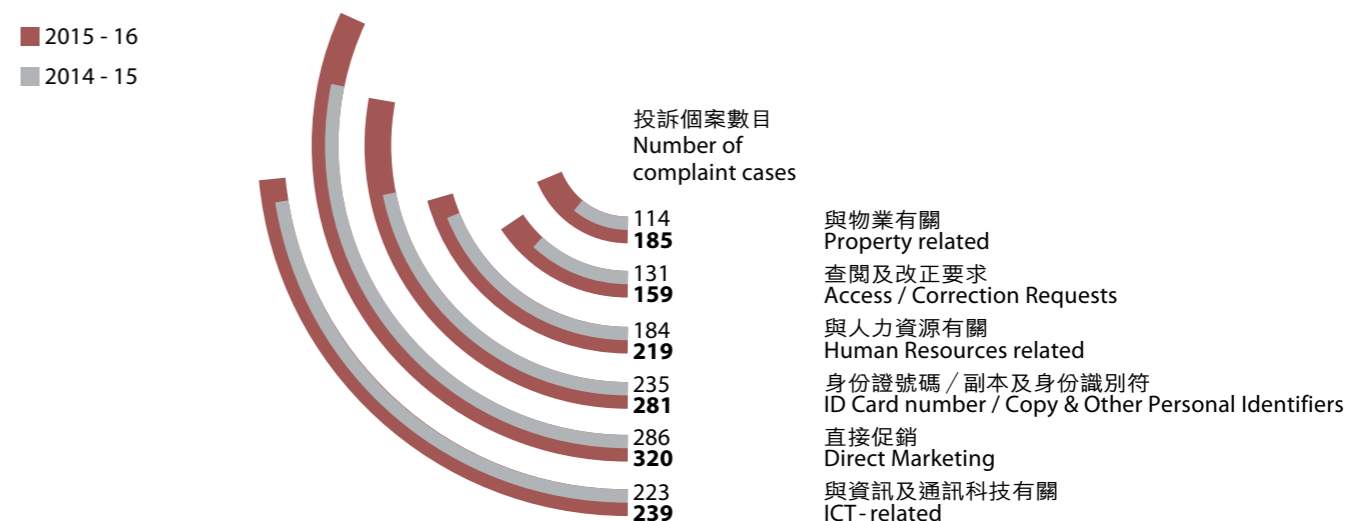
- 90宗與社交網絡有關；
- 85宗關於在互聯網上披露或洩漏個人資料；
- 54宗關於智能電話應用程式；
- 28宗關於網絡欺凌；及
- 22宗屬其他事項。

It is worth noting that the PCPD received a total of 127 electioneering-related complaints in 2015-16. The majority of these complaints (106 cases) was received in the third quarter of 2015-16 and was related to the 2015 District Council Election. Most of the complaints related to using personal data in electioneering activities without consent. The PCPD updated its Guidance on Electioneering Activities in August 2015 to provide candidates and their election agents with practical guidance on compliance with the requirements under the Ordinance.

Figure 3.6 shows the breakdown of complaints by topic. A total of 239 ICT-related complaints in 2015-16 represented a 7% year-on-year increase. The rising trend is principally attributable to the increasing popularity of smartphones and the Internet. ICT-related complaints involved:

- 90 cases related specifically to social networks;
- 85 cases concerned disclosure or leakage of personal data on the Internet;
- 54 cases related to smartphone applications;
- 28 cases involved cyber-bullying; and
- 22 cases related to other sub-topics.

圖 Figure 3.6 投訴涉及的範疇
Complaints by topic



在本年度，公署處理了253宗由上年度帶下來的投訴，加上新接獲的投訴，年內共須處理2,275宗投訴。在這些個案中，2,013宗（88%）在本年報期內已經完結，而餘下的262宗（12%），截至2016年3月31日仍在處理中。

In addition to the new complaints received, the PCPD handled 253 complaints carried forward from the previous year, bringing the total number of complaints handled during the year to 2,275. Of these, 2,013 (88%) were completed during the report year, and 262 (12%) were still in progress as at 31 March 2016.

年度投訴摘要
Summary of complaints handled in the year

	2015-16	2014-15	2013-14	2012-13
上年轉來的投訴 Complaints carried forward	253	329	393	381
接獲的投訴 Complaints received	2,022	1,690	1,888	1,233
經處理的投訴 Total complaints processed	2,275	2,019	2,281	1,614
已完結的投訴 Complaints completed	2,013	1,766	1,952	1,221
未完結的投訴 Complaints outstanding	262	253	329	393

投訴結果

本年報期內合共2,013宗個案完結，結案情況如下：

- 243宗（12%）在初步查訊期間經公署調停或調解而得到解決，被投訴者對投訴人提出的問題作出適當的糾正（私隱專員並向其中156間機構提出勸喻及／或建議）；
- 74宗（4%）在正式調查後獲得解決（當中有42宗（57%）經公署調停或調解後得到解決（見下文「正式調查結果」）；及
- 38宗（2%）交由其他規管機構例如警方跟進。（圖3.7）

圖3.11 顯示被投訴者經公署調停後所採取的糾正行動分類。

沒有展開調查的投訴個案：

- 789宗（39%）個案大多經由公署把投訴人的關注轉達至被投訴一方後得到解決，或私隱專員要求投訴人提供證據支持其指稱，但投訴人未有回應；
- 379宗（19%）沒有表面證據證明違規；
- 210宗（10%）不在條例的管轄範圍；
- 162宗（8%）在公署向被投訴者查詢後發現證據不足；及
- 118宗（6%）在初步查詢期間投訴人撤回投訴。

Outcome of Complaint Handling

2,013 cases were completed during the report period as follows (Figure 3.7):

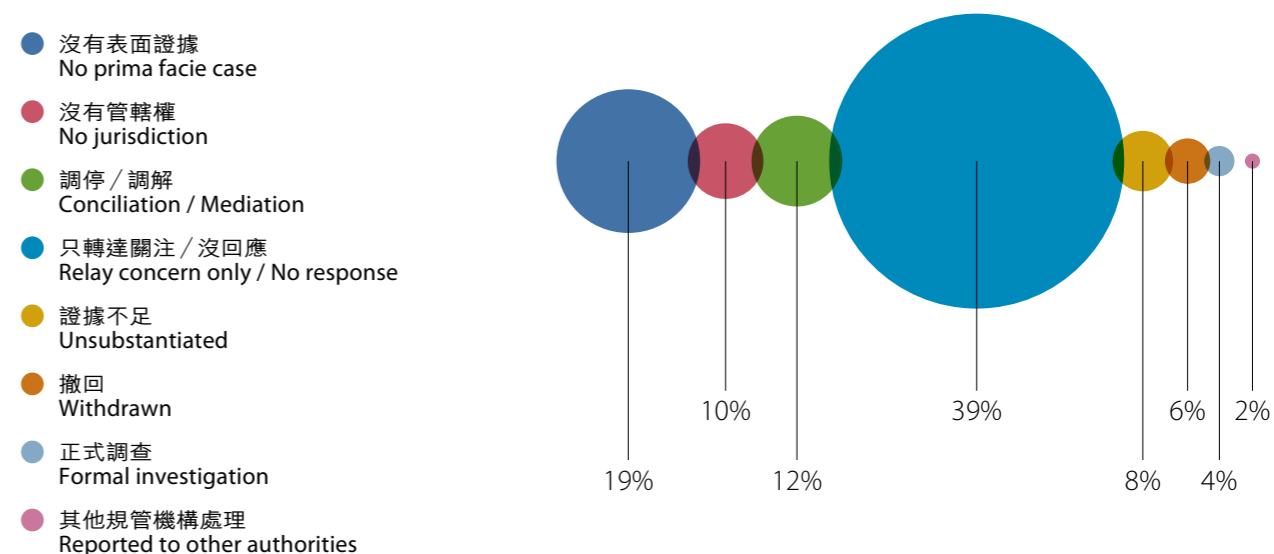
- 243 (12%) were resolved through conciliation or mediation during preliminary enquiries, i.e. the problems raised by the complainants were remedied by the parties complained against. (The Commissioner gave advice and / or recommendations to 156 organisations involved in these cases);
- 74 (4%) were resolved after formal investigation, and of these, 42 cases (57%) were resolved through conciliation or mediation, (see "Results of Formal Investigations" below); and
- 38 (2%) were transferred or reported to the other authorities e.g. Hong Kong Police.

Figure 3.11 shows the breakdown and categorisation of remedial actions taken by the parties complained against in conciliation.

Among the remaining cases which were not investigated:

- 789 cases (39%) involved mostly complaints where the matter at issue had been dealt with by relaying the complainants' concern to the parties complained against, or the complainants did not respond to the Commissioner's inquiries after being invited to provide evidence to support their allegations;
- 379 cases (19%) were found to have no prima facie case of contravention;
- 210 cases (10%) were outside the jurisdiction of the Ordinance;
- 162 cases (8%) were found to be unsubstantiated after enquiries with the parties complained against; and
- 118 cases (6%) were withdrawn by the complainants during the preliminary enquiries.

圖 Figure 3.7 投訴結果
Outcome of complaint handling



投訴個案的調查結果

正式調查結果

公署在本年報期內完成74宗正式調查，當中：

- 10宗（13%）有違反條例規定（保障資料原則）；
- 2宗（3%）沒有違反條例規定；
- 42宗（57%）在調查期間因雙方經調停或調解後解決糾紛；及
- 20宗（27%）因不同原因而終止調查，而在這些個案中，私隱專員毋須調查是否有任何違反情況。（圖3.8）

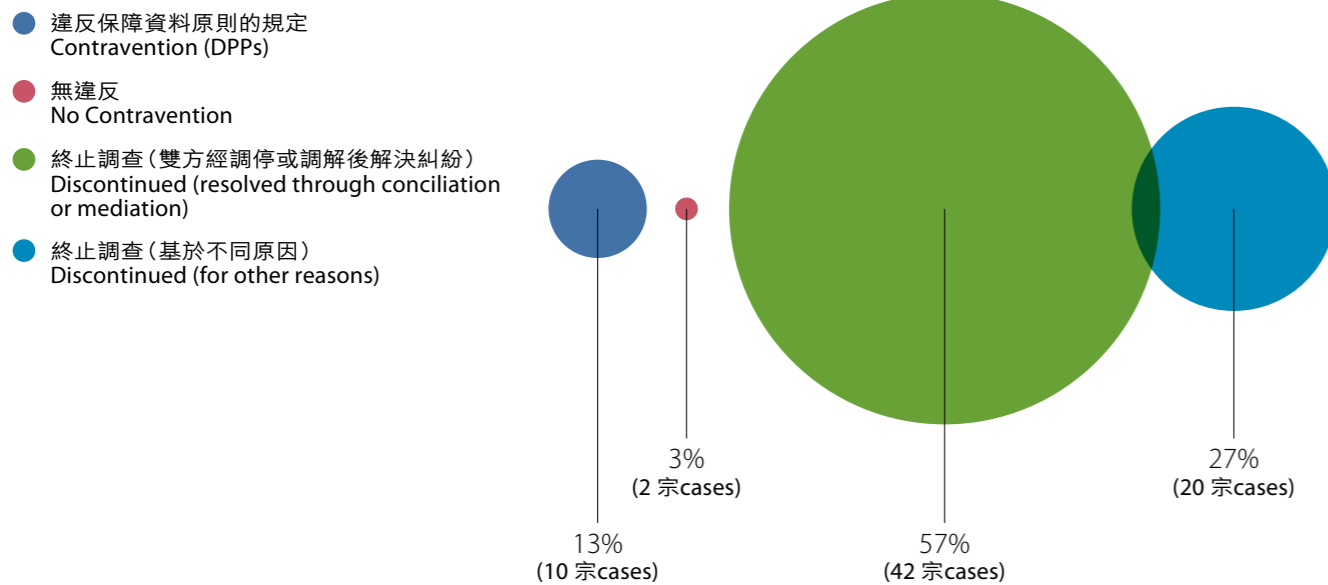
Results of Investigations of Complaint Cases

Results of Formal Investigations

During the report period, the PCPD completed 74 formal investigations, of which :

- 10 cases (13%) were found to have contravened the requirements under the Ordinance (the DPPs under the Ordinance);
- 2 cases (3%) were not found to have contravened the requirements under the Ordinance;
- 42 cases (57%) were resolved through conciliation or mediation during the investigation; and
- 20 (27%) were discontinued for various reasons, and amongst these remaining cases, it was unnecessary for the Commissioner to draw any conclusions as to whether or not there were any contraventions. (Figure 3.8)

圖 Figure 3.8 正式調查結果
Results of formal investigations



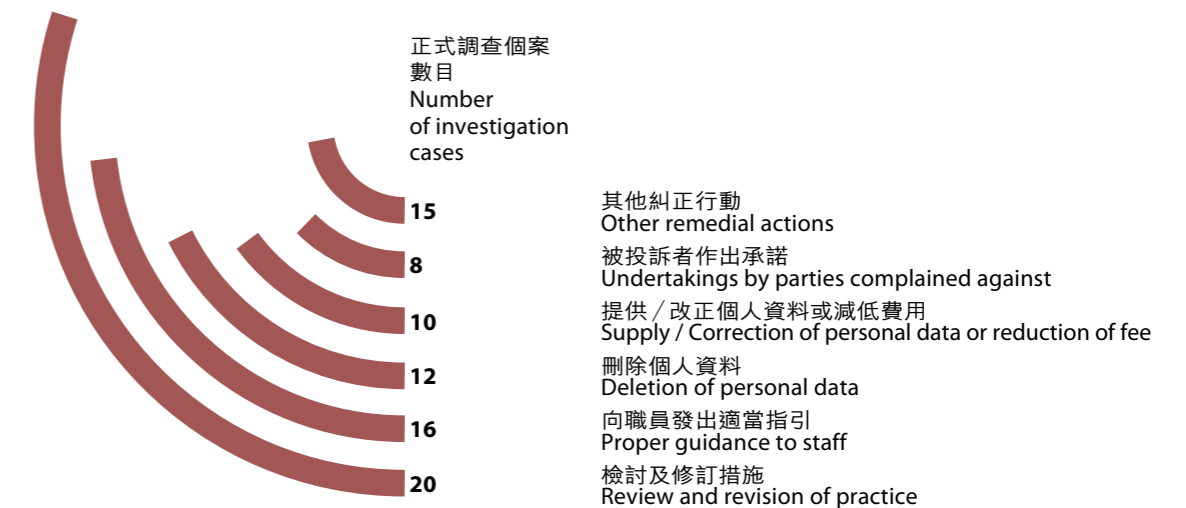
終止調查的個案的糾正行動性質

在42宗經公署調停或調解而得到解決的個案中，被投訴者所採取的糾正行動，請見圖3.9（註：在同一宗個案中，被投訴者採取的糾正行動可能多於一項）。

Nature of Remedial Action in Discontinued Cases

The nature of remedial action taken by the parties complained against in the 42 cases resolved through conciliation or mediation is categorised in Figure 3.9 (N.B.: more than one type of remedial action may have been taken by the party complained against in some cases).

圖 Figure 3.9 糾正行動的性質
Nature of remedial action



在42宗經公署調停或調解而得到解決的個案中，私隱專員對22宗個案的被投訴者發出警告。

Of the 42 conciliated or mediated cases, the Commissioner issued warning notices to the parties complained against in 22 cases.

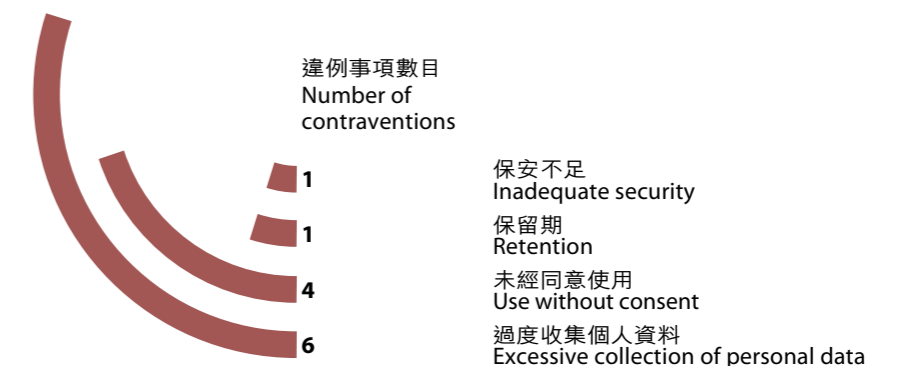
違例事項的性質

在確定違例的10宗個案中，共涉及12項違例事項。至於有關個案所涉及各項違規性質的詳細分類，請見圖3.10（註：一宗個案可涉及違反多於一項保障資料原則）。

Nature of Contravention

A total of 12 contraventions were involved in the 10 cases where the requirements under the Ordinance were found to have been contravened. The classification of the nature of all the contraventions involved in these cases can be found in Figure 3.10 (N. B.: One case may involve a contravention of more than one DPP).

圖 Figure 3.10 違例事項的性質
Nature of contravention



執法行動

公署對違反條例規定的個案採取了執法行動。

在確定違反條例規定的10宗個案中，私隱專員向其中九名被投訴者發出執行通知，以制止或防止他們的違規行為。至於餘下的一宗個案，在被投訴者採取糾正措施後，私隱專員向他發出警告信。

Enforcement Action

The PCPD takes enforcement action in cases of contravention of the requirements under the Ordinance.

Of the 10 cases found to involve contraventions of the requirements under the Ordinance, the Commissioner issued nine enforcement notices to the parties complained against to stop or prevent contraventions. In the remaining case, the Commissioner issued warning notice to the party complained against after he had taken measures to remedy the contravention.

感言 Sharing

我十分榮幸有機會在公署擔任調查主任一職，這份工作讓我有許多機會去接觸社會上不同階層的人，他們來自不同行業。在處理與保障個人資料私隱有關的個案時，我需要徹底掌握條例的規定，有時也需要去了解其他法例才可以協助投訴人解決問題。隨著經驗的累積，除了對公署的運作和相關法例越來越熟習外，也認識了不少其他政府法例，豐富了個人的視野。

對外方面，由於經常接觸不同界別的市民，也豐富了我的社會經驗。現在發現從工作中我開始了解多種行業的運作，包括模式、行規和習慣等，這些知識對自己個人的發展實在裨益不淺。

更加要感謝公署不時提供的多元化培訓活動，例如領袖訓練、調解技巧和英文寫作等，對日常的工作非常有幫助。

日常的工作雖然挑戰重重，但我定必努力學習，積極裝備自己，將學到的知識和技巧活學活用，盡心服務市民。

I am glad that I can work in the PCPD as an investigation officer. This job offers me many opportunities to meet people from all walks of life. In handling matters relating to protection of personal data privacy, I need to have a thorough understanding of the requirements under the Ordinance, and sometimes it is necessary for me to have a grasp of other laws so as to help the complainants solve their problems. As years go by, I have become more proficient in the PCPD's operation and the Ordinance, and I have also learnt more about many other ordinances. My work experience has broadened my horizon.

Meeting people from different sectors has also enriched my social experience. In my work, I came to know of the operation of different industries, including patterns, rules and practices. Such knowledge is very beneficial to my personal development.

I am also thankful to the PCPD's diversified training activities offered to me, e.g. leadership training, mediation skills and English writing. These training courses are very useful.

Although my work is challenging, I will try hard to equip myself and make use of the knowledge and skills learnt to serve the public with passion.



趙玉珍
個人資料主任
(執法及投訴)
Annie CHIU
Personal Data Officer
(Enforcement & Complaints)

經調停或調解而解決的個案的糾正行動性質

在本年報期間，共有285宗個案經公署調停或調解後得到解決（包括243宗在初步查詢期間得到解決的個案，及42宗在調查期間得到解決的個案），被投訴者對投訴人提出的問題作出了適當的糾正。被投訴者所採取的糾正行動，請見圖3.11（在一宗個案中，被投訴者採取的糾正行動可能多於一項）：

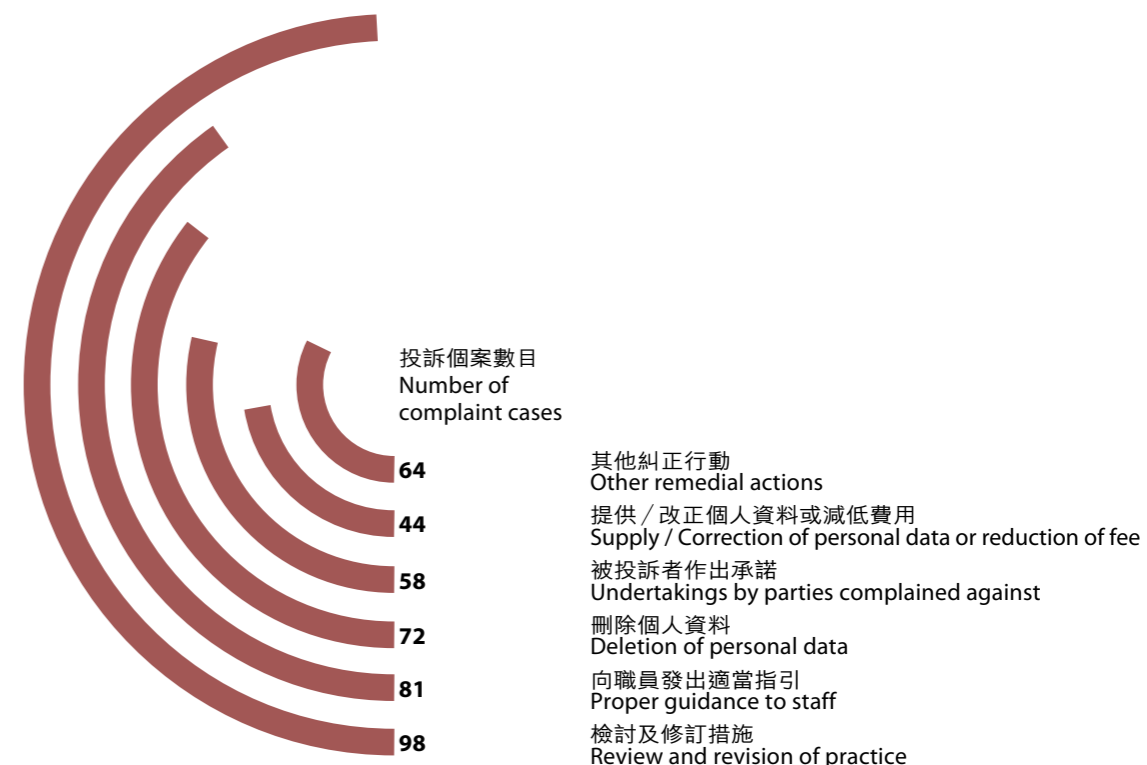
- 被投訴者修訂運作措施，以免日後再發生同類違規事件（98宗）；
- 被投訴者向有關職員發出適當指引，確保他們遵從條例規定（81宗）；
- 刪除被投訴者不必要地收集或向第三者披露的個人資料（72宗）；
- 被投訴者承諾停止被投訴的不當行為（58宗）；
- 被投訴者按投訴人的查閱／改正資料要求提供／改正個人資料，或減低依從查閱資料要求的費用（44宗）；及
- 符合投訴人期望的其他糾正行動（64宗）。

Nature of Remedial Action in Conciliated or Mediated Cases

During the report period, 285 cases were resolved through conciliation or mediation (243 during the preliminary enquiries and 42 during formal investigations), i.e. the problems raised by the complainants were remedied by the parties complained against. The remedial actions taken by the parties complained against are categorised in Figure 3.11 (N.B.: More than one type of remedial action may have been taken by the party complained against in some cases) and are summarised as follows:

- Revision of operational practices by the party complained against to prevent a similar breach in the future (98 cases);
- Proper guidance given by the party complained against to the staff concerned to ensure compliance with the Ordinance (81 cases);
- Deletion of personal data unnecessarily collected by the party complained against or disclosed to third parties (72 cases);
- Undertakings by the party complained against to cease the malpractice leading to the complaint (58 cases);
- Supply / correction of the personal data by the party complained against as per the complainants' data access / correction requests, or reduction in the fee for complying with the data access requests (44 cases); and
- Other remedial actions taken which met the complainants' expectations (64 cases).

圖 Figure 3.11 經調停或調解而解決的個案的糾正行動性質
Nature of remedial action in conciliated or mediated cases



個案研究：指導資料使用者遵守條例規定

CASE STUDY: GUIDING DATA USERS TO COMPLIANCE

個案1 — 幼稚園過度收集家長的香港身份證副本 — 保障資料第1(1)原則

投訴內容

投訴人為其子報讀一間幼稚園。該幼稚園除申請表格外，還要求投訴人提供她的香港身份證副本。投訴人質疑該幼稚園收集其香港身份證副本的目的。

該幼稚園向私隱專員解釋，香港身份證副本是用來核實遞交申請的家長或監護人與申請人（學童）的關係，以及方便該幼稚園向的家長或監護人發出「學生接送證」。

結果

鑑於香港身份證號碼屬敏感的個人資料，任何資料使用者都不應在缺乏真正需要或理據的情況下，輕率地收集香港身份證副本。

純粹為了確認申請人與家長或監護人的關係，該幼稚園可以在家長或監護人親身遞交申請或出席面試時，要求對方出示香港身份證，然後將申請人的出世紙或其他法律文件上所列的父或母或監護人的姓名進行核對。該幼稚園亦可根據核對後的結果，向學生的父母或監護人發出「學生接送證」。此外，如該幼稚園對前來接送學生的人士的身份有懷疑，該幼稚園可要求該人士出示香港身份證，然後與其紀錄進行核對。

私隱專員認為收集家長或監護人的香港身份證副本屬超乎適度，違反了保障資料第1(1)原則。

最終該幼稚園同意停止收集申請人家長或監護人的香港身份證副本，以及銷毀早前收集得的家長的香港身份證副本。

Case 1 – Excessive collection of copies of HKID Card of parents by a kindergarten – DPP1(1)

The Complaint

The Complainant applied for admission to a kindergarten for her son. Apart from the application form, the Complainant was requested to provide a copy of her HKID Card. The Complainant queried the purpose of the kindergarten to collect a copy of her HKID Card.

The kindergarten explained to the Commissioner that a copy of the Complainant's HKID Card was needed for verifying the relationship between the applicant (the student) and the Complainant who submitted the application. The copy of the Complainant's HKID Card also facilitated the kindergarten to issue the "student pick-up card" for the parent / guardian designated to pick up the student from school.

Outcome

Given that HKID Card number was a sensitive personal data, data user should not collect a copy of HKID Card lightly without genuine need or justification.

For the purpose of simply verifying the relationship between the applicant and his parent/guardian, the kindergarten could ask the parent/guardian to present his HKID Card when submitting the application in person or when attending the school interview. The kindergarten could then verify the name on the HKID Card against the names of the parents recorded on the birth certificate of the applicant or any other relevant legal document. Based on the verification result, the kindergarten might issue the "student pick-up card" accordingly. If the kindergarten doubted the identity of the person who came to pick up a student, it might ask that person to present his HKID Card and verify his name against the record.

The Commissioner was of the view that the collection of copies of HKID Card of the parents/guardians was excessive and in breach of DPP1(1).

As a result, the kindergarten agreed to stop collecting copies of HKID card of the parents/guardians, and to destroy all copies of HKID Card previously collected.

個案2 — 僱主在依從僱員的查閱資料要求時，收取超乎適度的費用 — 第28(3)條

投訴內容

投訴人向其僱主提出查閱資料要求，索取一份有關他工作表現評核報告的複本。他的僱主就四頁紙的評核報告，以劃一收費（每頁港幣50元），向投訴人收取合共200港元。投訴人認為費用超乎適度。

結果

根據行政上訴委員會上訴案件第37/2009號的決定中的原則，資料使用者只可向要求者收取跟依從查閱資料要求「直接有關及必需」的費用。資料使用者不應以商業準則收取費用。任何超出循規成本的費用，會被視為超乎適度。

四頁紙的評核報告的收費合共200港元，表面看來過高，故該機構有責任證明收取的費用，不是超乎適度。然而，該機構沒有提供釐訂劃一收費（每頁50港元）的基礎或證明200港元金額是為依從查閱資料要求的成本。

在私隱專員向該機構解釋條例第28(3)條的規定及行政上訴委員會上訴案件第37/2009號的決定中的原則後，該機構同意更改劃一收費為每頁二港元，以及向投訴人退回192港元。

Case 2 – An employer charged an excessive fee for complying with an employee's data access request – Section 28(3)

The Complaint

The Complainant made a data access request (the "DAR") to his employer for a copy of his appraisal report. His employer imposed a flat-rate fee (HK\$50 per page) on a requestor and charged the Complainant HK\$200 for an appraisal report of four pages. The Complainant considered the fee to be excessive.

Outcome

According to the principles laid down by the Administrative Appeals Board in Administrative Appeal No. 37/2009, a data user is allowed to charge a requestor only for costs which are "directly related to and necessary for" complying with a data access request. A data user should not charge a fee on a commercial basis. Any fees that exceed the costs of compliance would be considered excessive.

As the charge of HK\$200 for four pages appeared, on the face of it, to be exorbitant, the burden was on the Complainant's employer to prove that the fee of HK\$200 it had charged was not excessive. However, the Complainant's employer failed to provide details of the basis of the flat-rate (HK\$50 per page) or justify how the amount of HK\$200 was cost-related to the compliance with the DAR.

After the Commissioner had explained the requirements under 28(3) of the Ordinance and the principles laid down in Administrative Appeal No. 37/2009 to the Complainant's employer, the flat-rate of HK\$2 per page was charged instead and a total of HK\$192 was refunded to the Complainant.

個案3 —— 銀行不應於發給收款人的通知書上顯示匯款人的住址 —— 保障資料第3原則

投訴內容

投訴人指示甲銀行將一筆款項電匯至乙銀行的一個帳戶，其後發現乙銀行在發給收款人的電子通知書上顯示其姓名和住址資料。投訴人不滿乙銀行透過該電子通知書向收款人披露其住址，遂向公署作出投訴。

乙銀行向私隱專員解釋，當收到匯款機構（即甲銀行）發出的國際電匯，他們會根據業界慣例，從其中匯款人資料的一欄抽取兩行字加到電子通知書中，以提供足夠資料協助收款的客戶識別匯款人的身份。乙銀行指匯款機構一般會於該欄位的首行輸入匯款人姓名，並於第二行輸入匯款人住址。

結果

根據乙銀行提供的資料，他們在電子通知書上顯示匯款人的姓名及住址的目的，是為了提供足夠資料協助收款的客戶識別匯款人，然而乙銀行似乎並沒有考慮到，收款人可能根本不知悉付款人的住址（即本案中的情況），因此即使乙銀行在電子通知書上顯示有關資料，亦無助收款人識別匯款人，反而令匯款人的住址不必要地披露予收款人。私隱專員認為，在電子通知書上顯示付款人的姓名及戶口資料，已足以達到讓收款人識別匯款人的目的，因此，乙銀行在本案中的作為違反了保障資料第3原則。

經公署介入後，乙銀行同意修訂其電子通知書的格式，修訂後的電子通知書上只會顯示匯款人資料一欄的首行內容，以避免匯款人的住址不必要地披露予收款客戶的情況。

Case 3 – A bank should not show remitter's address on the electronic advice issued to payee – DPP3

The Complaint

The Complainant instructed Bank A to remit a sum of money by telegraphic transfer to an account at Bank B, and later found that the electronic advice issued to the payee by Bank B showed his name and address. Dissatisfied with Bank B's disclosure of his address to the payee on the electronic advice, the Complainant lodged a complaint with the PCPD.

Bank B explained that when it received an international telegraphic transfer from the remitting bank (i.e. Bank A), it would extract two lines of text from the field of remitter's information and put it into the electronic advice in accordance with the banking practices so as to provide sufficient information to the payee for identification of the remitter. According to Bank B, the remitting bank generally inputs the remitter's name in the first line of the field and the remitter's address in the second line.

Outcome

According to the information provided by Bank B, the purpose of showing the remitter's name and address on the electronic advice was to provide sufficient information to the payee for identification of the remitter. However, it seemed that Bank B had not considered the fact that the payee might not have known the remitter's address (as in this case). Therefore, the act of showing the data on the electronic advice could not help the payee to identify the remitter, but the remitter's address was unnecessarily disclosed to the payee. The Commissioner is of the view that showing the remitter's name and account data on the electronic advice is sufficient to achieve the purpose of identifying the remitter by the payee. Hence, the act of Bank B in the case had contravened DPP3.

After the PCPD's intervention, Bank B agreed to amend the format of its electronic advice, which would then only show the data in the first line of the field. Such amendment can avoid unnecessarily disclosing the remitter's address to the payee in future.

個案4 —— 物業管理公司不應未經住戶同意而向精神健康服務機構披露其個人資料，以轉介其予該機構 —— 保障資料第3原則

投訴內容

投訴人曾接受一間精神健康服務機構的上門家訪，其間同意加入該機構成為會員並使用他們的服務。該機構其後為投訴人撰寫一份關於其精神狀況的報告。由於該報告中提及她早前與鄰居之間的爭執詳情，投訴人相信有關資料是由其所住屋苑的管理公司向該機構提供。就此，投訴人向公署投訴該管理公司在未取得其同意下，向該機構披露他的個人資料。

該管理公司表示，由於投訴人曾多次與鄰居發生爭執，他們認為該機構或可介入為投訴人提供適當跟進，遂將投訴人轉介予該機構，故該機構派員到投訴人家中進行探訪。該管理公司承認在未取得投訴人的訂明同意下，轉介投訴人予該機構，並在過程中向該機構提供了投訴人的背景資料。

結果

該管理公司因為投訴人與鄰居發生爭執，便一廂情願地假設該機構可介入為投訴人提供適當跟進以改善情況，惟他們並無考慮投訴人的意願，便將其轉介予該機構，並向該機構披露其個人資料。私隱專員認為，由於向該機構作出轉介與該管理公司當初收集投訴人個人資料的目的（即為處理屋苑居民的爭執事宜）無關，而該管理公司又沒有取得投訴人的訂明同意，該管理公司的做法已違反了保障資料第3原則。

在公署介入後，該管理公司已因應本案，向員工發出書面指引及作出口頭訓示，規定員工在將住戶的個人資料轉介或發放予第三者前，必須事先取得當事人的書面同意。

Case 4 – A property management company should not refer a resident to a mental health service organisation by disclosing the resident's personal data without consent – DPP3

The Complaint

The Complainant had received a home visit from a mental health service organisation, during which he agreed to join the organisation as a member and use its services. The organisation later wrote a report on the Complainant's mental condition. As the report mentioned the details of disputes between the Complainant and his neighbour, the Complainant believed that the data was supplied to the organisation by the management company of his housing estate. Hence, the Complainant lodged a complaint with the PCPD against the management company for disclosing his personal data to the organisation without his consent.

According to the management company, as the Complainant had several disputes with his neighbour, it believed that the organisation might provide appropriate service to the Complainant. Hence, it referred the Complainant to the organisation, which then paid the Complainant a visit at his home. The management company admitted that it had, without the Complainant's prescribed consent, supplied the Complainant's background information to the organisation when making the referral.

Outcome

In view of the disputes between the Complainant and his neighbour, the management company wishfully assumed that the organisation could intervene to provide the Complainant with appropriate follow-up and hence improve the situation. However, the management company had not considered the Complainant's will before referring him and disclosing his personal data to the organisation. The Commissioner was of the view that the referral did not relate to the original purpose of collection of the Complainant's personal data by the management company (i.e. for handling disputes among residents of the housing estate), and the management company had not obtained the Complainant's prescribed consent before disclosure, thus the act of the management company violated DPP3.

After the PCPD's intervention, the management company gave written guidelines and verbal instructions to its staff, requiring them to obtain written consent from residents before transferring or releasing residents' personal data to any third party.

檢控及定罪個案

條例有關大幅修訂規管直接促銷活動機制的條文已於 2013年4月1日生效，自此更嚴格規管使用及提供個人資料作直接促銷。違反規定屬於刑事罪行，最高罰款由一萬元 (HK\$10,000) 提高至五十萬元 (HK\$500,000) 及監禁三年。若違規行為牽涉為得益而轉移個人資料供第三者作直銷之用，最高刑罰是罰款一百萬元 (HK\$1,000,000) 和監禁五年。

為深化現行轉介涉嫌違反條例的個案予警方的機制，私隱專員及警務處處長於2015年8月舉行會議。會後副私隱專員與警務處助理警務處長(支援)、助理警務處長(刑事)，以及香港警務處刑事總部、商業罪案調查科、東九龍總區刑事總部、葵青警區的高層人員會面。此外，公署亦定期舉辦與條例規定有關的講座及培訓供警務人員參與。

在本年報期間，有六宗被檢控的個案，全部涉及使用個人資料作直接促銷，其中四宗被定罪，餘下兩宗在本年報期間仍在審理中。下述個案4清楚顯示資料使用者(不論是機構或個人)均須遵守有關直接促銷條文的規定。

PROSECUTION AND CONVICTION CASES

The regulatory regime for direct marketing activities under the Ordinance has been substantially revamped and come into force on 1 April 2013. More stringent requirements are introduced in relation to the use of personal data and provision of personal data for use in direct marketing. Contravention of the requirements is a criminal offence and its maximum penalty was raised from a fine of HK\$10,000 to a fine of HK\$500,000 and imprisonment for three years. If the personal data is provided to a third party for its use in direct marketing in exchange for gain, non-compliance may result in a maximum penalty of a fine of HK\$1 million and five years' imprisonment.

In an effort to enhance the current mechanism of referring suspected offences under the Ordinance to the Police, a meeting was held between the Commissioner and the Commissioner of Police in August 2015, followed by a series of meetings between Deputy Commissioner and Assistant Commissioner of Police (Support), Assistant Commissioner of Police (Crime), senior officers of Crime Wing Police Headquarters, Commercial Crime Bureau, Kowloon East Regional Headquarters (Crime) and Kwai Tsing District. Besides, the PCPD regularly delivered lectures and training sessions on the requirements under the Ordinance to the Police officers.

In the report year, six cases, all of which related to the use of personal data in direct marketing, had been prosecuted. Four of such cases were concluded in convictions while the remaining two cases were still in progress in the report year. Case 4 below clearly shows that the direct marketing provisions are to be observed not only by organisational data users, but also by non-corporate data users.

個案1：一間電訊服務供應商沒有依從客戶的拒收直銷訊息要求

投訴內容

投訴人是一間電訊服務供應商的寬頻客戶。儘管該供應商曾確認收到投訴人書面提出的拒收直銷訊息要求，但該供應商的職員仍致電投訴人的流動電話並留言，告知他現有的服務及向他作出推廣。

結果

該供應商被裁定沒有依從投訴人的拒收直銷訊息要求，停止使用其個人資料作直接促銷，違反條例第35G(3)條的規定，被判罰款三萬元 (HK\$30,000) (註：該供應商不服判罪，已提交上訴通知書，聆訊待續)。

Case 1: A telecommunications service provider failed to comply with a customer's opt-out request

The Complaint

The Complainant was a customer of a telecommunications service provider for its broadband service. Despite this service provider's acknowledgement of the Complainant's written opt-out request, its staff still called the Complainant on his mobile number and left a voice message informing him of, amongst other things, its available services and promotions.

Outcome

The service provider was convicted, after trial, of failure to comply with the Complainant's request to cease to use his personal data in direct marketing, contrary to section 35G(3) of the Ordinance and fined HK\$30,000 (N.B.: This service provider subsequently filed a notice of appeal against its conviction, and the hearing was yet to complete).

個案2：一間儲存服務公司被裁定在使用客戶個人資料作直接促銷前沒有採取指明的行動通知客戶

投訴內容

投訴人使用公司A的儲存服務，並向公司A提供了個人資料，包括姓名、信用卡號碼、流動電話號碼、由他本人管理的公司電郵地址，以及現時的住址。其後，公司A結束在香港的業務，其業務由同樣提供儲存服務的公司B接管。

其後，公司B向投訴人傳送了一個直接促銷的電郵。在這電郵內，公司B指名道姓地稱呼投訴人，並附上新儲存服務報價及合約條款。但投訴人跟公司B從沒有任何來往，亦從未收過公司B通知會使用其個人資料作直銷用途，也未曾給予公司B其同意。

結果

公司B被控在使用投訴人的個人資料進行直銷前，未有採取指明的行動通知投訴人，違反條例第35C(2)條的規定。公司B認罪，被判罰款一萬元 (HK\$10,000)。

Case 2: A storage service company was convicted of using a customer's personal data in direct marketing without taking specified actions

The Complaint

The Complainant engaged the storage service of Company A and provided it with his personal data including his name, credit card number, mobile phone number, company email address managed by him and current residential address. Subsequently, Company A ceased its business in Hong Kong, and the business was taken over by Company B which provided similar storage service.

Thereafter, Company B sent a direct marketing email to the Complainant addressing the Complainant by his name and enclosing a storage service quotation with the terms and conditions of the service. The Complainant had no prior dealings with Company B and he had not been informed of, or given consent to Company B's use of his personal data in direct marketing.

Outcome

Company B was charged with the offence of using the personal data of the Complainant in direct marketing without taking specified actions, contrary to section 35C(2) of the Ordinance. Company B pleaded guilty to the charge and was fined HK\$10,000.

個案3：一間體檢公司被控沒有依從拒收直銷訊息要求

投訴內容

投訴人是一間體檢公司的前客戶。自2013年中，該公司多次致電投訴人，向他推銷身體檢查服務。儘管投訴人已口頭及書面向該公司作出拒收直銷訊息要求，但該公司在2014年7月繼續致電他作直銷推廣。

結果

該公司被控沒有依從投訴人的拒收直銷訊息要求，停止使用其個人資料作直接促銷，違反條例第35G(3)條的規定。該公司認罪，被判罰款一萬元(HK\$10,000)。

Case 3: A body-check service company was summonsed for failing to comply with an opt-out request

The Complaint

The Complainant was an ex-customer of a body-check service company. Since mid-2013, the company had repeatedly made direct marketing calls to the Complainant promoting its body-check services. Despite the Complainant's earlier verbal and written opt-out requests, the company continued to make direct marketing calls to him in July 2014.

Outcome

The body-check service company was charged with the offence of failing to comply with the Complainant's requests to cease to use his personal data in direct marketing under section 35G(3) of the Ordinance. The company pleaded guilty to the charge and was fined HK\$10,000.

個案4：一名個人因提供個人資料予他人作直接促銷而被判罰款

投訴內容

投訴人在一個社交場合向其校友提供英文名稱和手提電話號碼。該名校友在未有通知投訴人或取得其同意的情况下，將投訴人的英文名稱和手提電話號碼提供給另一保險代理作直銷之用。其後該保險代理致電投訴人意圖推介保險產品時，投訴人才得悉事件。

結果

該名校友被控在提供投訴人的個人資料予該保險代理作直接促銷用途前，未有採取指明行動通知投訴人，違反條例第35J(2)條的規定。該名校友辯解他早已取得投訴人的同意，惟法庭並不接納。該名校友最終被定罪，被判罰款五千元(HK\$5,000)。

這宗個案涉及一個人的資料使用者被控並被裁定違反條例的規定，也是首宗因違反條例第35J條的規定而被定罪個案(註：該名校友不服判罪，已提交上訴通知書，聆訊待續)。

Case 4: A non-corporate data user was fined for providing personal data to another for use in direct marketing

The Complaint

The Complainant's Christian name and mobile phone number were provided to his alumnus on a social occasion, and without informing or seeking his consent, the alumnus provided the Complainant's name and mobile phone number to an insurance agent for direct marketing. The case came to light when the insurance agent subsequently made calls to the Complainant with a view to promoting insurance products.

Outcome

The alumnus was charged with failing to take the specified actions under section 35J(2) of the Ordinance before so providing the Complainant's personal data to the insurance agent for direct marketing. The alumnus's defence was that he had the consent of the Complainant beforehand. His defence was not accepted by the court, and he was fined HK\$5,000 upon conviction as charged.

This is a case where a non-corporate data user was charged and convicted under the Ordinance, and it is also the first conviction under section 35J (N.B.: This alumnus subsequently filed a notice of appeal against his conviction, and the hearing was yet to complete).

投訴個案的得着

投訴個案1

美容中心過度收集客戶的個人資料——保障資料第1(1)原則

投訴內容

投訴人到一美容中心享用美容療程(包括纖型及美白)，職員先要求她填寫一份新客户表格，當中必須提供香港身份證號碼、出生日期、教育程度及職業。此外，職員要求投訴人於兩份接受該些美容療程的同意書上填寫她的香港身份證號碼。投訴人認為該美容中心不應收集她的個人資料，遂向公署作出投訴。

該美容中心解釋在新客戶表格中收集客戶的香港身份證號碼是作身份確認之用。此外，由於皮膚狀況與年齡有關，故客戶的出生日期是用作跟進客戶的皮膚進度。另外，客戶的教育程度及職業可讓前線職員更全面地了解有關客戶，並調整向客戶解釋服務的方式，以確保客戶清楚了解服務的內涵。

至於在同意書中收集客戶的香港身份證號碼一事，美容中心表示，他們的商業牌照已申報其業務性質為診所，而美容療程會因個別情況由醫生或治療師進行。若療程是由駐場醫生向客戶進行，即建立了醫生與病人關係，因而可收集有關客戶的香港身份證號碼。縱使療程由治療師進行，但由於纖型及美白美容療程為「高風險程序」，客戶亦應享有醫生與病人關係中相同的保障，故同樣屬於建立了醫生與病人關係。最後，由於可能有客戶因療程效果不理想而作出追討或申索，故有需要要求客戶在接受療程同意書中填寫香港身份證號碼，亦可避免客戶抵賴曾簽署有關同意書。

結果

私隱專員認為，為達致該美容中心跟進客戶的皮膚進度的目的而言，收集客戶的出生年份已足夠，毋須進一步收集出生月份及日期。此外，在沒有客戶的教育程度及職業的情況下，也不會影響該美容中心所提供的服務。

LESSONS LEARNT FROM COMPLAINT CASES

Complaint Case 1

Excessive collection of a customer's personal data by a beauty centre – DPP1(1)

The Complaint

The Complainant visited a beauty centre for its slimming and whitening treatments, and was required to fill in a registration form for new customers by providing her HKID Card number, date of birth, education level, and occupation. The Complainant was also requested to fill in her HKID Card number in two separate letters of consent for receiving the treatments. Dissatisfied with the beauty centre's excessive collection of her personal data, the Complainant lodged a complaint with the PCPD.

The beauty centre explained that the purpose of collecting a customer's HKID Card number in the registration form for new customers was for identity verification. Date of birth was collected for considering and providing follow-up advice and treatment for a customer's skin, which was age related. By assessing a customer's education level and occupation, the frontline staff could provide a tailor made presentation to the customer.

The beauty centre further explained that as its business nature was stated as "clinic" in the business licence and the treatments were considered as "high risk procedures" which might be carried out by doctors or therapists, depending on the circumstances, it needed to collect a customer's HKID Card number in the letters of consent for the beauty treatments. Hence, the doctor-patient relationship was established and it was justified for the beauty centre to collect the HKID Card number of its customers. Furthermore, a customer might claim against the beauty centre for any unsatisfactory treatments, and in order to prove that the content of the letters of consent was read and agreed to, it was necessary to collect the customer's HKID Card number in the letters of consent.

Outcome

The Commissioner took the view that for the purpose of follow up treatment on a customer's skin condition, collection of a customer's birth year would suffice, and the services provided by the beauty centre would not be dependent on a customer's education level and occupation.

另外，該美容中心只需於客戶填寫新客戶表格時要求她出示其他身份證明文件以核對她的身份，並檢視證件上的樣貌與現場所見的是否相符，已可達致核實身份的目的。此外，該美容中心可在向客人提供服務或療程前核對客人的電話號碼，及為客人安排特定客戶編號，去識辨客戶及作為尋找客戶紀錄的索引。

有關在同意書中收集客戶的香港身份證號碼方面，該美容中心認為它和它的治療師與它的顧客有醫生與病人的關係。但該美容中心並非按《診療所條例》註冊的診療所，而該美容中心大部分的療程均由治療師進行。明顯地，治療師的資歷不能與醫生對有關疾病及處理病人所受的訓練及他的專業評核相提並論。客戶對註冊醫生在治療前的評估、治療間的應變或治療後的跟進均較信任及具信心，亦從而建立醫生與病人關係。所以，療程若由註冊醫生負責進行才可以說得上是建立了醫生與病人關係，從而可收集有關客戶的香港身份證號碼。因此該美容中心不能在由治療師進行的療程的同意書中收集有關客戶的香港身份證號碼。

該美容中心若作為民事訴訟案件中的答辯人，它並不需要原告人（即提出索償訴訟的客戶）的香港身份證號碼以擬備答辯資料。

因此，私隱專員裁定該美容中心強制客戶必須 (i) 於填寫新客戶表格時，提供香港身份證號碼、出生日期、教育程度及職業，及 (ii) 在接受該美白療程及該纖型療程的同意書中向非由註冊醫生進行治療的客戶收集香港身份證號碼屬超乎適度。私隱專員向該美容中心發出執行通知，指示它採取措施糾正違反行為。該美容中心其後依從了行通知的指令。

Moreover, the beauty centre could verify a customer's identity by requesting her to produce any of her other identification documents for the purpose of checking the name and photo, and verify her telephone number on site. The beauty centre could also assign a unique membership number to a customer so as to identify her and locate her records before offering services or treatments to her.

The collection of HKID Card number in the letters of consent for the whitening and slimming treatments on the basis of there being a doctor-patient relationship between the customer and the beauty centre/therapist was misconceived, as the beauty centre was not a clinic registered under the Medical Clinics Ordinance. Moreover, the majority of the treatments were conducted by the therapists of the beauty centre. Certainly, the qualification of therapists was hardly comparable with the training and professional assessment that doctors received, and customers would have trust and confidence in registered doctors' pre-treatment evaluation, adaptability during treatment or post-treatment follow-up which created the doctor-patient relationship. Hence, HKID Card numbers in the letter of consent could only be collected for the treatments provided by registered doctors and not for the treatments provided by therapists.

In civil actions, the beauty centre as the respondent would not be required to submit the HKID Card number of the plaintiff (i.e. customer who brought the claim action) when preparing its statement of defence.

The Commissioner considered that it was excessive for the beauty centre to compulsorily require customers to (i) provide the HKID Card number, date of birth, education level and occupation in the registration form for new customers and (ii) provide the HKID Card in the letters of consent for the whitening and slimming treatments carried out by persons other than registered doctors. An enforcement notice was served on the beauty centre directing it to take remedial actions. The beauty centre subsequently complied with the enforcement notice.

投訴個案 2

醫生不必要地收集病人的香港身份證副本 —— 保障資料第 1(1) 原則

投訴內容

投訴人在一名醫生診症期間質疑他的診斷結果，令該名醫生非常憤怒。因此，該名醫生揚言要控告投訴人誹謗，並即場要求影印投訴人的香港身份證，否則不讓她離開診所。投訴人拒絕該名醫生的要求，並報警求助。投訴人最終沒有讓該名醫生影印她的香港身份證。投訴人在離開診所後，向公署投訴該名醫生。

結果

私隱專員發出的《身份證號碼及其他身份代號實務守則》（下稱「實務守則」）第 3.1 段訂明，除獲法律授權外，資料使用者不能強制要求任何個人提供香港身份證副本。實務守則第 3.2 段訂明，除了在該段所述的情況外，資料使用者不應收集香港身份證副本。

該名醫生在調查過程中，沒有提供理據顯示其在診症後要求影印投訴人的香港身份證的做法是符合實務守則的規定，亦沒有解釋他會將投訴人的香港身份證副本作甚麼用途。事實上，投訴人在該名醫生為她診症前已向診所姑娘出示了她的香港身份證作登記，而該名醫生一早已收集了投訴人的姓名、聯絡資料及香港身份證號碼。

雖然根據實務守則，該名醫生可為了確能正確找出病人過去的醫療紀錄而收集病人的香港身份證號碼，但該名醫生沒有必要收集病人的香港身份證副本。要不是投訴人拒絕，該名醫生便會在他的權威下收集了投訴人的香港身份證副本。如此收集香港身份證副本屬違反保障資料第 1(1) 原則。因此，私隱專員向該名醫生送達執行通知，指令他停止收集病人的香港身份證副本，除非是在實務守則所述的情況下收集。該名醫生其後依從了執行通知的指令。

Complaint Case 2

Unnecessary collection of a patient's Hong Kong Identity Card copy by a doctor – DPP1(1)

The Complaint

The Complainant doubted a doctor's medical advice during a medical consultation and consequently angered the doctor. In response, the doctor threatened to sue the Complainant for slander and demanded her to produce her HKID Card for copying in the clinic. The Complainant was not allowed to leave the clinic as she refused the doctor's request. Eventually, the Complainant called the Police for assistance and left the clinic without producing her HKID Card to the doctor. After leaving the clinic, the Complainant reported the case to the PCPD.

Outcome

Paragraph 3.1 of the "Code of Practice on the Identity Card Number and other Personal Identifiers" (the "Code") issued by the Commissioner stipulates that unless authorised by law, no data user may compulsorily require an individual to furnish a copy of his HKID Card. Paragraph 3.2 of the Code stipulates that a data user should not collect a HKID Card copy except in the circumstances set out therein.

In response to the investigation, the doctor had neither justified his request for copying the Complainant's HKID Card after the consultation by reference to the relevant requirements under the Code nor explained his purpose for the use of the HKID Card copy. In fact, the Complainant had already produced her HKID Card to the nurse for registration before the consultation, and her name, contact information and HKID Card number had previously been collected by the doctor.

While the collection of a patient's HKID Card number is permitted under the Code to ensure that the correct medical record is referred to when treating the patient, the collection of a patient's HKID Card copy by the doctor is not necessary. But for the Complainant's refusal, the doctor would have collected the Complainant's HKID Card copy in a position of authority. Such collection would be a contravention of DPP1(1). Therefore, the Commissioner served an enforcement notice on the doctor directing him to stop collecting any patient's HKID Card copy except in the circumstances set out in the Code. The doctor subsequently complied with the enforcement notice.

投訴個案 3

一名病人已要求醫院將其病情絕對保密的情況下，醫院仍不慎向病人的母親透露其病情——保障資料第4原則

投訴內容

投訴人在一間醫院確診感染嚴重疾病後，曾要求該醫院向其家人保密病情，院方同意此要求並記錄在其病歷牌板上。惟該醫院的護士其後仍致電投訴人的母親向她透露了投訴人的病情。

該醫院解釋事件源於投訴人須被轉介至另一醫院的專科病房，當時負責的護士欲根據投訴人的病歷牌板上的資料致電該專科病房安排轉院，惟該護士不慎撥打了寫在該牌板另一頁的緊急聯絡電話號碼（即投訴人母親的電話號碼），並在未有確認接聽電話者是否另一醫院職員的情況下向接聽人士（即投訴人的母親）透露了投訴人的病情。

結果

病人的病歷資料屬高度敏感的個人資料，處理時必須加倍小心謹慎。基於該醫院在本案中未有採取所有切實可行的步驟，以確保病人的個人資料受保障而不會受未獲准許的或意外的使用所影響，私隱專員裁定該醫院違反了保障資料第4原則的規定。

在調查的過程中，該醫院已向有關護士發出警告，並透過發出書面通告要求所有醫護人員日後在需要透過電話披露病人的病歷資料前，必須清楚核對電話號碼是否正確，及在確認對方的身份後才說出病人的病歷資料。私隱專員向該醫院發出警告，促請他們必須將上述要求向員工清楚傳達，並採取切實可行的措施確保員工依從有關要求，藉此促進員工緊遵條例下保障個人資料的規定。

Complaint Case 3

A hospital mistakenly disclosed the medical condition of a patient to the patient's mother though it had been requested to keep it confidential – DPP4

The Complaint

After having been diagnosed with serious illness, the Complainant requested the hospital to keep his illness confidential. The hospital acceded to the request and recorded it on his chart board. However, the hospital's nurse still called the Complainant's mother and disclosed his medical condition to her.

The hospital explained that the complaint stemmed from the necessity of transferring the Complainant to the Specialty Ward of another hospital. The nurse-in-charge intended to call the Specialty Ward for arranging the transfer according to the data on the Complainant's chart board. However, the nurse mistakenly dialled the emergency contact number (i.e. the telephone number of the Complainant's mother) on another page of the chart board and disclosed the Complainant's illness to the call receiver (i.e. the Complainant's mother) without first confirming that the receiver was a medical staff member of the Specialty Ward.

Outcome

Patients' medical records are highly sensitive personal data and must be handled with extra care. As the hospital in this case had not taken all the practicable steps to ensure that its patient's personal data was protected against unauthorised or accidental use, the Commissioner held that the hospital had contravened DPP4.

In the course of investigation, the hospital had given a warning to the nurse and issued a written notice to all medical staff requiring them to check the correctness of the telephone numbers of the receivers and confirm the receivers' identities before disclosing patients' medical records over the phone in future. The Commissioner issued a warning to the hospital urging it to clearly communicate the above requirements to its staff, and take practicable steps to ensure staff compliance so as to enhance staff's compliance with the personal data protection under the Ordinance.

投訴個案 4

電訊公司在商業客戶補領流動電話卡時，不必要地收集客戶代表的香港身份證副本——保障資料第1(1)原則

投訴內容

投訴人獲其僱主授權前往一間電訊公司的門市申請補領其僱主登記的流動電話卡。過程中，雖然投訴人已出示其僱主的商業登記證及公司印章，但該電訊公司仍要求掃描投訴人的香港身份證作記錄。投訴人認為該電訊公司涉及過度收集他的個人資料，遂向公署作出投訴。

該電訊公司向私隱專員解釋，根據公司的既定程序，若商業客戶要求補領流動電話卡，他們除了收集公司的商業登記證副本及公司印章外，還會收集公司代表的香港身份證副本，從而確認該名代表的身份，以防止有人冒認商業客戶取得流動電話卡。

結果

就確認商業客戶的代表是否獲合法授權方面，私隱專員認為該電訊公司應要求該名代表提供一份由商業客戶發出的授權書，當中載有該名代表的姓名；同時，為核實該名代表的身份，該電訊公司只需要他即場出示載有其相片的身份證明文件（例如香港身份證或職員證），以確認其容貌與其身份證明文件上的相符，及其身份證明文件上所顯示的姓名與授權書上的一致。如該電訊公司對該名代表的身份仍存疑，應直接聯絡商業客戶的負責人尋求澄清。

因此，私隱專員認為，該電訊公司在個案中收集商業客戶代表的香港身份證副本，屬超乎適度，違反了保障資料第1(1)原則的規定。

經公署介入後，該電訊公司已採取了多項補救措施，包括停止在辦理補領流動電話卡的過程中收集商業客戶代表的香港身份證號碼或副本，並將有關安排告知其前線職員；及銷毀過往收集得的商業客戶代表的香港身份證資料。

Complaint Case 4

Unnecessary collection of HKID Card copy of a corporate customer's representative by a telecommunications company when the customer applied for replacement of a mobile SIM card – DPP1(1)

The Complaint

The Complainant was authorised by his employer to apply for replacement of his employer's mobile SIM card at a branch of a telecommunications company. Although the Complainant had produced his employer's business registration certificate and company chop, the telecommunications company demanded to scan the Complainant's HKID Card for record. Considering that the telecommunications company had collected excessive personal data from him, the Complainant lodged a complaint with the PCPD.

The telecommunications company explained that according to its established practices, when a corporate customer applied for replacement of a mobile SIM card, it would collect a copy of HKID Card of the corporate customer's representative, in addition to the business registration certificate and company chop. The representative's HKID Card copy was collected for identity verification to prevent the SIM card from being obtained by someone impersonating the corporate customer.

Outcome

With respect to ascertaining if a corporate customer's representative is legally authorised by the corporate customer, the Commissioner was of the view that the telecommunications company should request the representative to provide an authorisation letter containing the representative's name issued by the corporate customer. To verify the representative's identity, the telecommunications company could request the representative to produce an identification document with photo (e.g. HKID Card or staff card) on-site to match it with the representative's appearance and name on the authorisation letter. If the telecommunications company still had doubt about the representative's identity, it could contact the person-in-charge of the corporate customer direct for clarification.

Hence, the Commissioner was of the view that the telecommunications company's collection of the HKID Card copy of the corporate customer's representative was excessive and contravened DPP1(1).

After PCPD's intervention, the telecommunications company took various remedial measures, which included ceasing collecting HKID Card number, or copy, of a corporate customer's representative when handling replacement of a mobile SIM card; notifying its frontline staff of the said arrangement; and destroying HKID Card data of corporate customers' representatives previously collected.

根據第 48(2) 條發表的調查報告

調查報告：僱主超乎適度及不公平收集員工指紋資料

私隱專員對一間時裝貿易公司展開正式調查，以確定該公司為達致保安及考勤的目的而收集員工的指紋資料，是否必須和公平。

調查源自該公司一名前僱員的投訴。該公司在該名僱員履新的第一天，透過指紋識別裝置收集了她的指紋資料。該公司的僱員必須將手指放在指紋識別裝置上，才能進入辦公室及陳列室，或記錄每天上班及下班的時間。

該名僱員不願意提供指紋資料，曾要求該公司採用其他方法以代替收集她的指紋資料，但不得要領。在別無選擇的情況下，該名僱員唯有讓該公司收集她的指紋資料。

調查結果

收集屬超乎適度 —— 保障資料第 1(1) 原則

該公司認為，由於其陳列室及辦公室均存放了價值不菲的時裝貨品，加上以往曾經發生數宗失竊事件，故有必要使用指紋識別裝置來加強保安。

公署的調查顯示，該公司已採用了多項的保安措施，包括閉路電視鏡頭、密碼鎖、門鎖及鏈鎖。故此，再安裝指紋識別裝置作為夜間的保安措施，實屬多此一舉。

PUBLICATION OF INVESTIGATION REPORT UNDER SECTION 48(2)

Investigation Report: Excessive and Unfair Collection of Employees' Fingerprint Data by Employer

The Commissioner initiated a formal investigation against a fashion trading company (the "Company") to ascertain whether the collection of employees' fingerprint data, for the purposes of safeguarding office security and monitoring staff attendance, was necessary and fair.

The investigation stemmed from a complaint lodged by an ex-employee of the Company. The Company collected the ex-employee's fingerprint data through a fingerprint recognition device on her first day of work. To access the office and the showroom, or to take attendance for work, employees were required to place their fingers on the fingerprint recognition devices.

The ex-employee was reluctant to provide her fingerprint data, and requested the Company to provide other alternatives in lieu of collecting her fingerprint data, but her request was ignored. Left with no alternative, the ex-employee let the Company collect her fingerprint data.

Findings of the Investigation

Excessive Collection – DPP1(1)

The Company argued that the fingerprint recognition devices were necessary for enhancing its security because its fashion items stored in the showroom and the office were of high value, and it had experienced several theft incidents.

The PCPD's investigation revealed that the Company had already installed several security devices to safeguard its property, including CCTV cameras, digital locks, ordinary door locks and a chain lock, and these measures rendered the fingerprint recognition devices redundant as a night – time security device.



該公司以往的失竊事件全部在日間發生，而犯案者全是該公司的員工及顧客。就此，安裝指紋識別裝置以防止外人擅自進入，亦不能防止此類失竊事件發生。該公司是透過閉路電視攝錄得的影像去追查這些失竊事件，並從中成功認出犯案者。從這些事實看來，閉路電視鏡頭是更有效的保安方法。

至於記錄員工出勤方面，該公司只有 20 名員工，故相對地較容易採納對私隱侵犯程度較低的做法來進行考勤，例如可讓僱員利用密碼或智能卡來記錄出勤，而不必使用指紋資料。

收集手法屬不公平 —— 保障資料第 1(2) 原則

該公司沒有讓僱員選擇以其他方法代替提供指紋資料，以達致保安及考勤的目的。該公司亦沒有告知僱員就提供指紋資料對其私隱的影響，以及該公司採取了甚麼措施防止資料被濫用或不當處理。在本案的情況下，即使僱員同意向該公司提供指紋資料，有關的同意也不是在自願及知情的情況下作出的。

因此，私隱專員認為該公司收集僱員的指紋資料違反了保障資料第 1(1) 原則及第 1(2) 原則。

執行通知及建議

私隱專員向該公司送達執行通知，指令它銷毀從前僱員及現職僱員收集得來的指紋資料，並停止向僱員收集指紋資料。該公司其後向私隱專員確認已經依從執行通知的要求。

確立使用指紋識別裝置指引

社會不應因指紋識別裝置的普及應用，而對保障個人資料私隱作出妥協。該公司為方便採用指紋識別裝置，卻忽略潛在的私隱問題，正是當中活靈活現的例子。本案說明盲目尊崇科技，而沒有深究及評估衍生的私隱風險，私隱權便成為科技的犧牲品。我們追求卓越科技無可厚非，但我們不應接受以不負責任的態度使用科技。

On the other hand, the theft incidents experienced by the Company were day-time thefts, all committed by its staff and customers, and as such, the installation of the fingerprint recognition devices to prevent unauthorised entry would not help prevent these thefts. The existing CCTV cameras, which in fact detected the thefts and identified the culprits concerned, appeared to be a more effective security means.

As for monitoring staff attendance, the Company had only 20 employees, it would be relatively easy to monitor staff attendance using less privacy intrusive means, such as password or a smartcard, instead of the use of a fingerprint recognition device.

Unfair Collection – DPP1(2)

The employees were neither provided with a choice to opt for other alternatives to satisfy the purposes of safeguarding the office security and monitoring staff attendance, nor informed of the privacy risks involved and the measures to prevent wrongful collection and misuse. In the circumstances, even the employees consented that the Company could collect their fingerprint data, the consent was not a genuine and informed consent.

The Commissioner therefore found the Company in contravention of DPP1(1) and DPP1(2) on the collection of employee's fingerprint data.

Enforcement Notice and Advice

An enforcement notice was served on the Company directing it to destroy all fingerprint data collected from its present and past employees, and to cease collecting its employees' fingerprint data. The Company had confirmed its compliance with the enforcement notice.

Establishing Guidelines for Use of Fingerprint Recognition Devices

As the use of fingerprint recognition device becomes increasingly common, it is imperative that privacy and data protection are not compromised. The case is a vivid example of a data user preferring the convenience and affordability of such devices to the neglect of the underlying privacy concerns. It illustrates the modern flow of sacrificing privacy rights at the altar of technology without understanding and assessing the privacy risks which technology can generate. Technology is certainly to be used but irresponsible use of technology must be discouraged.

指紋是與生俱來的獨特生理特徵，它是一種無可置疑的身份標識符，而且終生不變。正因指紋具有獨特及不變的性質，指紋資料是高度敏感的個人資料，故指紋資料僅限在有足夠理據的情況下收集，並須加以適當行政措施及技術加強保障，以避免未獲准許的存取或使用。

機構必須確定他們具有實際需要，而又沒有其他替代方法可達至相同目的及減低侵犯私隱的程度，才應考慮收集指紋資料。指紋識別裝置不應只因在市面上輕易購得、方便使用及價格便宜而被隨意採用。指紋識別裝置在需要高度保安的地方或許是一個合適的選擇，但純粹記錄員工出勤而言，採用指紋識別裝置的必要性則往往是令人質疑。

僱主在收集僱員的指紋資料時，須要緊記他們和僱員之間的談判實力並不均等，故不應該施加不適當的影響或威脅以獲得員工的同意，因為這種行為無異於不公平收集僱員的個人資料。僱員必須獲告之收集及使用指紋資料的私隱風險，並在清晰及自願的情況下，同意提供指紋資料。

調查報告：
www.pcpd.org.hk/tc_chi/enforcement/commissioners_findings/investigation_reports/files/R15_2308_c.pdf

Given the highly sensitive nature of fingerprint data, i.e., it is a unique physiological trait which an individual was born with and can irrefutably identify an individual, and it remains unchanged throughout the individual's lifetime, etc., fingerprint data should be collected only when justified, and used with appropriate procedural and technological safeguards to prevent unauthorised access to and use of the data.

An organisation must satisfy itself that fingerprint collection is necessary to meet a specific need and there is no other less privacy-intrusive means which could be equally effective to serve the same need. A fingerprint recognition device should not be used simply because it is readily available, convenient and cost-effective. It may be an appropriate tool to control entry to high security areas but to apply it merely for checking staff attendance is questionable.

An employer should not exert undue influence or threaten its employees when seeking to gain the latter's consent to collect their fingerprint data, as such conduct would amount to unfair collection of personal data, bearing in mind the disparity in bargaining power between an employer and his employees. The employees' consent must be genuine, unambiguous, and informed of the privacy risks associated with the collection and use of fingerprint data.

Investigation Report:
www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R15_2308_e.pdf

電子健康紀錄互通系統

《電子健康紀錄互通系統條例》(第625章)已於2015年12月2日生效，在參與電子健康紀錄互通系統(「互通系統」)的病人同意下，獲授權的公私營界別醫護提供者可取覽和互通病人的健康資料，作醫護相關用途。

互通系統內的電子健康紀錄屬《個人資料(私隱)條例》下的個人資料。為確保病人在互通系統的個人資料獲得適當保障，公署在2007年互通系統條例的立法階段初期，已參與政府就互通系統而成立的法律、私隱及保安問題工作小組，並於條例草案的審議階段就當中引起個人資料私隱關注的事宜提出意見及建議。

私隱專員就互通系統中的個人資料可執行和行使其在《個人資料(私隱)條例》下的職能和權力包括：

- 處理有關互通系統中涉及違反《個人資料(私隱)條例》的投訴，有需要時亦可展開主動調查；
- 就互通系統在處理個人資料方面進行視察；
- 就互通系統涉及個人資料私隱的事宜向市民及醫護提供者提供指引；及
- 處理涉及互通系統的資料外洩事故通報。

ELECTRONIC HEALTH RECORD SHARING SYSTEM

The Electronic Health Record Sharing System Ordinance (Cap 625) came into operation on 2 December 2015. With the consent of the patient, healthcare providers (in both the public and private sectors) can have access to and share the patient's health record in the Electronic Health Record Sharing System (the "eHR Sharing System") for healthcare-related purposes.

Electronic health record ("eHR") in the eHR Sharing System amounts to personal data under the Personal Data (Privacy) Ordinance. To ensure that a patient's personal data will be duly protected under the eHR Sharing System, the PCPD had participated in the government's Working Group on Legal, Privacy and Security Issues of the eHR Sharing System since the early stage of the legislative process of the eHR Sharing System in 2007. The PCPD also rendered comments and suggestions on issues related to personal data privacy at the Committee Stage of the Bill.

The functions and powers of the Commissioner under the Personal Data (Privacy) Ordinance in relation to personal data in the eHR Sharing System include:

- handling complaints of suspected breaches of the Personal Data (Privacy) Ordinance and initiating investigation if necessary;
- carrying out an inspection of the eHR Sharing System;
- providing guidance on personal data privacy in relation to the eHR Sharing System to citizens and healthcare providers; and
- handling any data breach notification in relation to the eHR Sharing System.

回響 Feedback

- 此外，個人資料私隱專員也提出了很多意見，多次出席會議並回答(《電子健康紀錄互通系統條例草案》委員會)委員的問題，對於我們的工作有很大的幫助，我亦想特別感謝他和他的同事。

法案委員會曾有一次因不夠法定人數而流會，但個人資料私隱專員也很大方與部分出席會議或遲到的委員，在咖啡閣中聯同政府官員照樣開了兩個多小時的會議……對我們的工作也相當有幫助。

The Privacy Commissioner also offered a lot of advice and attended meetings on a number of occasions to answer members' (of the Bills Committee on the Electronic Health Record Sharing System Bill) questions. This is very helpful to our work, so I also wish to thank him and his colleagues in particular.

On one occasion, a meeting of the Bills Committee was aborted due to a lack of quorum but the Privacy Commissioner was still very generous to hold a meeting with some of the members who were present or who were late in the café for more than two hours... it was quite helpful to our work.

莫乃光議員, JP
The Hon Charles Peter MOK, JP



2015年12月18日舉行了其中一場簡介會，讓公署職員深入了解互通系統。

One of the briefings was held on 18 December 2015 to explain the eHR Sharing System to the PCPD staff members.

為配合互通系統於2016年3月正式啟用，公署自2015-16年度第二季開始已著手進行一系列的籌備工作。除繼續就互通系統涉及個人資料私隱的事宜向政府提供意見外，公署亦與食物及衛生局轄下的電子健康紀錄統籌處緊密聯繫，就日後處理涉及互通系統的投訴設立雙向轉介機制。公署在邀請電子健康紀錄統籌處及醫院管理局的代表為公署職員主持簡介會的同時，亦與電子健康紀錄統籌處的人員分享其處理醫護界投訴個案的經驗。此外，公署於2016年初就保障互通系統中的個人資料私隱方面出版了兩份單張，分別供醫護接受者及醫護提供者參考*。

To prepare for the commencement of operation of the eHR Sharing System in March 2016, the PCPD undertook a series of preparatory work since the second quarter of 2015-16. Apart from continuing to render comments on personal data privacy-related issues in relation to the eHR Sharing System to the government, the PCPD had worked closely with the eHR Office under the Food and Health Bureau to set up a two-way referral mechanism in handling possible eHR-related complaints. Representatives from the eHR Office and Hospital Authority were invited to conduct briefing sessions for staff of the PCPD while the PCPD was also invited to share its experience with the eHR Office in handling complaints relating to the medical sector. Two sets of information leaflets on protection of personal data privacy in relation to the eHR Sharing System were published in early 2016 for the reference of the healthcare recipients and the healthcare providers respectively*.

* 詳情請參閱：
www.pcpd.org.hk/tc_chi/data_privacy_law/
electronic_health_record_sharing_system/ehrss.html

* The information leaflets can be downloaded at
www.pcpd.org.hk/english/data_privacy_law/electronic_health_record_
sharing_system/ehrss.html

回響 Feedback

- 最後，我想再次感謝私隱專員——他與他的同事相當有心，向我們提供了很多意見……我認為私隱專員在這情況下絕對是有很重要的角色，從保障市民私隱的角度看看怎樣做才可以符合有關私隱的條例或其他條例，令香港市民在這制度下得到充分保障。

Lastly, I wish to once again express my gratitude to the Privacy Commissioner – He and his colleagues are most sincere and have provided a lot of views to us…… But I think the Privacy Commissioner absolutely plays a most crucial role in looking into what measures should be taken to ensure compliance with the legislation on privacy or other legislation from the angle of privacy protection, in order for Hong Kong people to be provided with full protection under this system.

劉慧卿議員, JP
The Hon Emily LAU Wai-hing, JP

回響 Feedback

- 個人資料私隱專員亦就條例草案盡了很大努力，提出了很多疑點，而當局亦就着這些建議和疑點作出修訂，我們對此表示支持。

The Privacy Commissioner for Personal Data has also made great efforts regarding the Bill by raising a lot of points of doubt, and the authorities have made amendments in the light of these suggestions and points of doubt. We support all of these.

張超雄議員
The Hon Fernando CHEUNG Chiu-hung

回響 Feedback

- 個人資料私隱專員公署的代表亦有積極參與工作小組的討論，其大部分的建議也已獲接納。

The representative of the Office of the Privacy Commissioner for Personal Data has also taken an active role in the discussion of the Working Group and most of his recommendations were taken on board.

食物及衛生局局長高永文議員, BBS, JP
Dr the HON KO Wing-man, BBS, JP