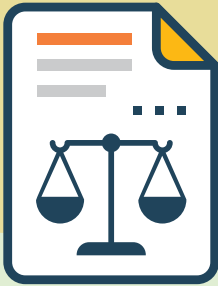
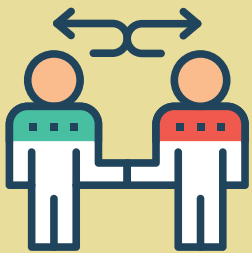


ENFORCING DATA PROTECTION

執法保障資料





調查不偏不倚

對於市民的投訴及查詢，公署具效率、公平公正地調查及排解。若發現有重大私隱風險的情況存在，我們主動作出調查。

THOROUGH AND IMPARTIAL INVESTIGATIONS

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



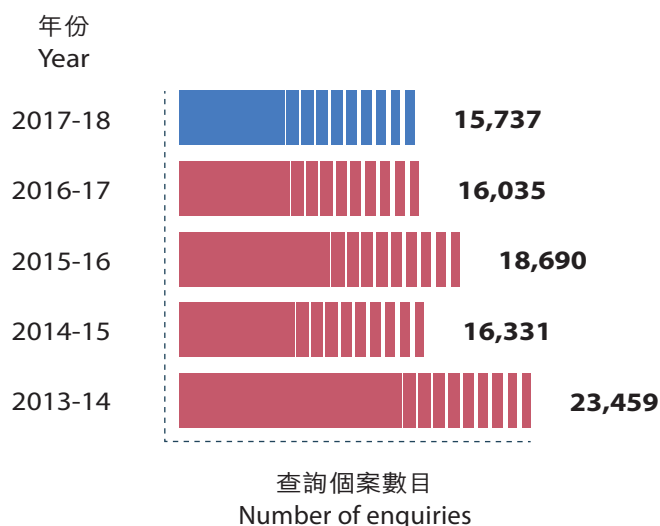
處理查詢

公署在報告年度共接獲 15,737 宗*查詢個案，較 2016/17 年度的 16,035 宗下跌 1.9%，平均每個工作天處理 64 宗查詢。大部分查詢 (82.7%) 經由公署的查詢熱線 (2827 2827) 及本年度起設立的中小型企業的專屬諮詢熱線 (2110 1155) 提出。

主要的查詢性質方面，30.5% 是關於收集 / 使用個人資料 (例如香港身份證號碼及副本)、10.6% 是與僱傭事宜相關；7% 是關於直接促銷活動。與使用互聯網有關的查詢由 2016/17 年度的 1,016 宗上升 4.9% 至 1,066 宗，主要涉及網絡起底、流動應用程式及網絡欺凌。

查詢數字減少的原因之一，相信和公署不斷透過推廣和教育工作，加強大眾對個人資料私隱保障的意識有關。公署出版各類指引，適時發出新聞稿及傳媒回應，又持續更新和優化其網站，令公眾能夠及早了解及掌握有關議題和知識。

圖 5.1 — 查詢個案數目



* 同一宗查詢可能涉及多項性質。
An enquiry may cut across different categories.

HANDLING ENQUIRIES

During the reporting year, the PCPD received a total of 15,737 enquiries*, 1.9% less than the 16,035 enquiries received in 2016/17. On average, 64 enquiries were handled per working day. The majority of the enquiries (82.7%) were made through the PCPD hotline (2827 2827) and the newly-launched dedicated hotline for SME (2110 1155).

The enquiries were mainly related to the collection and use of personal data (e.g. Hong Kong Identity Card numbers or copies) (30.5%), employment (10.6%), and use of personal data in direct marketing (7%). There was an increase of 4.9% in Internet-related enquiries, from 1,016 cases in 2016/17 to 1,066 cases in the reporting year. They mainly concerned cyber-profiling, mobile apps and cyber-bullying.

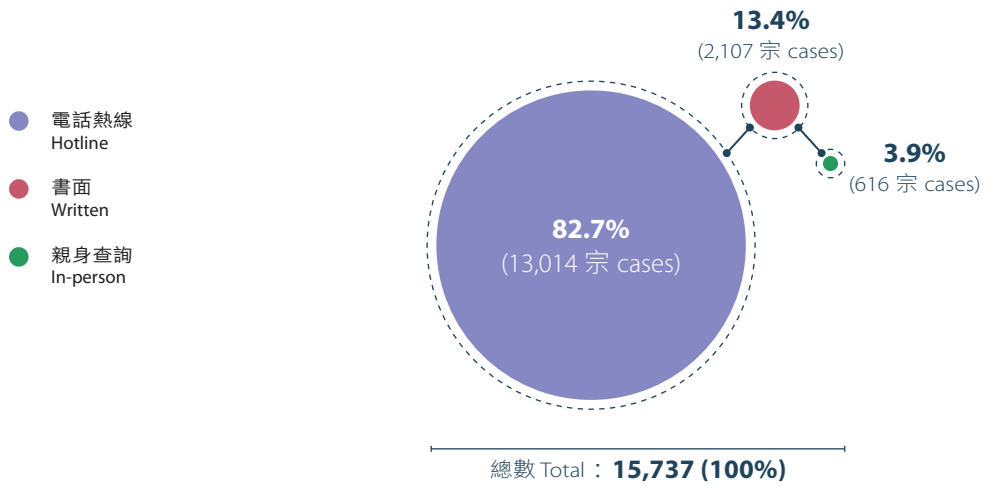
The drop in the number of enquiries received could be attributed to the heightened public awareness of personal data protection resulting from the PCPD's promotion and education. Those efforts included publishing various guidelines and releasing media statements and responses to timely address public concerns, as well as updating and revamping our website to make personal data privacy knowledge more readily accessible.

Figure 5.1 — Number of enquiries received

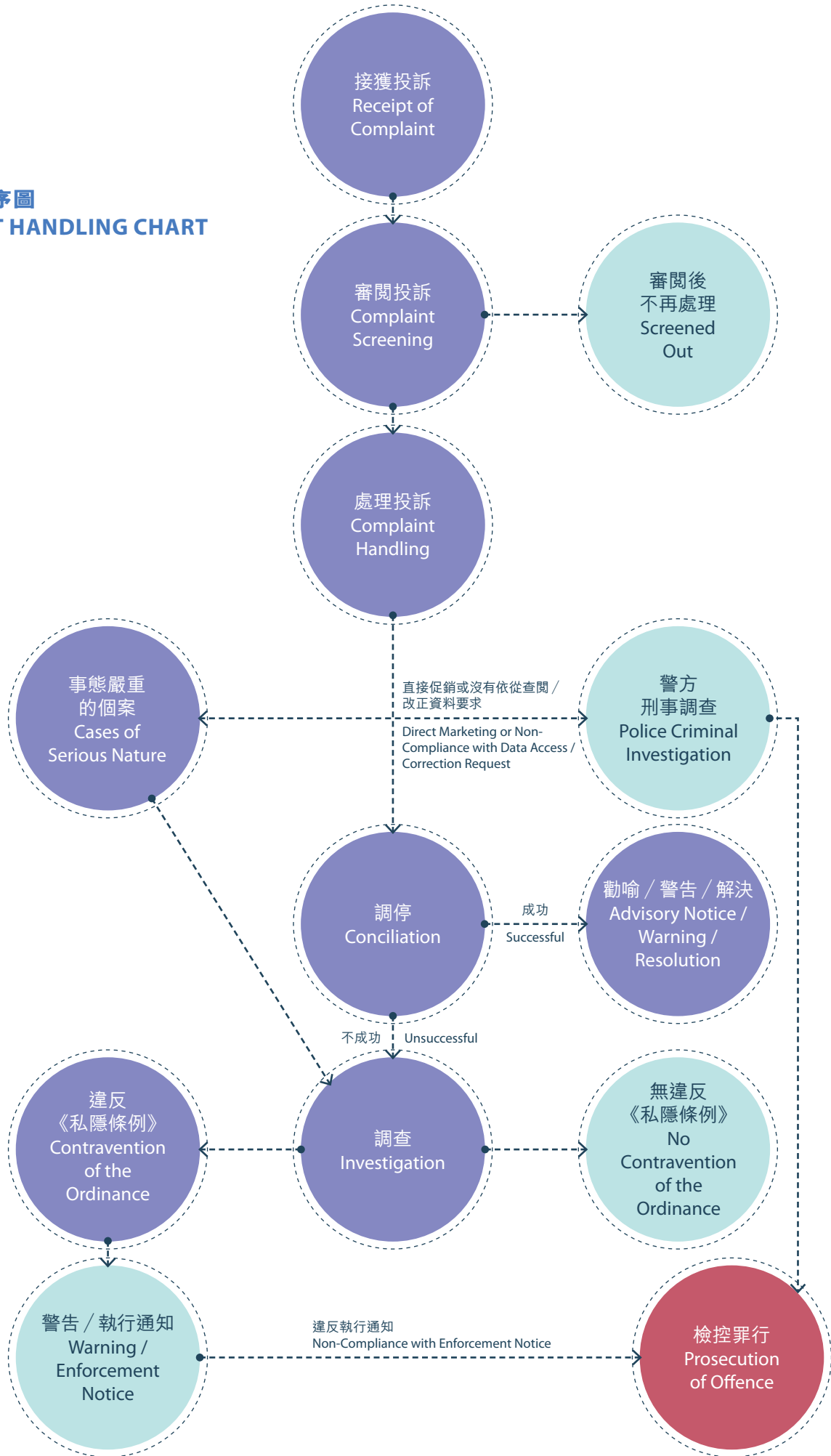


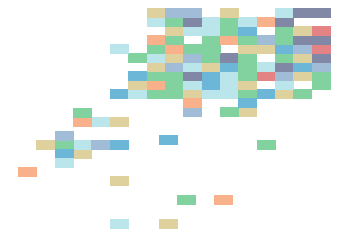
圖 5.2 — 提出查詢的途徑

Figure 5.2 — Means by which enquiries were made



處理投訴程序圖
COMPLAINT HANDLING CHART





調查投訴

接獲的投訴個案

公署在本報告年度共接獲 1,619 宗* 有關個人資料私隱的投訴，比上年度減少了 7%。(圖 5.3)

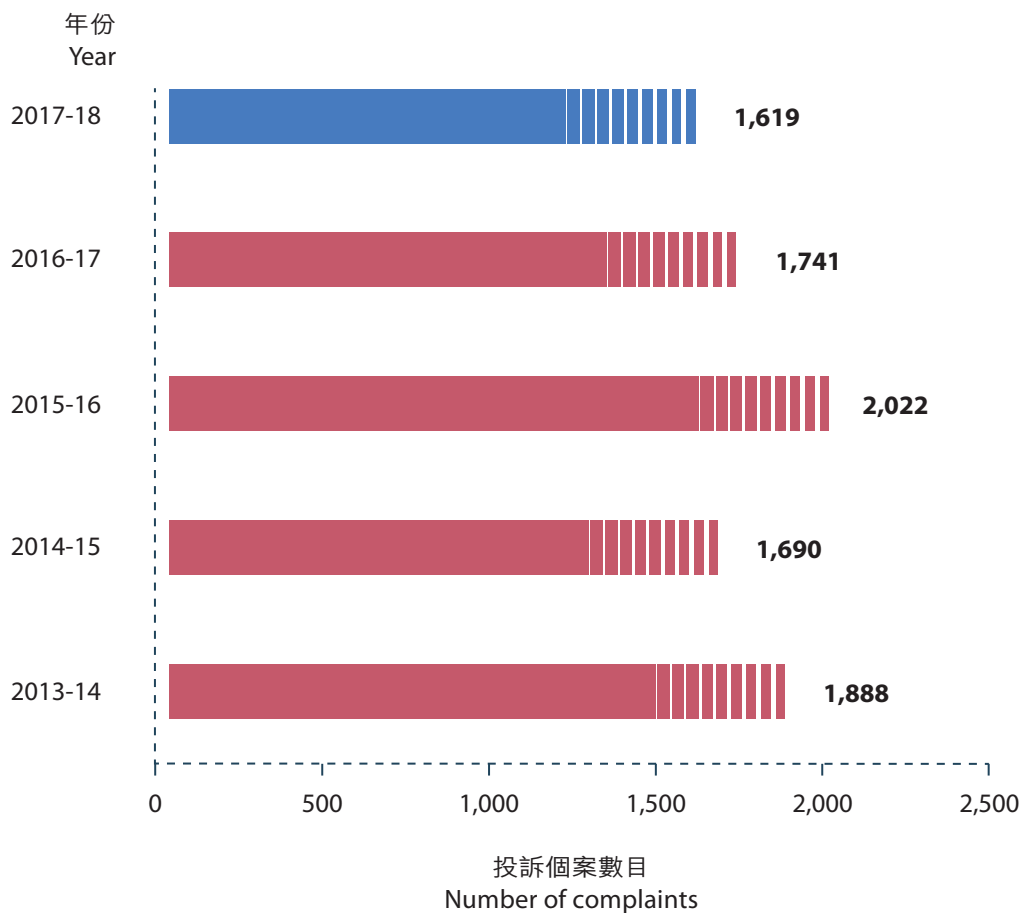
圖 5.3 — 投訴個案數目

COMPLAINTS INVESTIGATION

Data privacy complaints received

1,619 complaints* were received in 2017-18, being a 7% decrease from last year. (Figure 5.3)

Figure 5.3 — Number of complaints received



* 為統計目的，公署在本報告年度收到有關選舉事務處遺失載有選民個人資料的手提電腦的 1,944 宗同類投訴，只作 1 宗投訴計算。

For statistical purpose, the 1,944 complaints received in relation to the suspected theft of computers of the Registration and Electoral Office that contained personal data of registered electors were counted as 1 complaint.

被投訴者類別

在接獲的 1,619 宗投訴個案中，被投訴者可分為以下類別：

- 私營機構 (1,022 宗)，主要涉及：銀行及財務公司、物業管理公司及業主立案法團，以及電訊公司；
- 個人 (280 宗)；及
- 政府部門及公共機構 (317 宗)，主要涉及：醫院或醫療機構、警務處，以及房屋管理機構。(圖 5.4)

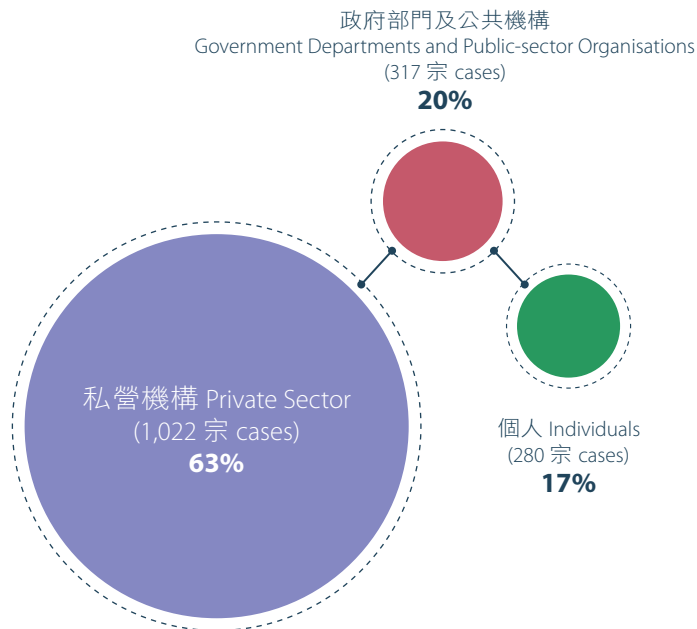
圖 5.4 — 被投訴者類別

Types of parties being complained against

Among the 1,619 complaints received, the types of parties being complained against are as follows:

- private-sector organisations (1,022 cases), with the majority including banking and finance institutions, property management companies and owners' corporations, and telecommunications companies;
- individuals (280 cases); and
- government departments and public-sector organisations (317 cases), with the majority including healthcare services institutions, the Hong Kong Police Force and housing organisations. (Figure 5.4)

Figure 5.4 — Types of parties being complained against





就違反《私隱條例》的投訴指稱

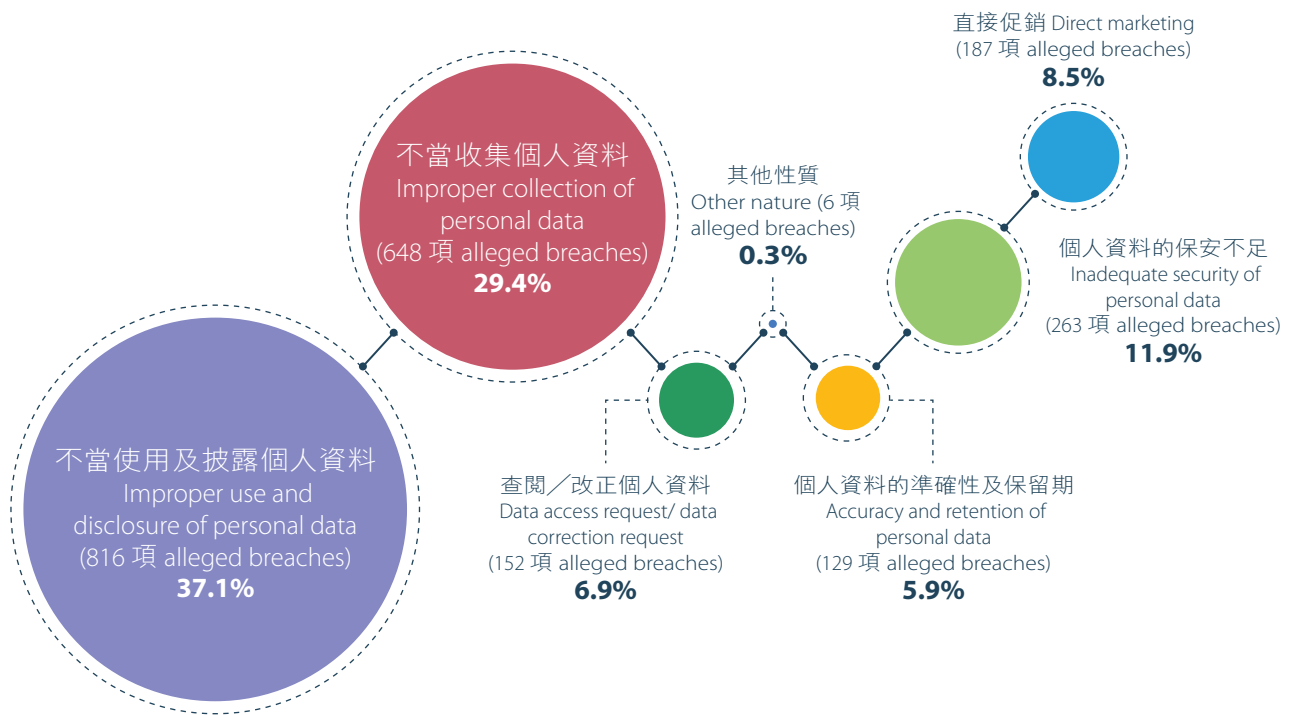
在本報告年度內接獲的 1,619 宗投訴中，共涉及 2,201 項違反《私隱條例》規定的指稱（同一宗投訴個案可涉及多於一項指稱），該些投訴指稱見圖 5.5。

圖 5.5 — 就違反《私隱條例》的投訴指稱

Nature of alleged breaches under the Ordinance

The 1,619 complaints involved a total of 2,201 alleged breaches under the Ordinance (one complaint case may include more than one allegation). The nature of the alleged breaches is shown in Figure 5.5.

Figure 5.5 — Nature of alleged breaches

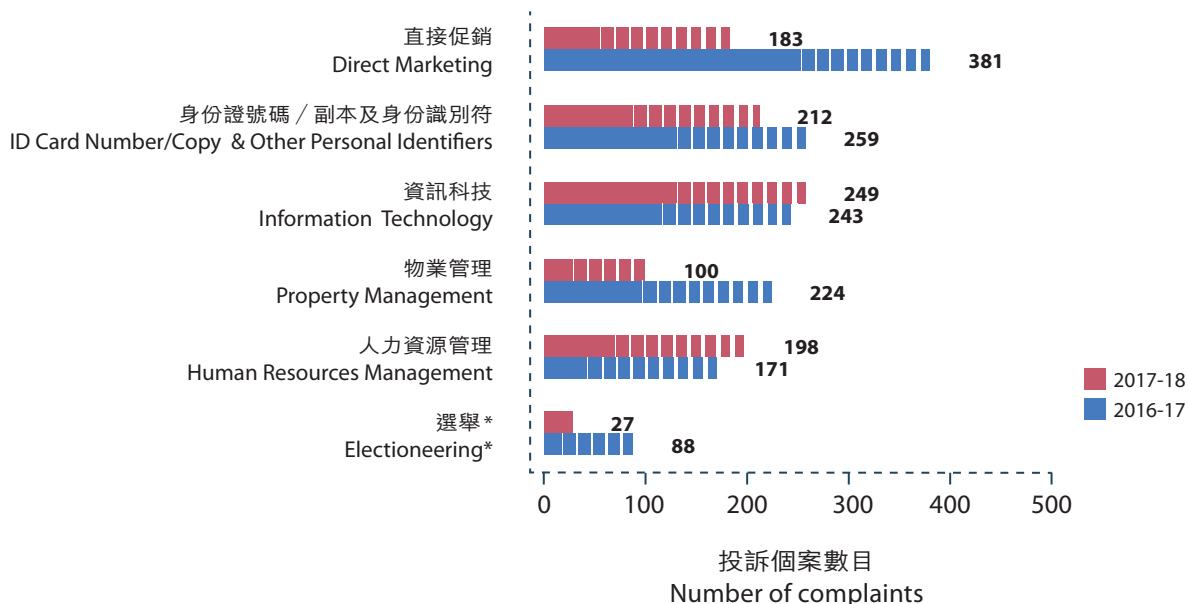


投訴所涉的主要範疇

跟上一個報告年度比較，公署於本報告年度收到的投訴中，與直接促銷及物業管理有關的有明顯下跌的趨勢，分別有52%及55%的跌幅。與資訊科技及人力資源管理有關的投訴，則分別有3%及16%的升幅。（圖5.6）

有關資訊科技的投訴中，涉及社交網絡和智能手機應用程式的投訴佔大多數，其餘的投訴涉及在互聯網上披露或洩漏個人資料、網絡欺凌等。至於有關人力資源管理的投訴中，主要涉及僱主安裝閉路電視監察員工、收集超乎適度的個人資料、向第三者披露員工的個人資料，以及沒有依從查閱資料要求。

圖 5.6 — 投訴所涉的主要範疇



* 為統計目的，公署在本報告年度收到有關選舉事務處遺失載有選民個人資料的手提電腦的1,944宗同類投訴，只作1宗投訴計算。

For statistical purpose, the 1,944 complaints received in relation to the suspected theft of computers of the Registration and Electoral Office that contained personal data of registered electors were counted as 1 complaint.

Major subjects of complaints

Compared with last reporting year, the numbers of complaints received during the reporting year by the PCPD about direct marketing and property management-related issues have decreased significantly by 52% and 55% respectively. On the other hand, the numbers of complaints concerning information technology and human resources management have increased by 3% and 16% respectively. (Figure 5.6)

As for the complaints relating to information technology, the majority of them were about social networks and smartphone applications, and the remaining complaints were mostly about the disclosure or leakage of personal data on the Internet and cyberbullying. Most of the complaints relating to human resources management were about monitoring employees through CCTV cameras, excessive collection of personal data, disclosure of employees' personal data to third parties, and failure to comply with data access requests.

Figure 5.6 — Major subjects of complaints



年度投訴摘要

在本報告年度，公署處理了193宗承接上一個報告年度的投訴，加上新接獲的1,619宗投訴，年內共須處理1,812宗投訴。在這些個案中，1,621宗(89%)在本報告年度內經已完結，而餘下的191宗(11%)，截至2018年3月31日仍在處理中。(圖5.7)

圖 5.7 — 過去五個年度投訴摘要

	2017-18	2016-17	2015-16	2014-15	2013-14
承接上年度的投訴 Complaints carried forward	193	262	253	329	393
接獲的投訴 Complaints received	1,619	1,741	2,022	1,690	1,888
共須處理的投訴 Total complaints processed	1,812	2,003	2,275	2,019	2,281
已完結的投訴 Complaints completed	1,621	1,810	2,013	1,766	1,952
未完結的投訴 Complaints under processing	191	193	262	253	329

Summary of complaints handled during the reporting year

During the reporting year, the PCPD handled 1,619 new complaints, in addition to 193 complaints carried forward from last reporting year, bringing the total number of complaints handled during the reporting year to 1,812. Of these, 1,621 (89%) were completed during the reporting year, and 191 (11%) were still in progress as at 31 March 2018. (Figure 5.7)

Figure 5.7 — Summary of complaints handled in the past five years

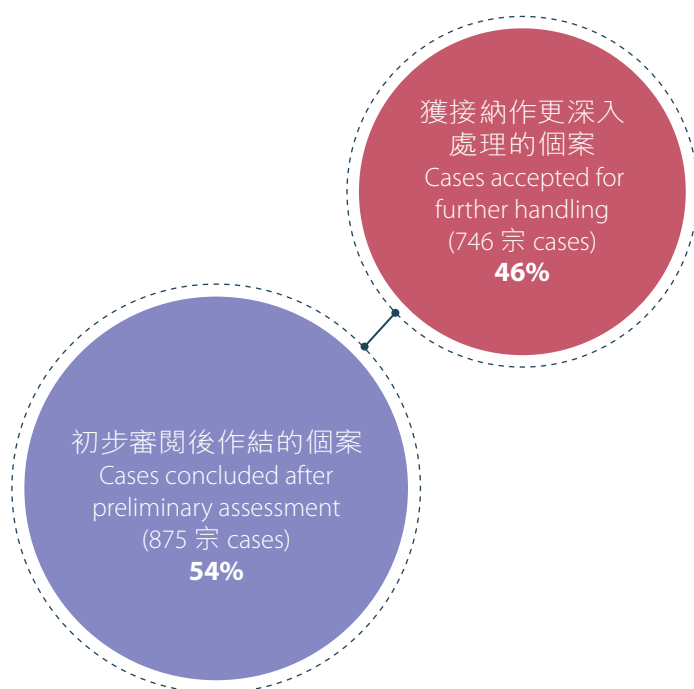
本年度已完結的投訴個案分類

在本報告年度內已經完結的1,621宗投訴，當中875宗經公署初步審閱後，基於以下原因結案：

- (i) 個案不符合《私隱條例》第37條定義的「投訴」，例如不涉及「個人資料」。部分個案則未能指明被投訴者的身份或匿名投訴等；
- (ii) 投訴人撤回投訴；
- (iii) 公署要求投訴人加以述明其指稱或提供補充資料後，投訴人未有作出回應；
- (iv) 投訴內容不在《私隱條例》的管轄範圍；或
- (v) 沒有違反《私隱條例》的表面證據。

其餘746宗個案獲公署接納作更深入處理。(圖5.8)

圖 5.8 — 本年度已完結的投訴個案分類



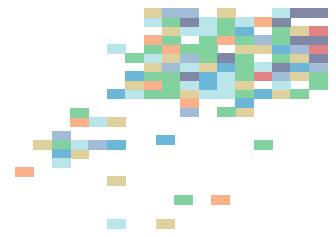
Categorisation of completed complaints

Of the 1,621 complaints completed during the reporting year, 875 were concluded after our preliminary assessment, on the grounds set out below:

- (i) the matters complained of fell outside the definition of “complaint” under section 37 of the Ordinance. For instance, the matters complained of did not involve “personal data” of the data subjects. In some cases, the complainants failed to specify the identities of the parties being complained against or the complaints were anonymous etc.;
- (ii) the complaints were withdrawn by the complainants;
- (iii) the complainants did not respond to the PCPD’s requests to provide evidence in support their allegations;
- (iv) the matters complained of were outside the jurisdiction of the Ordinance; or
- (v) no prima facie evidence of contravention.

The remaining 746 complaints were accepted for further handling. (Figure 5.8)

Figure 5.8 — Categorisation of completed complaints



公署處理投訴的方式

就該 746 宗獲公署接納作更深入處理的投訴，公署先以調停這種較便捷的解決爭議方式，嘗試解決資料當事人與被投訴者之間的糾紛。當中 635 宗經公署介入後得到解決（圖 5.9），並基於以下原因結案：

- (i) 被投訴者就投訴事項採取相應的糾正措施；
- (ii) 公署向投訴人分析所有在案資料後，投訴人不再追究；或
- (iii) 公署應投訴人要求向被投訴者表達關注，以讓被投訴者作出跟進。

此外，公署在調停期間，發現 16 宗投訴涉及刑事成份（例如有關直接促銷的條文），在公署確立表面證據成立後，投訴人同意轉介個案予警方進一步處理。

圖 5.9 — 調停、轉介警方與展開調查的投訴個案

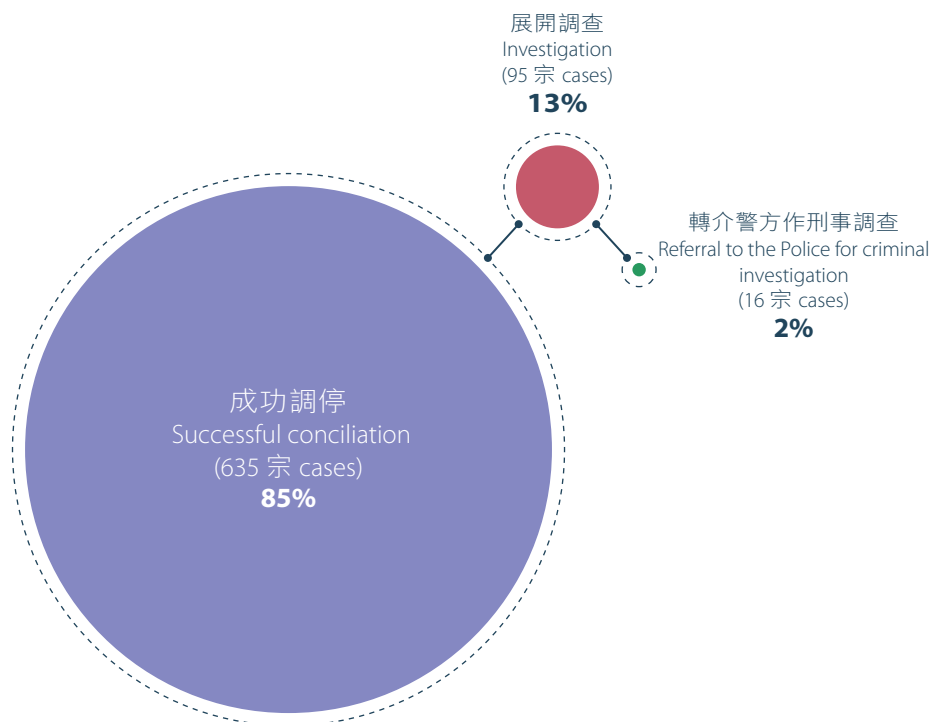
Modes of complaints handling

For those 746 complaints accepted for further handling, the PCPD attempted to resolve disputes between the data subjects and the parties being complained against by conciliation as a speedy and convenient dispute resolution alternative. 635 complaints were successfully resolved (Figure 5.9) on the following grounds:

- (i) remedial actions have been taken by the parties being complained against to resolve the problems raised by the complainants;
- (ii) the complainants withdrew their complaints after the PCPD had explained information in hand to them; or
- (iii) the PCPD had conveyed the complainants' concerns to the parties being complained against for their follow-up actions.

In the course of conciliation, 16 complaints were found involving criminal elements (e.g. direct marketing-related cases). Those complaints were referred to the Police when prima facie evidence of contravention was established and the complainant's consent for referral was received.

Figure 5.9 — Complaints resolved by conciliation, referral to the Police and investigation



餘下 95 宗的投訴因不適合或不能成功調停，而須展開調查，當中：

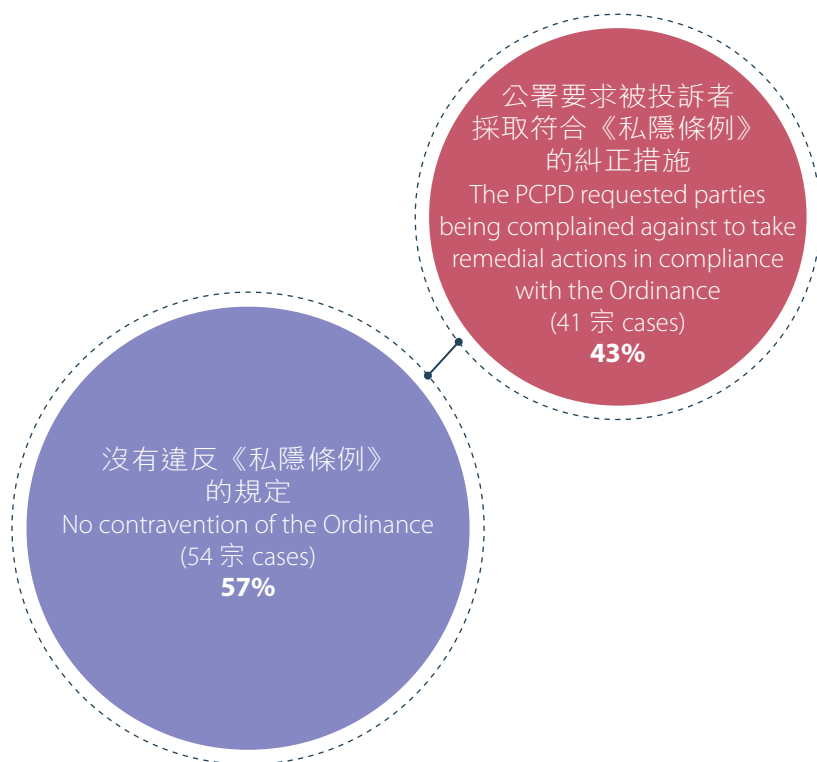
- 公署要求 41 宗的被投訴者採取符合《私隱條例》規定的相應糾正措施，公署並向部份被投訴者發出警告或執行通知。
- 餘下的 54 宗的被投訴者沒有違反《私隱條例》的規定，公署給予部分被投訴者建議，鼓勵他們建立保障個人資料的良好行事方式。(圖 5.10)

Investigations were carried out for the remaining 95 complaints, which were unsuitable for conciliation or not conciliated:

- in 41 complaints, the PCPD had requested the parties being complained against to take remedial actions in order to comply with the requirements of the Ordinance. Some of them were issued with warnings and enforcement notice by the PCPD.
- no contravention of the Ordinance was found in the remaining 54 complaints. Recommendations were given to some of the parties being complained against to encourage them to establish good practice in data protection. (Figure 5.10)

圖 5.10 — 展開調查的個案結果分類

Figure 5.10 — Categorisation of investigation cases





公署給予被投訴者的建議

公署除了向涉及違反《私隱條例》的被投訴者發出警告或執行通知外，在調停或調查的過程中亦會視乎情況提示或建議被投訴者採取糾正措施，以免重蹈覆轍，或鼓勵他們建立保障個人資料的良好行事方式。在本報告年度中，公署曾向被投訴者發出超過850項建議，要求他們：

- 遵從《私隱條例》的相關規定；
- 修訂與個人資料有關的政策和行事程序，以免再發生同類違規事件；
- 向職員發出指引，要求他們遵從有關的政策和行事程序；
- 依從投訴人的查閱／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；
- 刪除不必要地收集或向第三者披露的個人資料；
- 承諾停止被投訴的不當行為；
- 依從投訴人的拒絕接收直銷訊息要求；及
- 跟進公署轉達投訴人對其私隱的關注。

Recommendations given to the parties being complained against

Apart from issuing Enforcement Notices and warnings, the PCPD also, in some cases, advises parties being complained against to carry out remedial actions in the course of conciliation or investigation, with a view to preventing the recurrence of similar irregularities in future, and/or encourage them to establish good practice in personal data protection. During the reporting year, more than 850 recommendations were made to the parties being complained against to advise them to take the following actions:

- observe relevant requirements under the Ordinance;
- revise personal data-related policies and practices to prevent similar breach in future;
- provide proper guidance to staff to require compliance with relevant policies and practices;
- supply/correct the personal data to comply with the complainants' data access/correction requests, or reduce the fee for complying with the data access requests;
- delete personal data that was collected or disclosed to third parties unnecessarily;
- undertake to cease the malpractices leading to the complaints;
- comply with opt-out requests for not receiving direct marketing messages; and
- follow up on the privacy-related concern of the complainants.

個案選錄

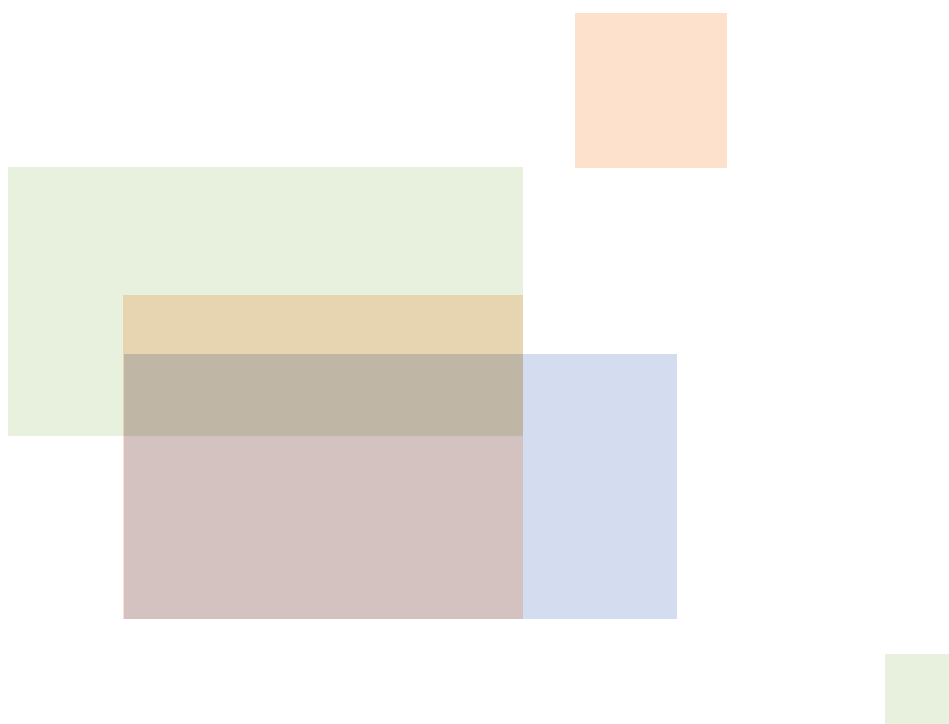
公司或機構在運用個人資料為業務或服務增值之餘，亦須有道德地顧及其作為對資料當事人所帶來的影響。以下選錄中的一些個案，說明個人資料私隱一旦被侵犯，對當事人的尊嚴、權利或利益可造成損害。

公署如認為投訴有理據，會建議涉事公司或機構作出糾正或補救。由資料當事人提出的投訴，可以令不當的處理個人資料方式得以修正，繼而惠及他人。公署希望個案選錄可供資料使用者作為借鑑，而一般市民可了解其個人資料私隱應獲得的保障。

SUMMARIES OF SELECTED CASES

Companies or organisations, when making use of personal data in enhancing business operations or services, are under ethical obligation to carefully consider the possible impact on the data subjects. The following selected cases illustrate how intrusion of personal data privacy may infringe the data subjects' dignity, rights and interests.

If complaints are found to be substantiated, the PCPD would recommend the companies or organisations involved to take corrective or remedial actions. Complaints made by data subjects can bring about the correction of malpractices of personal data handling, and subsequently benefit the community at large. By publishing these case summaries, we wish to provide data users with good lessons to be learnt, and to enhance data subjects' understanding of their privacy rights.





個案一：學校在沒有通知家長的情況下，向網絡程式供應商提供學生的個人資料，替學生開設服務帳戶 — 保障資料第3原則

投訴內容

投訴人女兒就讀的小學沒有事先通知家長，便向學校使用的網絡程式供應商提供學生的英文姓名、班別和學號，以便替學生設立服務(包括電郵、雲端硬碟、學習工具等)帳戶。學校並設定以學生的學生編號和出生日期為登入名稱和密碼。投訴人憂慮學校會監察學生使用該帳戶的情況，並擔心小學生不理解登入帳戶時須同意的服務條款，遂代表其女兒向公署作出投訴。

結果

學校表示他們雖然擁有學生帳戶的管理權，並可按教學需要設定學生可使用的服務，但沒法查閱學生的帳戶活動紀錄。學校解釋以學生姓名、班別及入學編號設定為帳戶姓名，目的是方便教師識辨學生的身份；而將密碼設定為學生的出生日期，此舉是方便學生記憶。學校強調有要求學生在首次登入後更改密碼。

公署認為家長當初提供學生的個人資料予學校時，並未獲告知有關資料會被轉移至網絡程式供應商，家長擔憂其子女的個人資料或被濫用是可以理解的。

Case 1: A school provided students' personal data to an online tool services provider for creating service accounts for students without notifying the parents — DPP3

The Complaint

The complainant's daughter was a primary school student. Without notifying the parents, the school provided its students' names, classes and class numbers to the contractor of its online tool for creating user accounts, which were used by students for logging into services provided by the tool such as email, cloud disk and learning applications. Student number and date of birth were used as default log-in name and password respectively. The complainant was worried that the school might keep track of students' account usage, and that the terms of conditions to be accepted upon logging in might be incomprehensible to primary students. The complainant therefore complained to the PCPD on behalf of her daughter.

Outcome

The school stated that although it had control over students' accounts and might decide on the services used by students according to teaching needs, it was unable to review students' account activities. Besides, the school explained that naming service accounts by student name, class and student number could facilitate identification of users by teachers. The setting of date of birth as default password was also done on purpose for easy recall by students. The school stressed that it had required the students to change their account password upon the first log-in.

When parents provided their children's personal data to the school, they were not informed that the data would be transferred to the contractor of its online tool. In the circumstances, parents' concern about possible misuse of their children's personal data was understandable.

經公署解釋《私隱條例》的相關規定後，學校表示會以其他字元組合為學生建立帳戶，及讓家長選擇是否保留學校已為學生建立的帳戶。此外，學校並制訂學生使用服務的政策，清楚訂明開立帳戶的目的及用途，並發放如何安全使用帳戶及學校的管理權等資訊，以釋除家長的憂慮。

借鑑

學校在本案中的行為出於善意，亦符合現今利用科技促進教育的大趨勢。然而，在本案發生前，學校未有周詳地考慮家長及學生在個人資料私隱方面的期望，亦未能及早告知家長及學生有關安排，家長在得悉子女的個人資料被如此使用難免感到驚訝，因而產生了憂慮。公署欣悉學校迅速作出的上述改善措施，令家長對學校重拾信任。

After the PCPD explained the relevant requirements under the Ordinance to the school, the school undertook that it would use other combinations of characters to create user account for students. For the existing accounts, parents might choose whether they would keep using them or not. Besides, the school would develop a policy on usage of the online tool, define the purposes of account creation, and publicise account safety and the school's right to manage the accounts, to alleviate parents' concern.

Lesson Learnt

The school's practice in question was well-intended, and was in line with the latest trend of facilitating learning with technology. However, the school had not thoroughly considered the personal data privacy expectation of parents and students, nor informed them of the relevant arrangements in advance. Parents would inevitably be surprised and worried when they learnt of such use of students' personal data. We are glad that the school responded timely with the above improvement initiatives to regain the parents' trust.





個案二：律師事務所將投訴人的私人信件發送至她辦公室的共用電郵信箱，以致信件遭第三者查閱 — 保障資料第4原則

投訴內容

代表投訴人丈夫的律師事務所將一封內容與投訴人正辦理離婚有關的私人信件，發送至投訴人辦公室公用的電郵地址。

該事務所向公署表示，他們曾將信件發送至投訴人的私人電郵地址，但不獲投訴人回應，該事務所遂將信件發去投訴人辦事處的電郵地址，並在電郵標題註明為私人密件。該事務所表示，他們是從網上搜尋到投訴人辦事處的電郵地址，加上他們當時未能從投訴人丈夫提供的資料確定投訴人的其他聯絡方法，故他們在發出電郵前未有先聯絡投訴人核實該電郵信箱是否由她本人開啟。此外，該事務所表示他們之所以發送該信件至投訴人辦事處的電郵地址，是希望盡快收到她的回應。

結果

公署認為，該事務所如有必要將信件發送至投訴人辦公室的電郵地址，他們應先將信件加密或先與投訴人核實該電郵信箱是否由她本人開啟，才將信件發出。公署認為，該事務所並無採取所有切實可行的步驟以保障投訴人的個人資料，違反保障資料第4原則。

經公署介入後，該事務所承諾會預先將郵件加密或與收件人溝通，才會以電郵方式發送載有個人資料及敏感資料的文件。

Case 2: A law firm sent a private letter to a general email address of the data subject's workplace, resulting in disclosing the letter to a third party — DPP4

The Complaint

A law firm, acting on behalf of the complainant's husband, sent a letter regarding the complainant's divorce, which was underway, to a general email address of her workplace.

According to the law firm, it initially sent the letter to the complainant's personal email address but received no response. It subsequently sent the letter to the general email address of the complainant's office, which had been obtained from the Internet. It clearly marked "Private and Confidential" in the subject heading of the email. Being unable to confirm other means of contact of the complainant from the information provided by her husband, the law firm had not contacted the complainant to ascertain whether she would personally check the emails received through the general email address of her office, before sending the email to her. The law firm explained that it sent the letter to the complainant through the general email address of her office in the hope of getting her prompt response.

Outcome

If the law firm needed to send the letter to the general email address of the complainant's office, it should ascertain in advance if the complainant personally checked the emails received via that office email address, or send the letter encrypted. We considered that the law firm had failed to take all practicable steps to ensure that the complainant's personal data was protected against unauthorised or accidental access, hence in breach of DPP4.

After the PCPD's intervention, the law firm undertook that when they had to deliver documents containing personal data or sensitive information to others under similar circumstances in future, they would communicate with the recipient in advance or encrypt the message.

借鑑

婚姻訴訟屬婚姻雙方之間的私人事務，一般人理應不希望無關人士知悉。本案的律師事務所的行為明顯未有周詳考慮投訴人的私隱期望，以致其婚姻訴訟被一眾同事得悉，是不專業且不負責任的行為。

律師事務所每天處理大量個人資料，可以此案為鑑，重新審視發送文件的流程，以確保個人資料私隱能得到保障。

Lesson Learnt

No one would welcome the details of his/her divorce proceedings, which are strictly private, be made known to unrelated parties. The law firm in this case had obviously failed to give due consideration to the privacy expectation of the complainant. Her divorce proceedings were hence made known to her colleagues. Such act of the law firm was unprofessional and irresponsible.

Law firms handle a large volume of personal data every day. They can take reference from this case as an example to review the current procedures in delivery of documents to ensure protection of personal data.





個案三：查閱資料要求的權利只限於取得指明的個人資料的複本，而不是指明的文件的副本 — 保障資料第 6 原則

投訴內容

一位即將退休的大學講師向校方申請延長聘用，校方審理後拒絕了其申請。講師其後向大學遞交一份查閱資料要求表格，以查閱審理其申請有關的文件，校方應講師的要求提供了有關資料。

講師收悉文件後，發現當中的一份綜合報告提及校方曾就處理其申請召開的會議。雖然該報告中已包括該會議的內容概要，但投訴人認為校方應獨立向他提供該會議紀錄的副本，他遂向公署投訴校方。

結果

《私隱條例》第 18(1)(b) 條規定，任何個人有權要求資料使用者提供其個人資料的複本。在司法覆核個案胡潔冰訴行政上訴委員會（法院案件編號 HCAL 60/2007）中，法庭裁定根據第 18(1)(b) 條，資料當事人只是有權取得其個人資料的複本，而非每份文件的副本。

公署認為，校方向講師提供的報告內已包含該會議紀錄中涉及投訴人的資料，即已向投訴人提供在該會議紀錄中他的個人資料的複本，因此校方不會因為沒有向投訴人提供該會議紀錄的副本而違反《私隱條例》的規定。

Case 3: The right of data access request is restricted to obtaining a copy of the specified personal data, not a copy of the document containing the personal data — DPP6

The Complaint

The complainant was a member of the teaching staff of a university. He applied for re-appointment beyond retirement age. However, his application was declined by the university. He later submitted a data access request to the university for a copy of the documents in relation to the assessment of his application. The university complied with the request by providing him with a copy of the personal data concerned.

The complainant noted from an integrated report (the Report) among the documents provided by the university that a meeting in relation to his application was held by the university. Despite that the Report already contained a summary of the meeting, the complainant considered that the university should have provided him with a copy of the minutes of the meeting (the Minutes). He therefore complained to the PCPD against the university.

Outcome

Under section 18(1)(b) of the Ordinance, an individual may make a request for access to his personal data held by a data user. In judicial review *Wu Kit Ping v. Administrative Appeals Board HCAL 60/2007*, the Judge ruled that the right of a data subject under section 18(1)(b) of the Ordinance was accessing a copy of his personal data, not a copy of the document containing his personal data.

The PCPD considered that the Report provided by the university to the complainant had already included the personal data of the complainant contained in the Minutes. Given that the university had already provided the complainant with his personal data contained in the Minutes, the university would not contravene the requirement of the Ordinance for not having provided him with a copy of the Minutes.

借鑑

《私隱條例》賦予市民查閱資料的權利，然而市民經常誤會可引用此權利以查閱任何載有他的個人資料的文件，或向機構取得文件複本。法例的原意是提供渠道以供資料當事人查閱資料使用者持有他的個人資料，以及在發現不準確時要求更正。查閱資料要求並不是文件透露程序，市民不應期待可以透過查閱資料要求取得任何指定文件的完整或局部副本。

Lesson Learnt

The Ordinance provides right of members of the public to access their personal data. However, it is a common misunderstanding that this right can be used to access any documents containing an individual's personal data, or for obtaining a copy of such documents. The legislative intent of data access request is to provide a channel to a data subject to access his or her personal data held by a data user, and to request correction when an inaccuracy is noted. Data access request is not a document discovery process. The public should not expect to obtain a full or partial copy of specific documents by making a data access request.





個案四：機構使用閉路電視搜證時仍須按法例確保所涉個人資料的保安 — 保障資料第4原則

投訴內容

一所大學校園的民主牆上出現了一些冒犯性的字句。事件引起公眾關注及傳媒廣泛報導，當中一份報章更公開了兩名男子涉嫌張貼有關字句的閉路電視片段截圖。

有市民懷疑是大學主動向報章披露這些閉路電視片段截圖，涉嫌侵犯截圖中人士的私隱，遂向公署作出投訴。公署隨即就該閉路電視片段截圖外洩事件對大學展開循規審查。

結果

審查資料顯示，大學關注假如是該大學的學生張貼有關字句，那些學生必蒙受巨大壓力而不知怎樣自處，因此校方認為有必要盡快確定涉案人士的身份，以便對有關學生進行輔導。另一方面，事件已影響學校聲譽，違反學生行為守則，大學因而須識辨涉案人士的身份，繼而作出調查及考慮採取紀律處分。

基於上述理由，大學保安中心在事件發生後翻查校園的閉路電視片段，並用手提電話拍攝相關的兩張截圖，然後傳送到大學管理層人員組成的即時通訊社交媒體群組中，希望能盡快識辨涉案人士。群組內的部分成員更將該兩張截圖轉發至十多名教職員及一名學生，要求他們協助識辨該兩人。

Case 4: An organisation is required by the law to ensure personal data security even when using CCTV for collection of evidence — DPP4

The Complaint

A banner with offensive message was posted on the “Democracy Wall” of a university. The accident aroused widespread public concern and media coverage. One of the local newspapers published two screenshots captured from the campus CCTV footage showing two men posting the banner.

Some members of the public suspected that the university had provided the screenshots to the media, intruding on the privacy of those two men. They complained to the PCPD against the university. The PCPD therefore initiated a compliance check against the university.

Outcome

As revealed in the compliance check, the university noted that if the banner was posted by its students, those students might experience great pressure and might not know how to deal with the situation. It was therefore necessary for the university to ascertain the identity of the persons involved to provide them with counselling. On the other hand, as the act of posting such a banner appeared to have violated the General Code of Student Conduct, and it damaged the university’s reputation, the university needed to identify the persons involved in order to conduct further investigation, and to consider disciplinary action.

Accordingly, the security centre of the university ascertained from campus CCTV footage that the banner had been posted by two men. Two screenshots were made and sent to the university’s senior management via an instant messaging social network group for the purpose of timely identification of the persons involved. For the same purpose, some members of the social network group forwarded the two screenshots to more than 10 other staff members and one student.

公署留意到大學以即時通訊社交媒體傳閱兩張截圖的目的是進行紀律調查，與其原先為保安理由而安裝閉路電視監察系統的目的並不相同，表面上或不符保障資料第3原則的規定。不過，如果是為調查及懲處嚴重不當行為（並不限於罪案）的目的而使用的個人資料，則受《私隱條例》第58條所豁免，以致有關資料不受保障資料第3原則所管限。

在考慮到事件影響大學校譽及有關行為涉及違反學生行為守則（如字句是學生張貼），公署認為《私隱條例》第58條的豁免適用，即大學以即時通訊社交媒體傳閱兩張截圖的做法不涉及違反保障資料第3原則的規定。

不過，公署認為即使該大學有必要第一時間將兩張截圖於該群組內傳閱，大學亦務必要提醒群組的成員該兩張截圖屬機密資料，不可隨意轉發，以及在完成使用截圖後，須立即將截圖刪除等。

由於該大學沒有採取所有合理地切實可行的保安措施去保障該兩名人士的個人資料，公署認為該大學違反了保障資料第4原則的規定。該大學接納公署的意見，並採取以下措施加強保障校園閉路電視片段：

- (i) 在該群組訂明各人均須遵守保密原則；
- (ii) 制定閉路電視監察政策及程序，包括清楚列明持有個人資料的種類、收集資料的主要使用目的及保留政策等事宜；及
- (iii) 為負責有關閉路電視系統的日常運作的職員制定詳細的工作指引，當中包括翻查及截取閉路電視片段的程序及保安措施。

The PCPD noted that there might be a prima facie contravention of DPP3 of the Ordinance by the university, given that the purpose of circulating the two screenshots through the instant messaging application for disciplinary investigation was different from the original purpose of installing the CCTV, which was for security. However, if the personal data was used for investigation and punishment of seriously improper conduct (not limited to crimes), such data was exempt from the provisions of DPP3 by virtue of section 58 of the Ordinance.

Given that the incident might damage the university's reputation and the act of posting such a banner appeared to have violated the General Code of Student Conduct (if it was done by the university students), the PCPD took the view that section 58 of the Ordinance would apply such that the circulation of the two screenshots by the university through the instant messaging application did not contravene DPP3.

However, the PCPD considered that even though the university needed to circulate the two screenshots within the social network group in a timely manner, it should have reminded the members of the group that the screenshots were confidential information not to be shared with others and they had to be deleted immediately after use.

All in all, the university failed to take all reasonably practicable steps to safeguard the two persons' personal data, thereby contravening DPP4 of the Ordinance. The university took the PCPD's advice and has taken the following actions to enhance the protection of the CCTV images:

- (i) stating in the social network group that members were required to maintain confidentiality;
- (ii) devising CCTV monitoring policies and procedures to ensure that matters relating to the types of personal data held and the main purposes for which the data collected was to be used, as well as the retention policies were clearly set out; and
- (iii) devising detailed operational guidelines for the CCTV operating staff, including procedures on retrieval and capturing of CCTV footage and security measures.



借鑑

法律保障所有人的個人資料私隱為基本人權，但這不是絕對的權利。《私隱條例》對不同人士的個人資料的保障並非在所有情況下均為相同。例如當有罪案、嚴重不當、不誠實或舞弊的行為發生時，為了可即時及有效地去偵測這些行為，涉案者的個人資料私隱並不會凌駕於社會的整體利益之上。正因如此，《私隱條例》第8部訂下了多項豁免的情況，使在防止及偵測這些行為時而使用的個人資料，不受《私隱條例》所管限，以避免犯罪者及干犯嚴重不當、不誠實或舞弊行為的人士以《私隱條例》作其「擋箭牌」，逃避調查及應有的懲處。

另一方面，大學作為資料使用者亦有責任保障個人資料，即使是為識辨涉事者的目的，亦必須顧及有關人士的合理期望。在本案中，大學輕視了網絡世界的無遠弗屆，對以即時通訊社交媒體傳送涉及個人資料的訊息的安全性警覺不足。

Lesson Learnt

Personal data privacy is protected by the law as a fundamental human right of any person. However, this is not an absolute right. The Ordinance affords different levels of personal data privacy protection to different people under different circumstances. For example, in order to promptly and effectively detect crime, seriously improper conduct, dishonesty or malpractice, the personal data privacy right of the offender shall not override the interests of society at large. Part 8 of the Ordinance therefore provides for exemptions for the use of personal data in the prevention and detection of such acts so that offenders and persons who committed seriously improper conduct, dishonesty or malpractice cannot use the Ordinance as a “shield” to fence off investigation or punishment.

That said, the university, being the data user, had an obligation to protect personal data privacy. Although there was a need to identify the persons involved in the incident, the university should not go beyond the reasonable privacy expectation of the data subjects. The university had underestimated the ubiquitous nature of the cyberspace, and lacked the vigilance expected of it in securely sending the personal data through instant messaging application.





個案五：專業團體不當地向其會員披露一名有興趣加入此行業的人士的犯罪紀錄 — 保障資料第3原則

投訴內容

投訴人多年前因不誠實行為而被定罪，有關定罪已失時效。投訴人向某專業團體查詢，在申請有關專業的見習職位時是否需要披露其上述的定罪紀錄詳情。

由於法例禁止此行業的會員在未得該專業團體的批准下，聘用曾因不誠實行為而被定罪的人士，故此該專業團體於其會員通告上向會員披露了投訴人的定罪紀錄詳情，以提醒會員在沒有該專業團體的批准下不得聘用投訴人。

投訴人向公署投訴該專業團體在未徵得他的同意下，向其會員披露他已失時效的定罪紀錄詳情。除此以外，他亦申請了司法覆核，指控該專業團體如此披露他的個人資料違法。

結果

法庭在司法覆核的裁決中指出，投訴人在案中只是查詢他可否加入有關專業此原則性問題，沒有資料顯示投訴人在查詢時已受聘於該專業團體的會員機構。由於投訴人只是在探究有關原則，而不是實際嘗試加入該專業，所以投訴人仍受《罪犯自新條例》的保障。法庭最終裁決該專業團體於其會員通告上披露投訴人曾被定罪資料的決定屬違法。

Case 5: A professional body improperly disclosed to its members the spent conviction of a person who was interested to enter the profession — DPP3

The Complaint

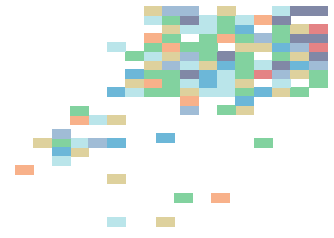
After many years of his conviction of dishonest conduct, the complainant wrote to a professional body to enquire if he needed to disclose the spent conviction in his intended application for traineeship in that profession.

The law prohibits members of the professional body from knowingly employing a person convicted of an offence of dishonesty without the professional body's permission. To warn its members against employing the complainant without its prior permission, the professional body disclosed details of the complainant's conviction in a circular to its members.

The complainant complained to the PCPD against the professional body for contravention of DPP3 in disclosing his spent conviction to its members without his consent. Separately, he applied for a judicial review, alleging that the professional body's decision to publish his spent conviction was unlawful.

Outcome

The Court held in the judicial review that the publication of the circular disclosing the complainant's spent conviction was unlawful. As far as the complainant's case was concerned, he was simply exploring the possibilities of entering the profession by making enquiries on a matter of principle. There was nothing to show that the complainant was at the material time employed by any of the professional body's members. The Court considered that the complainant should be entitled to the protection under the Rehabilitation of Offenders Ordinance until his intention to join the profession goes beyond merely exploring possibilities.



該專業團體依從法庭裁決，在相關的通告上刪除了投訴人的定罪紀錄詳情。此外，該專業團體亦聽取了公署的意見，將來在類似的情況下，在相關的通告上只會刊出有關人士曾因不誠實行為而被刑事定罪一事，有意招聘的會員可聯絡該專業團體，以「需要知道」的原則索取詳情。

借鑑

給予某些曾干犯罪行但已改過自新的人士不被標籤重投社會的機會，是公共政策的大方向。在本案中，對該專業團體而言，其上述做法可能只是一心維護會員的利益，是未有細想後果的無心之失，但投訴人可能因為該團體此舉而斷送了本來可得到的就業機會。假若該專業團體當初處理事件時能顧及有關人士的合理期望，細想其作為可招致的後果，或許便能避免本案的發生。

The professional body complied with the Court decision by deleting the details of the complainant's conviction from the circular. Besides, upon the PCPD's advice on protection of personal data, the professional body, in similar circumstances in future, would only state that the person concerned was once convicted of "a criminal offence involving dishonesty". Any member of the professional body who finds a prospective employee mentioned in the circular may then contact the professional body for details of that person's conviction on a need-to-know basis.

Lesson Learnt

The public policy calls for equal opportunities for rehabilitated ex-offenders to avoid them from being labeled and to help them re-integrate into the community. In this case, the professional body might be keen to protect its members' interests. However, it failed to carefully assess the possible consequences of its actions and consequentially made an unintentional mistake. Such act of the professional body might deprive the complainant of the job opportunities he might deserve. If the professional body had considered upfront the reasonable expectation of the complainant and the possible consequences of its actions, the complaint could probably be avoided.





個案六：機構於一名前僱員離職超過七年後仍保留其工作表現的個人資料 — 保障資料第2(2)原則

投訴內容

投訴人為一名地產代理，他曾因僱主指其工作表現欠佳而離職。於投訴人離職後，該僱主一直保留有關投訴人工作欠佳的紀錄。投訴人在十年後再次受聘於該僱主，而他從同事口中得知他因過往工作表現欠佳，而曾被僱主考慮永不錄用。及後，投訴人再度離職，並向公署投訴該僱主多年來仍保留他首次入職時的個人資料，包括工作表現紀錄。此外，他亦指稱該僱主將考慮永不錄用他的資料向其他同事披露。

結果

該僱主向公署解釋，地產代理行業的僱員於離職後再次入職是慣常現象，因此他們會將僱員的人事資料包括工作表現紀錄永久保存，以備將來前僱員再次申請入職時作考慮。

保障資料第2(2)原則規定，資料使用者須採取所有切實可行的步驟，以確保個人資料的保存時間不超過將其保存以貫徹該資料被使用於或會被使用於的目的（包括任何直接有關的目的）所需的時間。公署制訂的《人力資源管理實務守則》（守則）第4.2.3段訂明，僱主不應保留前僱員的個人資料超過七年，由前僱員離職日期起計，除非：有具體理由規定僱主須保留有關資料一段較長的期間；或前僱員給予訂明同意可將有關資料保留超過七年。

Case 6: Retention of an employee's unsatisfactory employment records by an employer over seven years — DPP2(2)

The Complaint

The complainant was an estate agent. He left his job when his employer, a property agency company (the Company), was dissatisfied with his performance. Since then, the Company had retained records of the complainant's unsatisfactory performance. When the complainant rejoined the Company ten years later, he learnt from his colleagues that the Company had once intended not to employ him again due to his poor performance in the past. The complainant left the Company again and complained to the PCPD against the Company for retaining his personal data related to his first-time employment for too long. He also alleged that the Company revealed to his colleagues its intention of not employing him again.

Outcome

The Company explained to the PCPD that it was common for estate agents to rejoin their companies after departure. It therefore permanently retained former employees' personal data, including job performance records, for consideration of employment in future.

DPP2(2) stipulates that all practical steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used. As for continued retention of personal data of former employees, paragraph 4.2.3 of the Code of Practice on Human Resource Management (the Code) issued by the PCPD stipulates that the employer should not retain such data for a period longer than seven years from the date the former employee ceases employment with the employer unless there is a subsisting reason that obliges the employer to retain the data for a longer period or the former employee has given prescribed consent for the data to be retained beyond seven years.



經公署介入調查後，該僱主已修訂有關保留前僱員的個人資料的政策，訂明前僱員的人事紀錄一般不得保存超過七年。假如該僱主需要處理與前僱員有關的訴訟或履行合約上的責任，該名前僱員的人事紀錄將被保留至有關個案完結。

此外，該僱主在此案調查期間已依從公署的建議，銷毀了投訴人第一次受僱期間的人事紀錄包括工作表現紀錄。關於投訴人指稱僱主將考慮永不錄用他的資料向其他同事披露，因他提供的舉證資料不足而未能成立。

借鑑

僱員離職，即代表賓主關係結束，僱員的個人資料在其離職後合理時間內應予以銷毀。離職僱員的個人資料保留時間越久，其準確性亦會大大減低，假如僱主仍使用這些資料考慮離職僱員再次入職的申請，便可能對僱員構成不公。僱主作為資料使用者，有責任公平和具道德地處理資料。公署希望各僱主能以此案為鑒，重新審視自己保存前僱員個人資料的政策，以確保符合《私隱條例》及守則的上述規定。

After the PCPD's intervention, the Company revised its retention policy, which now states that the personal data of former employees should generally not be retained for more than seven years. In case the Company needs to handle a court case related to an ex-employee or fulfill its obligations under an employment contract, the personal data concerned would be retained until the purposes are achieved.

During the investigation, the Company destroyed the complainant's employment records (including the performance records) collected in his employment a decade ago. As for the allegation against the Company for disclosure of its decision of blacklisting the complainant, it was found unsubstantiated.

Lesson Learnt

Upon the end of employment relationship following the departure of an employee, the employer should destroy the employee's personal data within a reasonable period of time. The longer the personal data is kept, the less accurate it may become. If employers assess an application for re-employment with reference to the outdated personal data, it would be unfair to the prospective employee. Employers as data users are obliged to handle personal data in a fair and ethical manner. The PCPD calls on employers to review their data retention policy for former employees, so as to comply with the requirements under the Ordinance and the Code.



檢控及定罪個案

在本報告年度有四宗被檢控的個案，除一宗涉及《私隱條例》第50B條「關乎沒有遵從專員的要求等的罪行」外，其餘均涉及使用個人資料作直接促銷。四宗個案均被定罪。



個案 1：一名公司董事沒有遵從私隱專員的合法要求 — 《私隱條例》第50B條

投訴內容

投訴人於2014年委託僱傭中介公司聘請外籍家庭傭工，並提供他的個人資料辦理有關手續。其後投訴人向公署投訴，指該公司在未得他同意下將他的個人資料披露給第三者。

公署在調查過程中，曾多次發信及致電該公司的負責人以了解案情，但一直未獲回覆。私隱專員其後根據《私隱條例》第44(1)條向該公司的唯一董事發出傳票，要求他在傳票所指定的時間及地點接受公署的訊問，及提供傳票註明與個案相關的資料，但該董事無合法辯解而沒有到公署接受訊問和提供資料，公署遂把個案轉介警方作刑事調查。

結果

該董事被控在沒有合法辯解的情況下不遵從私隱專員的傳召到其席前提供資訊，違反了《私隱條例》第50B(1)(b)條。該董事於2017年6月30日承認控罪，被罰款HK\$3,000。

PROSECUTION AND CONVICTION CASES

During the reporting year, four cases had been prosecuted. Among them, one was related to section 50B of the Ordinance (failure to comply with requirements of the Privacy Commissioner) and the rest were related to the use of personal data in direct marketing. All four cases were convicted.

Case 1: A company director convicted of failing to comply with a lawful requirement of the Privacy Commissioner — Section 50B of the Ordinance

The Complaint

A complainant engaged an employment agency to recruit a foreign domestic helper in 2014 and provided his personal data for the employment purpose. The complainant later complained to the PCPD, alleging that the employment agency had transferred his personal data to a third party without his consent.

During the course of investigation, the PCPD had repeatedly requested the relevant person of the employment agency in writing and by telephone to provide the necessary information required for investigation. Upon failing to obtain a reply, the Privacy Commissioner issued a summons to the sole director of the employment agency under section 44(1) of the Ordinance requiring him to attend the office at the specified date and time for examination and to provide relevant information as stated. However, the director failed to attend the office without lawful excuse. The PCPD then referred the case to the Police for criminal investigation.

Outcome

The director was charged with the offence of failing to comply with a summons issued by the Privacy Commissioner to attend before him to provide relevant information without lawful excuse, contrary to section 50B(1)(b) of the Ordinance. The director pleaded guilty to the charge and was fined HK\$3,000 on 30 June 2017.



個案 2：一名理財顧問被裁定在使用投訴人的個人資料作直接促銷前沒有採取指明的行動通知投訴人，以及未有告知該人可拒收直接促銷訊息的權利 — 《私隱條例》第 35C 及 35F 條

投訴內容

投訴人在一間政府有關機構工作，她的姓名和辦公室電話可從政府電話簿內取得。2015 年 10 月，該名理財顧問致電投訴人的辦公室電話，以中文全名稱呼投訴人，向她推銷該顧問任職的理財服務公司的投資產品。投訴人表示她並非該理財服務公司的客戶，亦未曾同意讓該公司使用其個人資料作直銷用途，在電話交談的過程中該顧問亦未有告知投訴人她有權要求該顧問停止如此使用有關資料。

結果

該顧問被控在使用他人的個人資料作直接促銷前，未有採取指明行動通知資料當事人，違反了《私隱條例》第 35C(2) 條，以及在首次使用他人的個人資料作直接促銷時，未有告知該人他有權要求被告在不向其收費的情況下停止使用他的個人資料作促銷用途，違反了《私隱條例》第 35F(1) 條。被告於 2017 年 11 月 17 日承認上述兩項控罪，被判罰每項控罪各 HK\$10,000。

Case 2: A financial consultant of a financial services company convicted of using the complainant's personal data in direct marketing without taking specified actions and failing to notify the complainant of his opt-out right — sections 35C and 35F of the Ordinance

The Complaint

The complainant worked in a government-related organisation. Her personal data, including her name and office phone number, could be obtained from the Government Telephone Directory. In October 2015, the complainant received a call from the defendant on her office phone number, addressing the complainant by her Chinese full name. The call was to promote the investment products of the financial services company. The complainant stated that she was not a customer of the financial services company and had never consented to its use of her personal data in direct marketing. During the phone conversation, the defendant did not notify the complainant of her opt-out right.

Outcome

The consultant was charged with the offence of (1) using the personal data of the complainant in direct marketing without taking specified actions, contrary to section 35C(2) of the Ordinance; and (2) failing to inform the complainant, when using her personal data in direct marketing for the first time, of her right to request not to use her personal data in direct marketing without charge, contrary to section 35F(1) of the Ordinance. The consultant pleaded guilty to both charges and was fined HK\$10,000 for each charge on 17 November 2017.



個案3：一間健身公司被控沒有依從拒收直銷訊息要求 — 《私隱條例》第35G條

投訴內容

投訴人於2011年曾參加一間健身公司的試玩計劃，在登記時提供了他的姓名和手提電話號碼。試玩完畢，投訴人沒有繼續使用該公司的任何服務。及後，該公司於2013年致電投訴人向他作出服務推廣，通話期間投訴人已即時向該公司作出拒收直銷訊息要求，但該公司於2015年12月再次致電他作直銷推廣。

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，違反了《私隱條例》第35G(3)條的規定。該公司於2017年12月11日承認控罪，被判罰款HK\$7,000。

Case 3: A fitness company convicted of failing to comply with an opt-out request — section 35G of the Ordinance

The Complaint

The complainant joined a trial service of a fitness company in 2011 and provided his personal data, including his name and mobile phone number, during registration. After the trial, he did not continue to use the service of the company. The complainant later received a direct marketing call from the company in 2013 and he immediately made his opt-out request during the telephone conversation. However, the complainant received a direct marketing call again from the company in December 2015.

Outcome

The company was charged with an offence under section 35G(3) of the Ordinance for failing to comply with the requirement from a data subject to cease to use his personal data in direct marketing. The company pleaded guilty to the charge and was fined HK\$7,000 on 11 December 2017.





個案 4：一間超級市場被控在沒有當事人同意下使用其個人資料作直接促銷 — 《私隱條例》第 35E 條

投訴內容

投訴人是該超級市場購物網站的顧客，並曾向該公司提供其電郵地址等個人資料作登記之用，投訴人從沒向該公司表示願意收取直接促銷的資訊，但該公司於 2016 年 1 月向投訴人寄發一封直接促銷電子郵件。

結果

該公司被控在沒有投訴人同意下使用其個人資料作直接促銷，違反了《私隱條例》第 35E(1) 條的規定。該公司於 2018 年 1 月 2 日承認控罪，被判罰款 HK\$3,000。

Case 4: A supermarket convicted of using the personal data of a data subject in direct marketing without obtaining the data subject's consent — section 35E of the Ordinance

The Complaint

The complainant was a registered customer of the online supermarket of the company and provided his personal data including his email address to the company for registration. The complainant had never indicated to the company that he wished to receive any direct marketing materials. In January 2016, the complainant received a direct marketing email from the company.

Outcome

The company was charged with an offence for using the personal data of a data subject in direct marketing without obtaining the data subject's consent, contrary to section 35E(1) of the Ordinance. The company pleaded guilty to the charge and was fined HK\$3,000 on 2 January 2018.

