執法保障資料
ENFORCING DATA PROTECTION

調查全面、不偏不倚

對於市民的投訴及查詢，私隱公署具效率、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

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

私隱公署在報告年度接獲的查詢個案為23,779宗*，較2018/19年度的17,168宗上升39%。其中有2,478宗是關於一名警務人員在鏡頭前展示一名記者的身份證一事、1,028宗關於有人於葬禮拍攝一名警務人員，以及1,018宗關於一名區議員披露警務人員的個人資料。撇除上述事件的查詢個案後，公署接獲的查詢個案為19,255宗，其中33%是關於收集/使用個人資料（例如身份證號碼或副本）；8%是與僱傭相關的個人資料處理；6%是關於使用閉路電視的查詢。

與使用互聯網有關的查詢由2018/19年度的840宗上升至2019/20年度的1,695宗，升幅超過一倍，主要涉及網絡欺凌、於互聯網及社交平台收集及使用個人資料。

* 一宗查詢可能涉及多項性質

圖 5.1 – 查詢個案數目

HANDLING ENQUIRIES

During the reporting year, PCPD received a total of 23,779 enquiries*, which represented an increase of 39% as compared to 17,168 enquiries in 2018/19. Of these enquiries, 2,478 cases were about a police officer showing a reporter's Hong Kong Identity Card before camera; 1,028 cases were about photo-taking of a police officer at a funeral; and 1,018 cases were about disclosure of a police officer's personal data by a District Council member. Excluding the cases of the aforesaid incidents, PCPD received 19,255 enquiries. The enquiries mainly related to the collection/use of personal data (e.g. Hong Kong Identity Card number or copies) (33%), handling of personal data in employment (8%), and use of CCTV (6%).

Internet-related enquiries increased by 102% to 1,695 cases in 2019/20 from 840 cases in 2018/19. They mainly concerned cyberbullying, collection and use of personal data on Internet and social media platforms.

* An enquiry may involve multiple nature

Figure 5.1 – Number of enquiries received

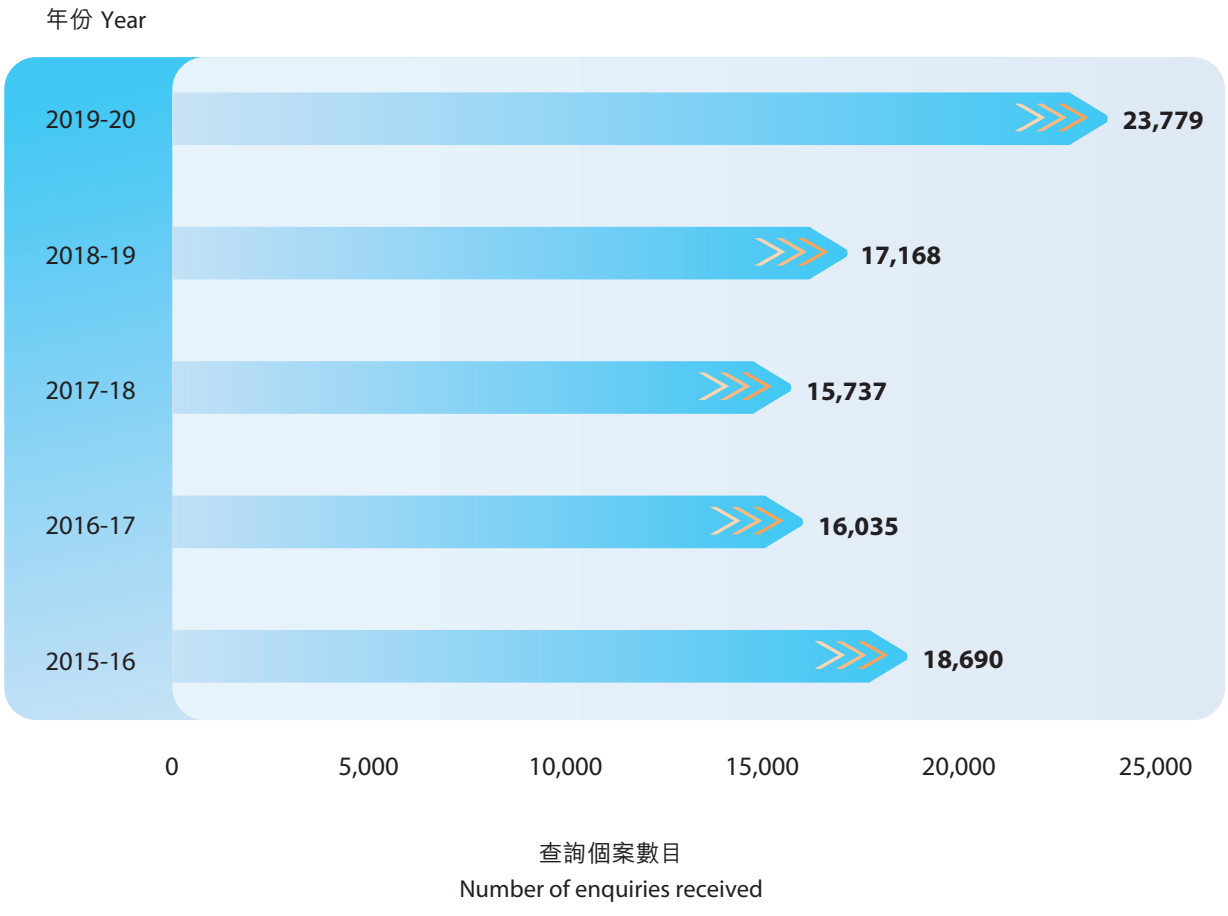
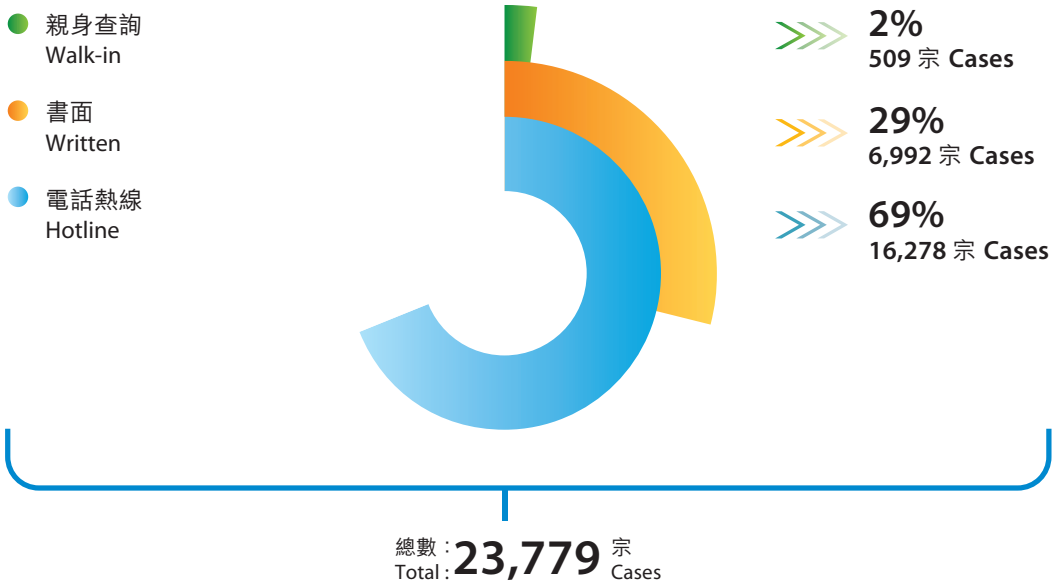


圖 5.2 – 提出查詢的途徑

Figure 5.2 – Means by which enquiries were made



調查投訴

投訴的整體趨勢

自2019年6月以來，社會事件帶來一些前所未有的挑戰，當中包括「起底」。「起底」涉及未經當事人同意而披露其個人資料以達致滋擾或恫嚇的目的，對受害人造成或可能造成心理或身體傷害及/或財產損害。在本報告年度，私隱專員共接獲及發現接近5,000宗有關「起底」及網絡欺凌的個案，當中的受害人來自各行各業，包括政府官員、公眾人物、警察、教師及學生。因此，在本報告年度所接獲的投訴大增，創近年新高。

此外，值得留意的是，在本報告年度的下半年，由同一事件而衍生多宗或類似的投訴有上升趨勢，尤其是在2019年12月26日一名警務人員在鏡頭前展示一名記者的身份證的事件引起公眾廣泛關注，私隱專員接獲大量投訴。

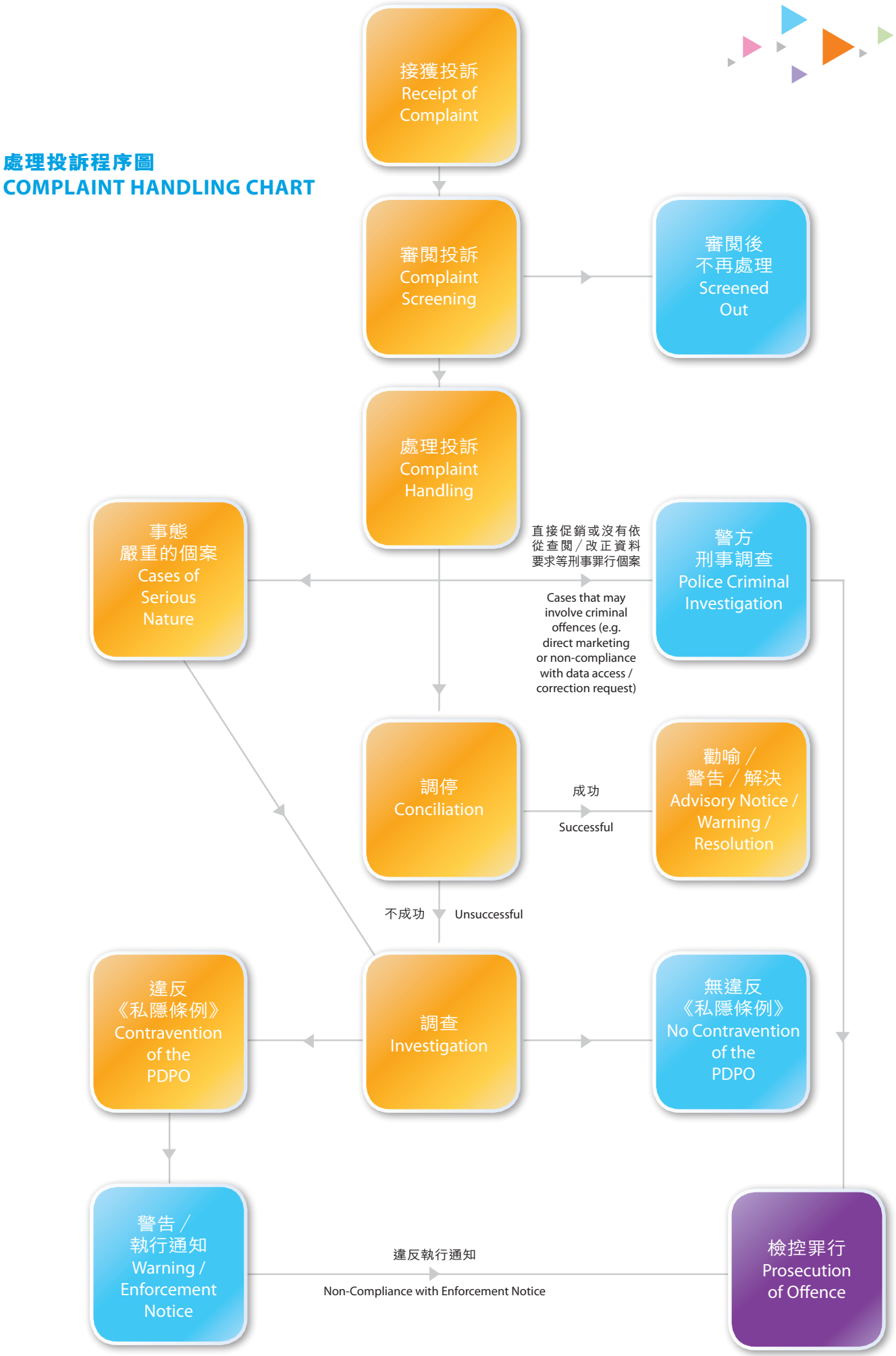
COMPLAINTS INVESTIGATION

Overall trend of complaints

Since June 2019, social incidents had given rise to some unprecedented challenges to our society, one of which being "doxxing". Doxxing involves non-consensual disclosure of an individual's personal information for the purposes of harassment or intimidation, thus causing or likely to cause psychological or bodily harm to the victims and/or physical damage to their properties. During the reporting year, PCPD received and discovered close to 5,000 cases relating to doxxing and cyberbullying, in which the victims came from all walks of life, including government officials, public figures, police officers, teachers and students. As a result, the number of complaints received during the reporting year increased significantly, reaching a record high in recent years.

It is also worth noting that there had been a rising trend of multiple or similar complaints in the second half of the reporting year. In particular, the incident of a police officer showing a reporter's Hong Kong Identity Card before camera on 26 December 2019 caused widespread public concern and a huge influx of complaints to PCPD.

處理投訴程序圖
COMPLAINT HANDLING CHART



接獲的投訴個案

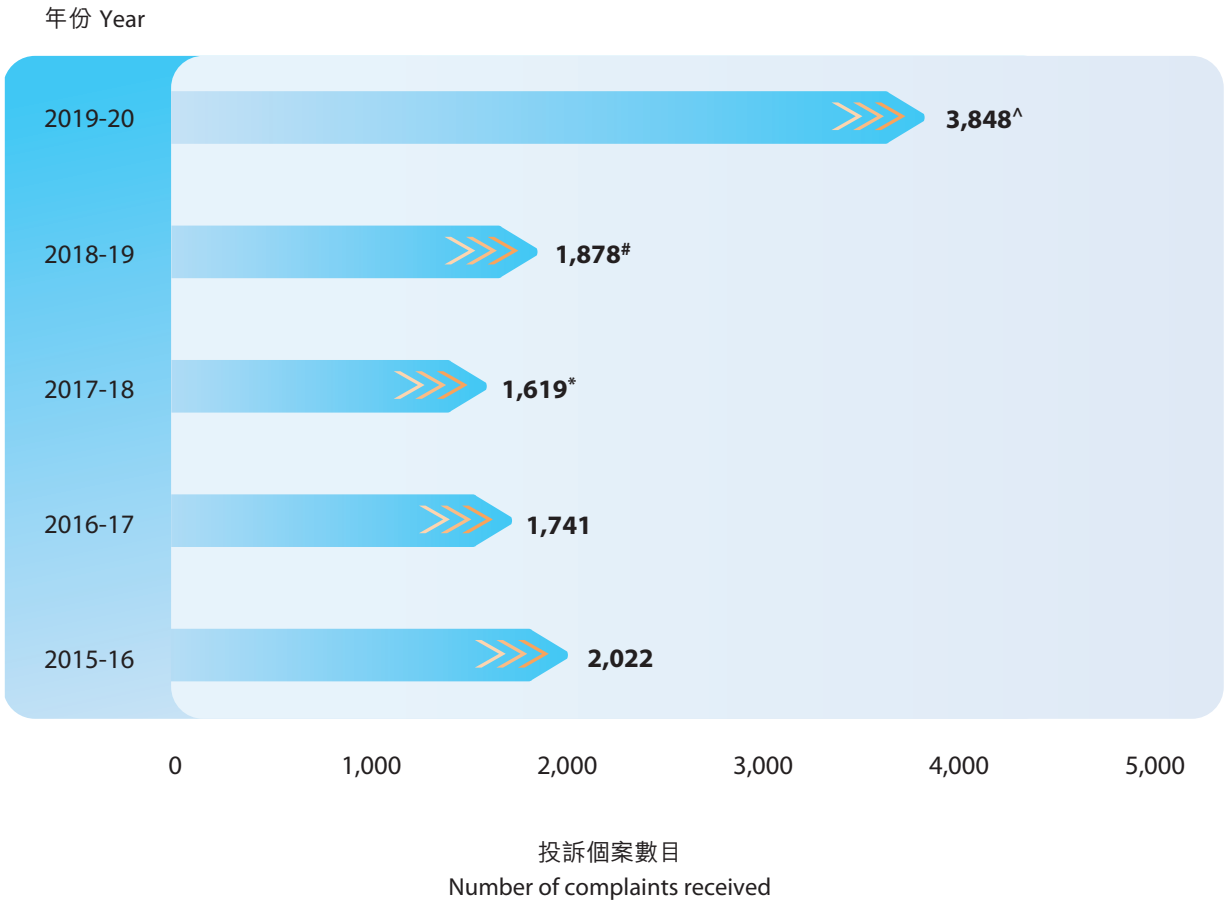
私隱公署在本報告年度共接獲11,220宗投訴，當中包括4,707宗由社會事件持不同意見而引發的「起底」和網絡欺凌的投訴，及醫護人員被「起底」的投訴(「起底」個案)(詳見第57頁)，以及2,665宗有關兩宗警務人員在鏡頭前展示記者身份證的事件的投訴。撇除「起底」個案及以上兩宗事件，公署在本報告年度接獲3,848宗投訴，較上一年度上升105%。(圖5.3)

圖 5.3 - 投訴個案數目

Complaints received

11,220 complaints were received in 2019-20, which included 4,707 complaints relating to doxxing and cyberbullying arising from divergent opinions in social incidents and doxxing of medical personnel (the doxxing cases) (see P.57 for details), and 2,665 complaints relating to two incidents of police officer showing a reporter's Hong Kong Identity Card before camera. Discounting the doxxing cases and the two incidents above, PCPD received 3,848 complaints in 2019-20, being a 105% increase from last year. (Figure 5.3)

Figure 5.3 – Number of complaints received



^ 當中包括428宗有關一名藝人在社交平台披露一份機組人員名單的投訴；669宗有關一名保安人員涉嫌偷取居民信件的投訴。

\# 當中包括143宗有關一間航空公司外洩客戶個人資料事件的投訴。

* 為統計目的，私隱公署在該報告年度收到有關某政府部門遺失載有選民個人資料的手提電腦的1,944 宗同類投訴，只作一宗投訴計算。

^ 428 complaints were about the disclosure of a list of operating cabin crew by an artist on her social media platform. 669 complaints were about suspected theft of residents' letters by a security guard.

\# 143 complaints were about an airline company's data leakage incident.

* For statistical purpose, the 1,944 complaints received in relation to the loss of notebook computers of a government department that contained personal data of registered electors were counted as one complaint.

被投訴者類別

在接獲的3,848宗投訴個案中，被投訴者可分為以下類別：

- 私營機構（2,071宗），主要涉及：物業管理公司、銀行及財務公司，以及教育機構；
- 個人（1,210宗）；及
- 政府部門及公共機構（567宗），主要涉及：醫院或醫療機構，負責運輸事宜的部門，以及負責學生資助事宜的部門。（圖5.4）

圖 5.4 – 被投訴者類別

Types of parties being complained against

Among the 3,848 complaints received, the types of parties being complained against were as follows:

- private organisations (2,071 cases), with the majority including property management companies, banking and finance institutions and education institutions;
- individuals (1,210 cases); and
- government departments and public organisations (567 cases), with the majority concerning healthcare services institutions, departments handling transport matters and students' finance matters. (Figure 5.4)

Figure 5.4 – Types of parties being complained against

就違反《私隱條例》的投訴指稱

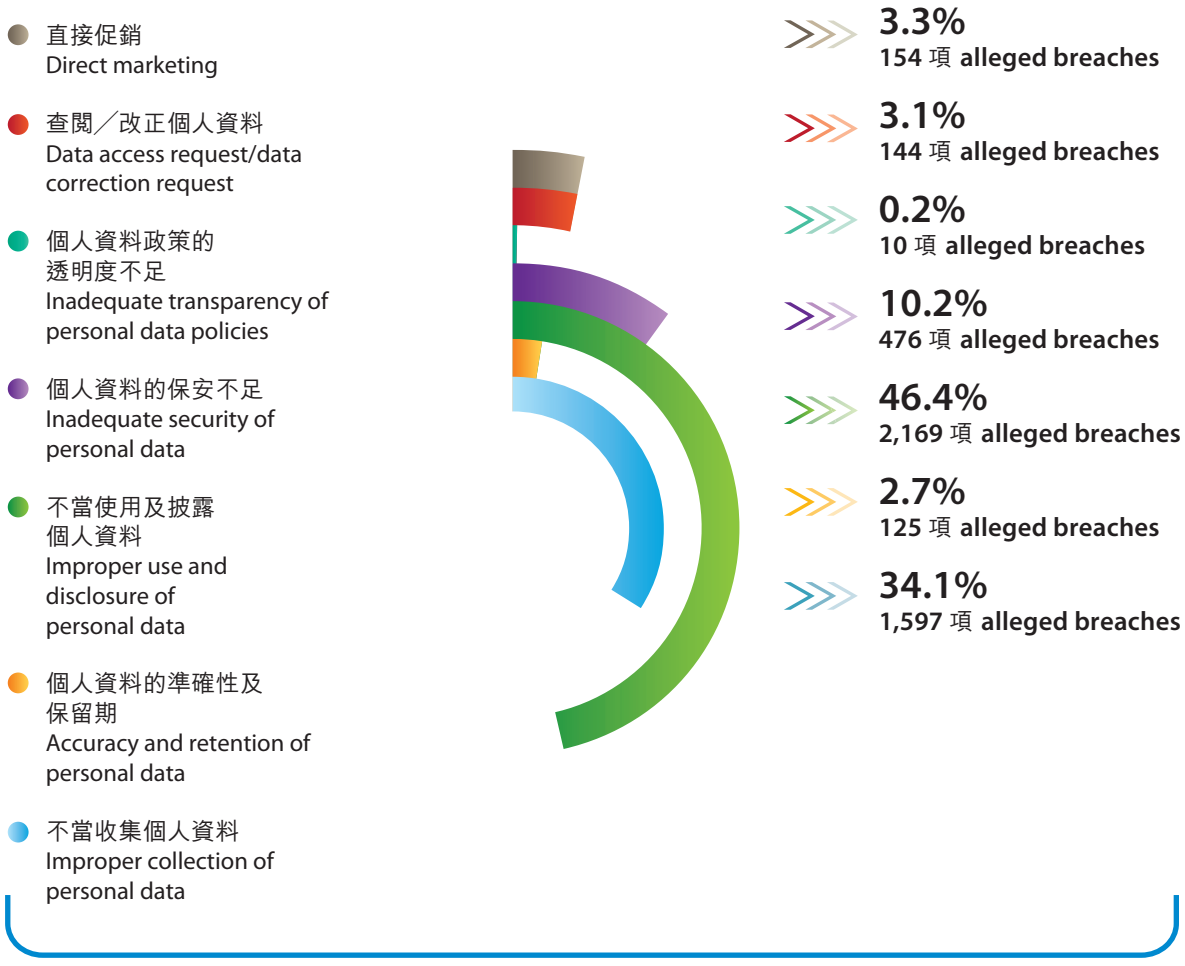
在本報告年度內接獲的3,848宗投訴中，共涉及4,675項違反《私隱條例》規定的指稱（同一宗投訴個案可涉及多於一項指稱），該些投訴指稱見圖5.5。

圖 5.5 – 就違反《私隱條例》的投訴指稱

Nature of alleged breaches under the PDPO

The 3,848 complaints involved a total of 4,675 alleged breaches under the PDPO (one complaint case may have 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，私隱公署於本報告年度收到的投訴中，與資訊科技及物業管理有關的分別大幅增加了124%及677%。（圖5.6）

有關資訊科技的投訴中，大部分是關於網上社交網絡及智能手機應用程式，相信這上升趨勢與形式多樣的網上社交網絡普及化有關，因為它不但可作為個人分享渠道，更兼具新聞及購物平台功能。

涉及物業管理事宜的投訴大增，主要是因為一宗有關一名保安人員涉嫌偷取居民信件的事件而衍生多宗投訴。

Major subjects of complaints

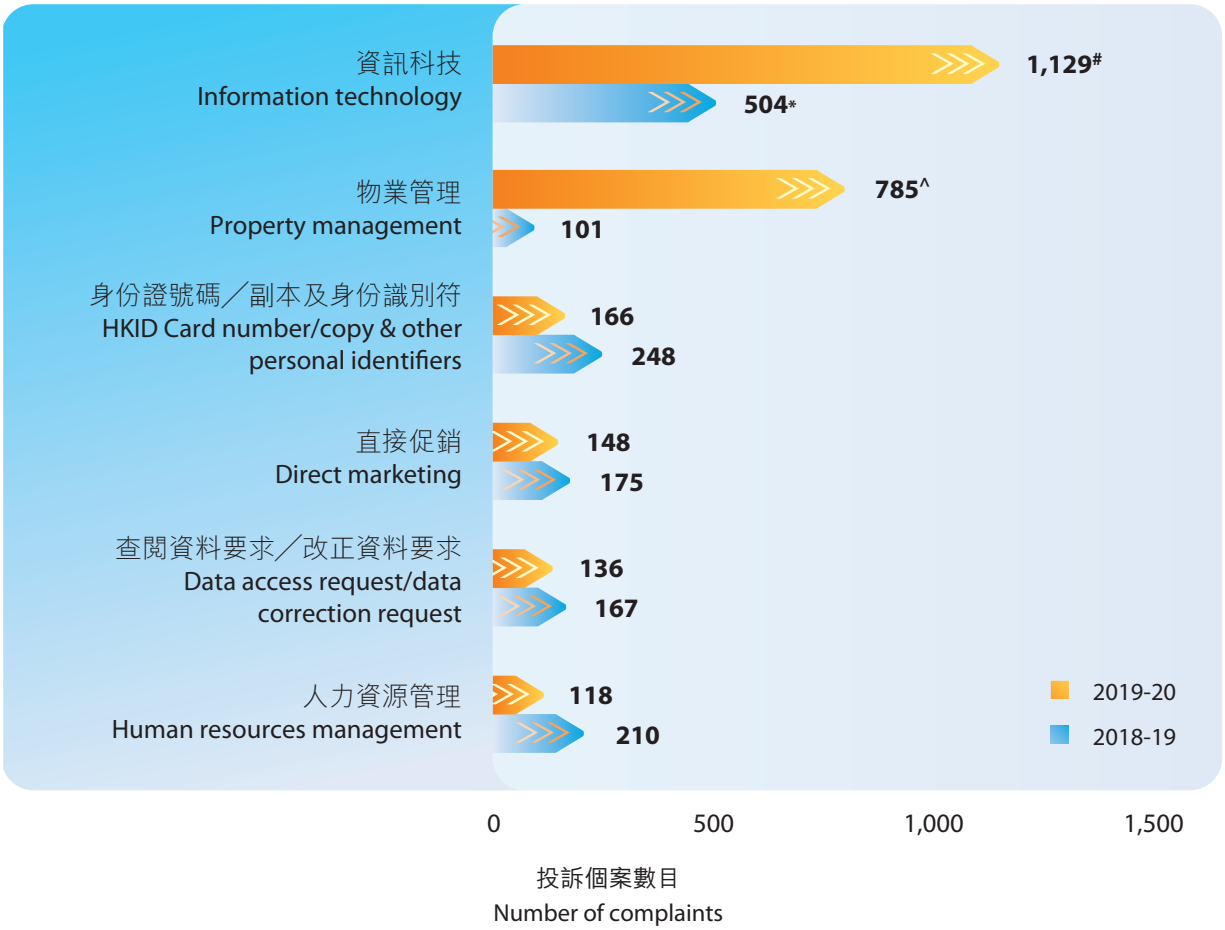
Compared to the previous reporting year, the number of complaints received by PCPD during the reporting year relating to information technology and property management-related issues significantly increased by 124% and 677% respectively. (Figure 5.6)

As for the complaints relating to information technology, the majority of them were about online social networks and smartphone applications. Understandably, the rising trend can be explained by the popularity of online social networks which have now served not only as a personal sharing channel, but also as a multi-functional platform for news activity and shopping.

The upsurge of complaints about property management-related issues was mainly due to the multiple complaints regarding suspected theft of residents' letters by a security guard.

圖 5.6 – 投訴所涉的主要範疇

Figure 5.6 – Major subjects of complaints



當中包括428宗有關一名藝人在社交平台披露一份機組人員名單的投訴。

* 當中包括143宗有關一間航空公司外洩客戶個人資料事件的投訴。

^ 當中包括669宗有關一名保安人員涉嫌偷取居民信件的投訴。

428 complaints were about the disclosure of a list of operating cabin crew by an artist on her social media platform.

* 143 complaints were about an airline company's data leakage incident.

^ 669 complaints were about suspected theft of residents' letters by a security guard.

年度投訴摘要

在本報告年度，私隱公署處理了292宗承接上年度的投訴，加上新接獲的11,220宗投訴（包括4,707宗「起底」和2,665宗有關兩宗警務人員在鏡頭前展示記者身份證的事件的投訴），年內共須處理11,512宗投訴。在這些個案中，10,042宗（87%）在本報告年度內經已完結，而餘下的1,470宗（13%），截至2020年3月31日仍在處理中。（圖5.7）

Summary of complaints handled during the reporting year

During the reporting year, PCPD handled 11,220 newly received complaints (including 4,707 complaints about doxxing and 2,665 complaints about the two incidents of police officer showing a reporter's Hong Kong Identity Card before camera), and 292 complaints carried forward from the previous reporting year, bringing the total number of complaints handled during the reporting year to 11,512. Of these, 10,042 (87%) were completed during the reporting year, and 1,470 (13%) were still in progress as at 31 March 2020. (Figure 5.7)

圖 5.7 – 過去五個年度投訴摘要

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

	2019-20	2018-19	2017-18	2016-17	2015-16
承接上年度的投訴 Complaints carried forward	292	191	193	262	253
接獲的投訴 Complaints received	11,220	1,878	1,619	1,741	2,022
共須處理的投訴 Total complaints processed	11,512	2,069	1,812	2,003	2,275
已完結的投訴 Complaints completed	10,042	1,777	1,621	1,810	2,013
未完結的投訴 Complaints under processing	1,470	292	191	193	262

已完結的投訴個案分類

在本報告年度內已經完結的10,042宗投訴，當中包括4,232宗有關「起底」個案的投訴及2,648宗有關兩宗警務人員在鏡頭前展示一名記者的身份證的投訴。撇除「起底」個案及上述事件，私隱公署在本報告年度完結的投訴宗數為3,162宗，當中1,412宗經公署初步審研後，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屬匿名投訴等；

(ii) 投訴人撤回投訴；

(iii) 私隱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1,750宗個案獲私隱公署接納作進一步處理。（圖5.8）

圖5.8 – 已完結的投訴個案分類

Categorisation of completed complaints

10,042 complaints were completed during the reporting year, including 4,232 complaints relating to doxxing and 2,648 complaints relating to the two incidents of a police officer showing a reporter's Hong Kong Identity Card before camera. Taking out the doxxing cases and the incidents above, PCPD completed 3,162 complaints in 2019-20, of which 1,412 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 PDPO. For instance, the matters complained of did not involve "personal data". 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 PCPD's requests for further evidence in support of their allegations;

(iv) the matters complained of were outside the jurisdiction of the PDPO; or

(v) no *prima facie* evidence of contravention.

The remaining 1,750 complaints were accepted for further handling. (Figure 5.8)

Figure 5.8 – Categorisation of completed complaints

私隱公署處理投訴的方式

就該1,750宗獲私隱公署接納作進一步處理的投訴，公署先以調停這種較便捷的方式，嘗試解決資料當事人與被投訴者之間的糾紛。當中1,582宗（90%）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) 私隱公署向投訴人分析所有在案資料後，投訴人不再追究；或

(iii) 私隱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，私隱公署發現125宗投訴涉及刑事成份（當中115宗關於在網上披露車主的個人資料），在公署確立表面證據成立，及投訴人同意下，公署轉介有關個案（例如：未經資料當事人同意而使用其個人資料於直接促銷，或披露未經資料使用者同意而取得的個人資料的罪行）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 complaint handling

For those 1,750 complaints accepted for further handling, PCPD attempted to resolve disputes between the data subjects and the parties being complained against by conciliation as a speedy and convenient alternative. 1,582 complaints (90%) were successfully resolved (Figure 5.9) on the following grounds:

(i) remedial actions had been taken by the parties being complained against to resolve the problems raised by the complainants;

(ii) the complainants withdrew their complaints after PCPD had explained the information in hand to them; or

(iii) PCPD had conveyed the complainants' concerns to the parties being complained against for their follow-up actions.

125 complaints were found involving criminal nature (of which 115 were related to the disclosure of vehicle owners' personal data online). Those complaints were referred to the Police when *prima facie* evidence of contravention of the relevant requirements under the PDPO was established (e.g. offences for using personal data in direct marketing without consent from data subjects; or offences for disclosing personal data obtained without consent from data users) and the complainants' consent for referral was obtained.

Figure 5.9 – Complaints resolved by conciliation, referred to the Police and for investigation

餘下43宗的投訴因不適合或不能成功調停，而須展開調查，當中：

- 私隱公署要求11宗的被投訴者採取符合《私隱條例》規定的相應糾正措施，私隱公署並向部分被投訴者發出警告或執行通知。

- 餘下的32宗的被投訴者沒有違反《私隱條例》的規定，私隱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）

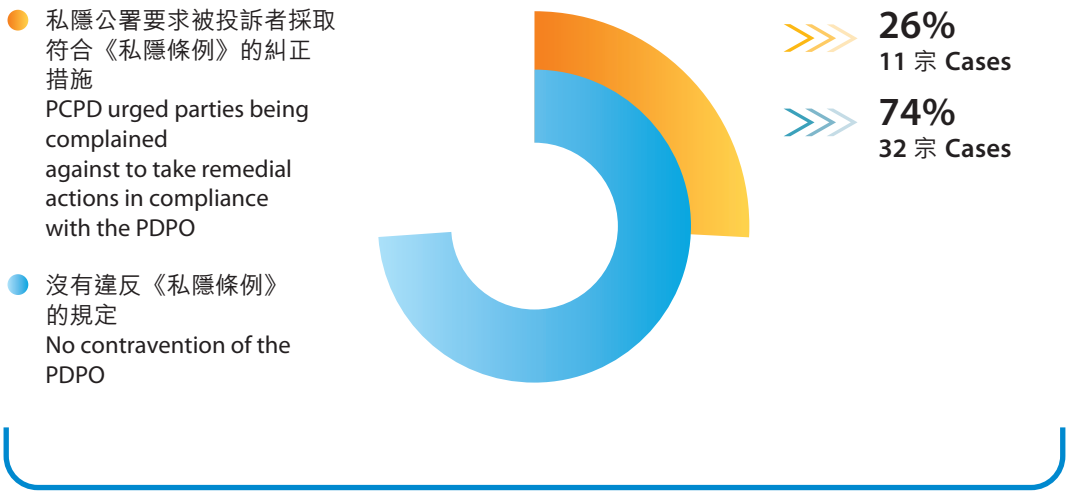
Investigations were carried out for the remaining 43 complaints, which were unsuitable for conciliation or not conciliated:

- in 11 complaints, PCPD had urged the parties being complained against to take remedial actions in order to comply with the requirements of the PDPO. Some of them were issued with warnings and Enforcement Notices by PCPD;

- no contravention of the PDPO was found in the remaining 32 complaints. Recommendations were given to some of the parties being complained against to encourage them to establish good practices 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



私隱公署給予被投訴者的建議

私隱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900項建議，要求他們：

- 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
- 跟進私隱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, PCPD also, in some cases, advised the 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, or encourage them to establish good practices in personal data protection. During the reporting year, more than 900 recommendations were made to the parties being complained against to advise them to take the following actions:

- revising personal data-related policies and practices to prevent similar breaches in future;
- providing proper guidance to staff to require compliance with relevant policies and practices;
- supplying/correcting personal data to comply with the complainants' data access/correction requests, or reducing the fees for complying with the data access requests;
- deleting personal data that was collected or disclosed to third parties unnecessarily;
- undertaking to cease the malpractices leading to the complaints;
- complying with opt-out requests for not receiving direct marketing messages; and
- following up on the privacy-related concern of the complainants as referred by PCPD.

對「起底」個案的跟進行動

在4,707宗「起底」個案中，有1,402宗在公署進行初步調查後轉介警方跟進。公署運用《私隱條例》所賦予的權力跟進所有「起底」個案，並取得成果。跟進行動包括去信促請有關網上平台移除網絡連結，並把涉嫌違反法庭禁制令的個案轉介律政司跟進（44宗）。公署曾166次去信16個網上平台，促請它們移除2,867條非法的網絡連結。1,777條網絡連結（62%）其後被移除。

在本報告年度，公署已經完成審閱及調查約九成接獲的「起底」個案（4,232宗）。

私隱公署要求移除非法的網絡連結（共2,867條）的結果

Follow-up actions on doxxing cases

Of the 4,707 doxxing cases, 1,402 cases were referred to the Police to follow up after preliminary investigation by PCPD. PCPD followed up on all doxxing cases with the powers conferred by the PDPO and yielded results. Follow-up actions included writing to the online platforms concerned urging the removal of the web links, and referring cases of suspected violations of court injunction orders to the Department of Justice to follow up (44 cases). PCPD wrote 166 times to 16 online platforms, urging them to remove a total of 2,867 illegal web links. 1,777 web links (62%) were subsequently removed.

During the reporting year, PCPD completed screening and investigation of about 90% (4,232 cases) of the doxxing cases received.

Results of PCPD's removal requests on illegal web links (2,867 web links in total)

「起底」個案的審閱及調查（截至2020年3月31日）

Progress of screening and investigation of doxxing cases as of 31 March 2020

個案選錄 · 以作借鑑

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私隱影響。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。

私隱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，可以令不當處理個人資料的方式得以修正，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，提升企業尊重個人資料的意識，在日常業務中實踐數據道德，而市民可了解其個人資料私隱的權利。

SUMMARIES OF SELECTED CASES • LESSONS LEARNT

Companies and organisations are under ethical obligations to carefully consider the possible privacy impact on the data subjects when using personal data for their businesses or services. The following selected cases illustrate how individuals' dignity, right and interest might be affected by having their personal data privacy intruded.

If complaints are substantiated, PCPD would recommend the companies or organisations take corrective or remedial actions. The correction of malpractices in handling personal data by companies or organisations, as a result of the complaints raised by data subjects, can eventually benefiting the community at large. By publishing these case summaries, we wish to provide data users with good lessons to learn, raise the organisational awareness of respecting personal data and applying data ethics in daily businesses, and to enhance citizens' understanding of their personal data privacy rights.

個案一：法團在社交平台披露一名業主的姓名及住址 – 保障資料第3原則

投訴內容

投訴人是一屋苑單位業主。投訴人就其單位的滲水問題入稟小額錢債審裁處，向該屋苑的業主立案法團（「法團」）提出索償。法團為了通知其他業主此事，將投訴人向小額錢債審裁處提交的申索書副本張貼在屋苑大堂及上載到由該屋苑業主組成的網上社交平台群組。

由於該申索書載有投訴人的姓名及完整住址資料，投訴人向私隱公署投訴法團在未得他同意下公開披露他的個人資料。法團其後將張貼在屋苑大堂的該申索書移除，但仍在該網上社交平台群組披露該申索書。

法團在回覆私隱公署的查問時表示，法團是根據《建築物管理條例》第26A條的規定，通知全體業主法團將進入法律程序，而須公開訴訟各方的身份、案件編號、審理案件的法院、案件性質，及申索的金額或尋求的補救。

結果

私隱公署注意到，《建築物管理條例》只要求法團在相關的建築物展示載有法律程序的詳情的通知，當中並無明文規定法團須展示有關法律文件的全部內容。該條例亦無明文規定法團須在相關建築物以外的地方或平台（如網上社交平台）展示有關通知。再者，根據民政事務總署發出的《〈建築物管理條例〉（第344章）常見問題》的書刊，法團須展示的法律程序的詳情只包括涉及法律程序的各方的身分，當中並無要求法團須披露訴訟各方的姓名及其聯絡資料。

Case 1: An Incorporated Owners (IO) disclosed an owner's name and address on social network platform - DPP3

The complaint

The complainant was a flat owner of a private housing estate. The complainant made a claim to the Small Claims Tribunal against the IO of the estate in respect of a water seepage problem of his flat. In order to notify other owners of the case, the IO posted a copy of the complainant's claim form filed to the Small Claims Tribunal at the lobby of the estate and uploaded it onto an online social platform composing of the owners of the estate.

Since the claim form contained the complainant's name and full address, the IO's act had disclosed the complainant's personal data without his consent. The complainant then lodged a complaint with PCPD against the IO. The IO had subsequently removed the claim form posted at the lobby, but refused to remove the one posted on the online social platform.

In response to PCPD's inquiry, the IO stated that it had to notify all the owners of the legal proceedings to which the IO was a party in accordance with section 26A of the Building Management Ordinance (BMO). The IO insisted that information about the capacity of the parties of the proceedings, case number, the forum of the case, nature of the case and the amount claimed or remedies sought must be disclosed.

Outcome

PCPD noted that the BMO only requires the IO to display a notice containing particulars of the proceedings in the building. There is no provision requiring the IO to display all the content of the legal documents, nor any provision requiring the IO to display the notice in places outside the building (e.g. online social platform). Moreover, according to the publication "Frequently Asked Questions on Building Management Ordinance (Cap. 344)" issued by the Home Affairs Department, the particulars of proceedings that must be displayed include only the capacity of the parties of the proceedings but not the names and contact information of the parties.

私隱公署認為，就達致通知業主有關訴訟的目的而言，法團只須向各業主述明有一單位業主（即：投訴人的身分）入稟小額錢債審裁處向法團提出申索。就此，法團將載有投訴人的姓名及完整住址的該申索書上載到該網上社交平台群組，是不必要地披露了投訴人的個人資料，違反了保障資料第3原則的規定。

儘管私隱公署已作出勸喻，但法團仍未從該網上社交平台群組移除該申索書。因此，公署向法團發出執行通知，指令法團：(1)從該網上社交平台群組移除該申索書，或在該申索書中刪除所有與投訴人有關的個人資料；(2)制定相關政策、行事方式及/或指引，以規定法團及其委員會成員，除非事先得到資料當事人的同意，否則在公開披露法庭文件前，必須先將可識辨涉事當事人的個人資料從有關文件中刪除；(3)將上述政策、行事方式及/或指引發布給所有法團委員會成員；(4)採取適當措施，以確保法團新一屆的委員會成員獲悉有關政策、行事方式及/或指引。

借鑑

物業管理團體在履行物業管理職責時，必須保障及尊重住戶的個人資料。私隱公署發出的《物業管理指引》指出，雖然物業管理團體可能會公開張貼通告以通知業主有關大廈的管理事宜，但物業管理團體應仔細考慮及衡量公開個別人士的資料之必要性及程度。與張貼目的無關而非必需的個人資料應從通告上略去。過度披露個人資料或別有用心地將文件公開展示，可能會違反《私隱條例》保障資料第3原則的規定。

PCPD deemed that for the purpose of notifying the owners of the proceedings, the IO only needed to mention that an owner of a flat (i.e. the capacity of the complainant) had made a claim to the Small Claims Tribunal against the IO. Hence, the IO's act of uploading the claim form containing the complainant's name and full address to the online social platform was unnecessary disclosure of the complainant's personal data, contravening the requirements of DPP3.

PCPD had requested the IO to remove the claim form from the online social platform, but the IO did not accede to the request. An Enforcement Notice was eventually served on the IO, directing it to (1) remove the claim form from the online social platform, or delete the complainant's personal data on the claim form; (2) formulate policies, practices and/or guidelines requiring the IO and its committee members to delete information which could identify data subjects from any legal documents before disclosing the documents, unless prior consent of the data subject had been obtained; (3) disseminate the policies, practices and/or guidelines above to all the committee members of the IO; (4) adopt proper measures to ensure that future committee members of the IO know the policies, practices and/or guidelines.

Lesson learnt

When performing their duties, property management bodies must protect and respect residents' personal data. PCPD's Guidance on Property Management Practices pointed out that although property management bodies may have to inform owners of building management affairs by displaying notices in public, property management bodies should carefully consider and assess the necessity and extent of publishing individual's personal data. Personal data which is not necessary for the purpose of posting the notice must be edited out. Excessive disclosure of personal data or public display of a document with an ulterior motive may contravene DPP3 of the PDPO.

個案二：制服團體收集未成年人士的個人資料作招募團員之用 – 保障資料第 1(2) 原則

投訴內容

投訴人指稱一個制服團體在公開招募青少年團員的活動中，使用威嚇手法，迫使沒有成人陪同的青少年提供他們及父母的個人資料，強行為他們申請入團。

該團體向私隱公署強調，招募活動現場備有宣傳單張等物品，向在場人士解釋招募活動的用意，申請入隊必須出於申請人的意願。根據該團體的既定招募程序，如有12至17歲的青少年有意申請入隊，需要自行填寫申請書。申請人只需填寫本人的基本個人資料，以供該團體初步核實年齡資格，以及安排申請人與家長或監護人共同出席面試。在面試當日，申請人會在家長或監護人陪同下，補回表格上尚未填寫的資料及證明文件。該團體承認在招募時，他們不會主動向青少年解釋上述情況，故部分沒有家長或監護人陪同的青少年，或會在申請書上填寫家長或監護人的個人資料。

結果

私隱公署在審視該團體的上述招募方式後，不認為做法構成以不公平方式收集個人資料，而公署在個案中並無發現任何資料顯示該團體涉及強迫申請人提供個人資料，以致涉及違反保障資料第1(2)原則的規定。不過，公署認為，向青少年收集個人資料，涉及較重大的私隱關注。該團體有責任向青少年解釋清楚填寫表格的要求，避免青少年在入表階段，在家長或監護人不知情下填寫他們的個人資料。

Case 2: A uniform group collected minors' personal data for recruitment of group members - DPP1(2)

The complaint

The complainant alleged that in an activity organised by a uniform group, teenagers who were not accompanied by adults were forced to apply for admission to the group, and provide their and their parents' personal data in an application form .

In replying to PCPD, the group stated that recruitment leaflets distributed onsite emphasised that all applications should be made on the applicants' own will. The group stated that applicants between 12 and 17 of age only needed to fill in their own particulars for preliminary verification of their age and arrangement for interview with the applicants and their parents at a later stage. On the interview day, the applicants accompanied by their parents would then complete the remaining parts of the application form. The group admitted that they did not explain to the applicants this arrangement during the activity. They believed that some teenage applicants might have filled in the personal data of their parents in the application forms without consulting their parents.

Outcome

After examining the recruitment practices of the group, PCPD did not consider that the group had collected personal data in an unfair manner, and there was no evidence showing that the group had forced applicants to provide personal data, thereby contravening DPP1(2). However, PCPD was of the view that collection of personal data from teenagers involved great privacy concerns. It was the responsibility of the group to clearly explain the requirements of completing the application form to teenagers so that they would not provide the personal data of their parents without their knowledge.

經私隱公署介入後，該團體同意改善招募安排，向有意申請的青少年提供書面填表指示，清晰標示需填寫的項目。該團體已要求主管在招募活動前向當值隊員清晰講解，並透過加強巡查以確保新安排得以落實。

After PCPD's intervention, the group agreed to improve the recruitment arrangement by providing written instructions on the items that needed to be filled in at the initial application stage. The group had requested its supervisors to clearly brief duty officers before recruitment activities and increase the frequency of inspection to ensure the implementation of the new arrangement.

借鑑

在日常生活中，無論是成年人或青年人，都總有機會面對需要提供個人資料的處境。由申請成為商戶會員享受購物優惠，以至開設網上帳戶進行網上活動，都涉及提供個人資料。

社會有責任保護閱歷尚淺的青年人避開私隱陷阱。所有向青少年收集個人資料的資料使用者，應以此案為鑑，因應青少年的心智成熟程度，本著尊重、互惠和公平的價值觀，制定適切的收集個人資料安排，只收集足夠而不超乎適度的個人資料，同時以易於理解的方式向青少年解釋收集資料的原因。此外，前線人員在與青少年溝通時，亦必須謹言慎行，注意說話方式及內容，避免令青少年感到受壓及產生誤會，以確保青少年可自由自主地決定是否提供個人資料。

Lesson learnt

In our daily lives, there are many situations, from application for membership of loyalty programmes to application for online accounts, that require us, no matter adults or minors, to provide personal data.

The community has the duty to protect minor's privacy rights from being infringed on. All data users collecting personal data from minors should learn from this case. They should make appropriate arrangements for collecting personal data in a respectful, mutually beneficial and fair manner, the maturity of subjects considered. Only adequate (but not excessive) personal data should be collected and the purpose of collection should be explained in an easily understandable way. Moreover, when communicating with minors, frontline officers should be mindful of their presentation and choice of words to avoid leaving them under the impression that they are pressurised to provide their personal data.

個案三：僱員透過查閱資料要求向僱主查詢他是否被視為具潛質的員工 – 保障資料第6原則

投訴內容

為確保內部升遷交接暢順，一機構的管理層決定物色具潛質的員工，以專注培訓他們將來出任管理人員或其他重要職位。因此，該機構內部製備了一份具潛質的員工名單供管理層考慮，但該名單內容沒有對外公佈。

投訴人向該機構遞交一份查閱資料要求表格，要求該機構確認「他的姓名是否在該份具潛質的員工名單上」。由於該機構的政策是不會向員工披露他是否被管理層視為一名具潛質的員工，該機構沒有回覆投訴人的要求。投訴人遂向私隱公署投訴該機構未有依從其查閱資料要求。

結果

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，法官表示《私隱條例》的原意為保障個人資料私隱，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資料使用者作出更正。

Case 3: An employee made a data access request to his employer with an intention to find out whether he was considered having potential - DPP6

The complaint

An organisation had conducted an exercise to identify staff having potential so that appropriate training would be provided to them to prepare them to assume management roles or other important positions in the future. A classified list of staff having potential was therefore compiled and passed to the organisation's management for consideration.

The complainant submitted a data access request to the organisation requesting it to confirm "whether his name was on the list of the staff having potential". As the list was a classified document of the organisation, no reply was given to the complainant. The complainant then complained against the organisation for failing to comply with his data access request.

Outcome

In the judicial review case of *Wu Kit Ping v. Administrative Appeals Board* HCAL 60/2007, the Judge held that the purpose of the PDPO is to protect the personal data privacy of an individual, and to enable an individual to access, and correct the incorrect personal data held by a data user.

在本個案中，投訴人提出查閱資料要求的目的，並不是查閱該機構持有與他有關的僱傭紀錄（例如他的履歷資料、工作表現報告、培訓紀錄或申領假期/員工福利紀錄等），而是希望得悉他是否被管理層視為一名具潛質的員工。私隱公署認為，投訴人的要求與他的個人資料私隱無關。投訴人在《私隱條例》下只可查閱該機構是否準確地記錄他的個人資料，以及在發現不準確時要求僱主作出更正。該機構在《私隱條例》下沒有責任向投訴人確認「他的姓名是否在該份具潛質的員工名單上」。

In this case, the complainant's purpose for making the data access request was not to access his employment-related data held by the organisation (e.g. his resume, performance appraisals, training records or applications for leave/staff benefits records, etc.), but to find out whether he was considered as a staff member having potential. PCPD considered that the complainant's request was not related to his personal data. Under the PDPO, the complainant had the right to access his personal data held by the organisation to ascertain if it was accurate, and if it was inaccurate, he could request his employer to correct it. The organisation had no duty under the PDPO to confirm to the complainant "whether his name was on the list of staff having potential".

借鑑

《私隱條例》賦予僱員向僱主查閱其個人資料的重要權利，而僱主作為資料使用者亦須按法例規定妥善處理僱員的查閱資料要求。然而，僱員可能會誤會《私隱條例》下賦予他們有關權利的用意，以為這權利等同於一項絕對的知情權，可用作要求僱主回答所有與僱員有關的問題，或為僱員編寫指定形式的報告或信件等（例如要求僱主提供離職證明信）。事實上，查閱個人資料的權利在於讓個人知悉某資料使用者是否持有他的個人資料，並在認為他的個人資料不準確時，有權向資料使用者提出改正資料要求。因此，僱員不應期望可透過行使查閱個人資料權利以找尋資料作檢視僱主的行政安排或管理決定，亦不應利用此權利解決僱傭糾紛。

Lesson learnt

The PDPO provides an important right to employees to access their personal data, and employers as data users are obligated to handle data access requests in accordance with the PDPO. However, employees may misunderstand that the right given to them under the PDPO is an absolute right to information and they can use it to fish for answers in employment-related matters, or to obtain reports or letters in specified format (e.g. requesting employers to provide reference letters). In fact, the right to making data access requests 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 inaccuracy is noted. Employees should not expect to obtain information for checking the employer's administrative arrangements or management decisions, or for resolving employment disputes by exercising their right of data access request.

個案四：透過具容貌識辨功能的攝影機作職員考勤及保安用途 – 保障資料第 1 原則

投訴內容

投訴人是一名教師。他不滿其學校在他不知情及未取得其同意的情況下，於校門位置安裝了一部具容貌識辨功能的攝影機，作職員考勤及保安之用。

結果

就收集生物辨識資料方面，私隱公署認為，鑑於生物辨識資料屬性質敏感的資料，資料使用者須首先考慮有關收集是否必需的。因此，資料使用者須考慮可否收集敏感性較低的資料，但仍能達致相同效果的做法。此外，收集資料的方法亦必須在公平的情況進行，故資料使用者須確保已給予資料當事人自主及知情的選擇。

在本個案中，私隱公署在了解事件後，得知校方在保安方面，已於校門裝有閉路電視系統，亦有安排保安員駐守。在考勤方面，校方亦要求教師以門禁卡進出。此外，校方看來並沒有就透過該攝影機收集僱員容貌資料一事給予僱員自主及知情的選擇。

Case 4: Use of camera with facial recognition function for attendance recording and security purpose - DPP1

The complaint

The complainant was a teacher. He was dissatisfied that his school installed a camera with facial recognition function at the school entrance for employee attendance recording and security purpose without notifying him and obtaining his consent.

Outcome

On collection of biometric data, PCPD is of the view that biometric data is sensitive data and data users must first consider the necessity of collecting such data. Data users must consider whether it is feasible to collect less sensitive data to achieve the same purpose. The means of collection must be fair in the circumstances, so data users have the obligations to ensure that data subjects are given a free and informed choice to choose whether to have their biometric data collected.

In this case, PCPD learnt that for security purpose, a closed-circuit television system had already been installed at the school entrance with a security guard stationed there. For attendance recording purpose, teachers were required to use access cards to enter and leave the school. PCPD also noted that the school had not given its employees a free and informed choice on the collection of their facial images by the camera.

雖然該校表示安裝該攝影機只屬測試性質，其後亦已移除該攝影機，惟私隱公署認為，即使有關的安裝只屬測試性質，校方仍須在處理收集生物辨識資料方面符合私隱保障的規定。就此，私隱公署促請該校日後如涉及收集僱員的生物辨識資料，必須三思此舉可否以其他較不侵犯私隱的方法取代，並制訂有關的私隱政策，以緊遵《私隱條例》的相關規定。

Although the school stated that the installation of the camera was just for trial testing and it had subsequently removed the camera, PCPD considered that the school still needed to comply with the privacy protection requirements on handling biometric data. PCPD strongly advised the school to consider whether there were any less privacy intrusive alternatives to the collection of employees' biometric data in future and to formulate privacy policies for compliance with the PDPO.

借鑑

在數碼世代下，以人工智能辨識被攝錄人士身份的技術日趨成熟，不少僱主希望將有關技術引入其業務，以達至加強保安及方便監察僱員考勤之用。然而，生物辨識資料（如DNA樣本、指紋、容貌等）是直接與個人有關，往往是獨一無二及不可改變。而當生物辨識資料與另一資料庫的個人資料連結，又或經整合和分析後，可直接或間接辨識個別人士的身份，屬《私隱條例》下的個人資料，受《私隱條例》所規管。

就如本個案，如僱主純粹希望加強保安及方便監察僱員考勤情況的話，僱主應先考慮採取其他私隱侵犯程度較低的方法來代替收集其生物辨識資料。僱主若不採取這些措施，他便須具備充分的理由方可如此收集僱員的生物辨識資料，亦應給予僱員機會選擇是否容許僱主收集或處理有關資料。僱主應以提高透明度及能理解性為大原則，以簡單易明的方式告知所有受影響僱員，才可與僱員建立信任。

科技及人工智能為市民大眾及機構帶來好處及便利是不用置疑的。然而，當相關技術涉及個人資料私隱的議題時，資料使用者便須在其帶來的好處及保障個人資料私隱之間取得平衡，在善用科技促進業務的同時，亦尊重他人的私隱權利。

Lesson learnt

In the digital era, the technology of using artificial intelligence to identify individuals is getting more sophisticated. Many employers may wish to use the technology for enhancing security and facilitating staff monitoring. Biometric data (e.g. DNA samples, fingerprints, facial features, etc.) is unique and immutable, and when it is consolidated and analysed, a particular individual can be directly or indirectly identified, so it is personal data under the PDPO and is regulated by the PDPO.

In this case, if the employer simply wanted to enhance security and facilitate monitoring of employees' attendance, the employer should first consider adopting other less privacy intrusive alternatives to the collection of biometric data. If employers do not adopt these alternatives, they must have overriding reasons to justify the collection of biometric data and provide their employees with a choice to allow such collection or handling of their biometric data. Based on the principles of enhancing transparency and explainability, employers should inform all the affected employees of collection of biometric data in a simple and easily understandable way to gain trust from them.

Undoubtedly, technologies and artificial intelligence bring forth benefits and convenience. However, when the technologies involve collection or use of personal data, data users must carefully strike a balance between the benefits and protection of personal data privacy. While technologies are being used to facilitate businesses, individuals' privacy right should also be respected.

個案五：銀行改善網上更新個人資料的版面，採取尊重私隱的設定以確保銀行在取得客戶真正的同意下才使用其個人資料作直接促銷 –《私隱條例》第 35C 條及第 35G 條

投訴內容

投訴人是某銀行的客戶，他透過網上銀行服務更新他的聯絡資料。投訴人在有關更新個人資料的版面上輸入他的新聯絡資料。該銀行在該版面上詢問客戶是否「不接受銀行使用客戶的個人資料作直接促銷」。由於投訴人早已書面向該銀行提出拒收直銷訊息要求，因此他認為沒有需要再於有關更新個人資料的版面上選取上述方格來向該銀行確認他不同意該銀行使用他的個人資料作直接促銷的意願。

由於投訴人在網上向該銀行遞交他的新聯絡資料時沒有同時選取「不接受銀行使用客戶的個人資料作直接促銷」的方格，因此該銀行當作他取消早前提交的拒收直銷訊息要求，並將投訴人視為同意該銀行使用其個人資料作直接促銷的客戶。該銀行其後向投訴人發出直接促銷電話，投訴人遂向私隱公署投訴該銀行未有依從他的拒收直銷訊息要求。

結果

私隱公署向該銀行重申投訴人不同意該銀行使用他的個人資料作直接促銷的意願，而該銀行亦確認不會再向投訴人發出直接促銷訊息。此外，公署促請該銀行檢視有關更新個人資料的版面設定，以確保客戶應獲清晰及真正的選擇，自行決定是否接受該銀行使用其個人資料作直接促銷。

Case 5: A bank improved its personal data update webpage by adopting a setting that respected privacy to ensure that the bank had obtained customers' valid consent before using their personal data for direct marketing - Sections 35C and 35G

The complaint

The complainant was a customer of a bank. He updated his contact information through its online banking service. When he input his new contact information on the personal data update webpage, he was asked whether he "do not accept the use of customer's personal data for direct marketing by the bank". As the complainant had previously made a written opt-out request to the bank, he believed that he did not need to tick the box to confirm that he did not consent to the use of his personal data for direct marketing by the bank.

As the complainant had not ticked the above-mentioned box, the bank considered that he had cancelled his previous opt-out request and regarded the complainant as a customer who consented to the use of his personal data for direct marketing. The bank later gave the complainant a direct marketing call. The complainant then complained to PCPD that the bank did not comply with his opt-out request.

Outcome

PCPD reiterated to the bank that the complainant did not consent to the use of his personal data for direct marketing by the bank, and the bank confirmed that no direct marketing message would be sent to the complainant anymore. Moreover, PCPD urged the bank to review its personal data update webpage to ensure that customers were given a clear and genuine choice to decide whether to accept the use of their personal data for direct marketing.

該銀行同意有關處理客戶拒收直銷訊息要求的流程設計應對客戶而言是公平及具透明度的。因此，該銀行改善了網上更新個人資料的版面，將本來供客戶選取「不接受銀行使用客戶的個人資料作直接促銷」的方格改為供客戶選取「接受銀行使用客戶的個人資料作直接促銷」的方格。如客戶未有選取「接受銀行使用客戶的個人資料作直接促銷」的方格，該銀行不會使用客戶的個人資料作直接促銷。

借鑑

雖然在《私隱條例》下，資料當事人「同意」資料使用者使用其個人資料作直接促銷的定義可包含資料當事人「表示不反對」，但要符合「表示不反對」的定義，資料當事人必須曾明確地表示他不反對資料使用者使用他的個人資料作直接促銷。換言之，對於早已向資料使用者提出拒收直銷訊息要求的客戶而言，即使他在資料使用者再次詢問他有關接受直接促銷的意願時選擇不回應，這亦不能隨便被推定為他「同意」銀行使用他的個人資料作直接促銷，或他希望取消早前的拒收直銷訊息要求。

機構透過網上或應用程式介面向客戶收集個人資料及讓他們選擇是否接受直接促銷訊息時，應採取「貫徹私隱的設計」，確保機構只會在已清晰通知客戶及取得真正的同意下，才收集和使用他們的個人資料作直接促銷之用。這不僅能贏取客戶的信任，更有助提升行業的專業形象及直銷的效用。

The bank agreed that the flow of handling customers' opt-out requests should be fair and transparent to the customers. Hence, the bank had improved the personal data update webpage by changing the wording of the box from "do not accept the use of customer's personal data for direct marketing by the bank" to "accept the use of customer's personal data for direct marketing by the bank". If customers did not tick the box of "accept the use of customer's personal data for direct marketing by the bank", the bank would not use their personal data for direct marketing.

Lesson learnt

Under the PDPO, a data subject's "consent" to the use of his personal data for direct marketing by data users can include the data subject's "indication of no objection". However, to satisfy the definition of "indication of no objection", the data subject must have expressly indicated that he does not object to the use of his personal data for direct marketing by data users. In other words, for a customer who has already made an opt-out request to the bank, even when the bank asks again if he would accept direct marketing and he does not respond, the bank cannot conveniently presume that he "consented" to the use of his personal data for direct marketing, or he wanted to cancel his previous opt-out request.

When collecting customers' personal data or allowing them to make an opt-in or opt-out choice online or through applications, organisations should adopt the Privacy-by-Design approach to ensure that organisations collect and use customers' personal data for direct marketing only when customers are clearly informed and their genuine consent is obtained. Thus, organisations not only win trust from customers, but also enhance their professional image in the industry, as well as the effectiveness of direct marketing.

個案六：僱主向全體員工披露獲考慮晉升的員工的詳細個人資料 – 保障資料第3原則

投訴內容

投訴人獲僱主考慮晉升。僱主除了成立遴選委員會以考慮投訴人是否適合晉升外，亦向全體員工徵詢他們對投訴人的工作表現的評價，並同時將投訴人的完整履歷資料及出生日期披露予全體員工作參考之用。

投訴人不滿僱主隨意披露他的個人資料，事前亦沒有取得他的同意，遂向私隱公署作出投訴。

結果

雖然該僱主聲稱向全體員工披露投訴人的個人資料是為了取得他們對投訴人的工作表現的評價，以考慮投訴人是否適合晉升，但就此目的而言，僱主可向與投訴人的工作崗位直接有關的員工（例如投訴人的上司及組員）了解投訴人的工作表現，而並沒有實際需要向全體員工披露投訴人的完整履歷資料及出生日期。因此，私隱公署認為，此舉涉及違反保障資料第3原則的規定。

Case 6: An employer disclosed to all staff the personal data of staff members who were considered for promotion - DPP3

The complaint

The complainant was considered for promotion by his employer. In addition to setting up a selection board for considering the suitability of the complainant, the employer also consulted all staff about the work performance of the complainant and disclosed the full resume and date of birth of the complainant to them for reference.

The complainant was dissatisfied that the employer carelessly disclosed his personal data without obtaining his prior consent. Hence, he made a complaint to PCPD.

Outcome

The employer claimed that the disclosure of the complainant's personal data to all staff was to seek their comments on the complainant's work performance to consider his suitability for promotion. However, the employer could have only consulted staff members who were directly related to the post of the complainant (e.g. the complainant's supervisor and teammates) to achieve such purpose. There was no practical need to disclose the complainant's full resume and date of birth to all staff. Hence, PCPD considered that such move was in contravention of DPP3.

經私隱公署介入後，該僱主修訂其考慮晉升員工的程序，承諾日後在考慮晉升員工時，除了遴選委員會外，不會將獲考慮晉升的員工的完整履歷資料及出生日期披露予其他員工。此外，該僱主就事件向投訴人致歉，並要求其他員工銷毀投訴人的個人資料。

After PCPD's intervention, the employer amended the procedures for considering staff promotion and undertook that in future it would not disclose the full resume and date of birth of staff members being considered for promotion to all staff, except the selection board. Moreover, the employer apologised to the complainant and requested other staff members to destroy the complainant's personal data.

借鑑

根據私隱公署發出的《人力資源管理實務守則》，僱主不應在未取得僱員的明示及自願同意下，向第三者披露僱員的僱傭資料，除非披露該資料的目的與僱傭直接有關，或是法律或法定主管機關規定必須披露該資料。此外，僱主向第三者轉移或披露僱傭資料時，應避免披露超越第三者的使用目的所需的資料。

企業需要使用個人資料以進行人力資源管理，期間必須遵守《私隱條例》及《人力資源管理實務守則》。除了客戶的個人資料外，企業亦有責任保障僱員的個人資料，締造一個保障個人資料私隱的工作環境及運作模式。

Lesson learnt

According to PCPD's Code of Practice on Human Resource Management, an employer should not disclose employment-related data of employees to a third party without first obtaining the employees' express and voluntary consent unless the disclosure is for purposes directly related to the employment, or such disclosure is required by law or by statutory authorities. Moreover, when employment-related data is transferred or disclosed to a third party, an employer should avoid disclosure of data in excess of what is necessary for the purpose of use by the third party.

While organisations need to use personal data for human resource management, they should comply with the PDPO and the Code of Practice on Human Resource Management. Apart from customers' personal data, organisations are also responsible for the protection of employees' personal data in order to create a working environment and operational model were personal data privacy is protected.

個案七：牙科診所 – 向病人展示其他病人的醫療紀錄 – 要求病人將醫療報告發送到其手機 – 保障資料第4原則

投訴內容

投訴人到牙科診所求診。牙醫與投訴人商討治療方案期間，展示另一位病人的牙骨X光片，以輔助解說，但該X光片清晰顯示了該名病人的姓名。另一方面，由於投訴人要向牙醫提供早前的驗血報告，該牙醫的助理遂要求投訴人以手機即時通訊軟件傳送給她。投訴人認為由上述兩件事情可見，該診所對病人的個人資料保障不足，遂向私隱公署作出投訴。

結果

就個人資料保安方面，私隱公署認為，牙科診所作為資料使用者，有責任確保員工在使用或處理個人資料（尤其涉及敏感的個人資料，如病歷資料、化驗報告等）時，須依從《私隱條例》附表1的保障資料第4原則，必須採取所有切實可行的步驟，以確保個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

Case 7: Dental clinic - display of other patient's medical record to a patient -requesting a patient to send his medical record by mobile phone - DPP4

The complaint

The complainant went to a dental clinic for medical consultation. To illustrate his explanation when discussing the treatment plan with the complainant, the dentist showed an X-ray film of another patient's dental exostosis with the patient's name clearly shown. Moreover, as the complainant needed to provide the dentist with his earlier blood test results, the dentist's assistant requested the complainant to send the results through a mobile instant messaging application. The complainant considered that the two incidents showed the clinic's inadequate personal data protection for patients and made a complaint with PCPD.

Outcome

Regarding personal data protection, PCPD considered that the clinic as a data user was obliged to ensure staff's compliance with DPP4 of Schedule 1 to the PDPO when using or handling personal data (especially when sensitive personal data was involved, e.g. medical records, laboratory test results, etc). Staff must adopt all the practicable steps to ensure personal data was protected against unauthorised or accidental access, processing, erasure, loss or use.

無疑使用手機通訊軟件傳送文件日益普遍，但在傳送敏感的個人資料時，資料使用者應加倍提高警覺。私隱公署建議診所應採取其他較安全的傳送方式，例如加密電郵或親身送遞。作為良好的行事方式，即使要求病人以手機通訊軟件提交個人資料，診所職員亦應向病人說明這種傳送方式的風險，以及讓病人自行選擇提交方式。同時，診所亦應提醒職員，不可轉發經手機通訊軟件接收的病人資料，以及在完成使用有關文件的目的後，必須立即將文件刪除。

Undoubtedly, the use of mobile communication applications in transmitting documents is becoming more common. But data users should exercise vigilance when transmitting sensitive personal data. PCPD recommended the clinic to adopt transmission means with higher security, e.g. encrypted email or delivery by-hand. As a good practice, the clinic staff should explain the risk to the patient when requesting the patient to submit his personal data through mobile communication applications, and allow the patient to choose the means of submission. Moreover, the clinic should also remind its staff that forwarding of patients' personal data received by mobile communication applications was not allowed, and the personal data must be deleted once the purposes of using the documents were achieved.

另一方面，在本個案中，雖然牙醫在向病人講解治療方案時，以類似個案的X光影像輔助，希望使病人易於理解，看來是出於好意。但如當中不慎披露了其他病人的個人資料，或有違《私隱條例》的相關規定，效果適得其反。私隱公署要求該診所敦促職員，日後在類似本案的情況下必須加倍謹慎小心。

Besides, in this case, it appeared to be a goodwill of the dentist to refer to a similar X-ray film to help the patient understand the treatment plan. However, if other patient's personal data was inadvertently disclosed, the relevant requirements of the PDPO might be contravened. PCPD requested the clinic to urge its staff to be more careful when encountering similar situation in future.

借鑑

公眾對個人資料私隱保障的期望與日俱增，加上病歷資料屬性質敏感的個人資料，醫護從業員亦特別小心謹慎處理病人資料，提高個人資料的保安意識。醫療機構亦須因應資料性質的敏感程度，從而採取相應而均稱的資料保安措施，方能符合公眾的合理期望及履行數據道德責任。

Lesson learnt

Since public expectation on personal data privacy protection is rising and medical records are sensitive personal data, medical practitioners should be more vigilant in handling patients' data and be aware of personal data security. Medical institutions should also adopt proper and proportionate data security measures in accordance with the sensitivity of the data, in order to fulfil the reasonable expectation of the public and the duty of data ethics.

檢控及定罪個案

在本報告年度有五宗被檢控及被定罪的個案，全部涉及使用個人資料作直接促銷。

PROSECUTION AND CONVICTION CASES

In the reporting year, 5 cases had been prosecuted and convicted. They were all related to the use of personal data in direct marketing.

個案1：一名保險代理人在使用投訴人個人資料作直接促銷前沒有採取指明的行動通知投訴人，以及未有告知該人她拒收直接促銷訊息的權利 –《私隱條例》第35C及35F條

投訴內容

投訴人的手提電話收到一名保險代理人發出的即時通訊訊息，推廣其任職的保險公司的儲蓄計劃，訊息中有提及投訴人的姓氏。投訴人表示她並不認識被告，並曾查問被告從何得悉其姓氏及電話號碼，但被告未能提供滿意的答覆。該代理人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

該代理人被控(1)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(2)在首次使用投訴人的個人資料作直接促銷時，未有告知她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，違反了條例第35F(1)條。該代理人承認上述兩項控罪，每項控罪分別被判罰款4,000元，共被判罰款8,000元。

Case 1: An insurance agent of an insurance company convicted for using the complainant's personal data in direct marketing without taking specified actions and failing to notify the complainant of her opt-out right – sections 35C and 35F of the PDPO

The complaint

The complainant received an instant communication message on her mobile number, addressing her by her surname, from the insurance agent for promoting a saving plan of the insurance company that the agent worked for. The complainant said that she did not know the agent and questioned how he obtained her surname and telephone number. The agent failed to provide a satisfactory reply. Neither had the agent notified the complainant of her opt-out right.

Outcome

The agent 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 PDPO; 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 PDPO. The agent pleaded guilty to both charges and was fined HK$8,000 in total (HK$4,000 in respect of each charge).

個案二：一間銀行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 2016 年 8 月透過互聯網申請該銀行的信用卡時，選擇拒收該銀行的直接促銷資訊，但其後卻於同年 10 月收到該銀行推廣保險服務的來電。

結果

該銀行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。該銀行承認控罪，被判罰款 HK$10,000。

Case 2: A bank convicted for failing to comply with an opt-out request – section 35G of the PDPO

The complaint

The complainant applied for the bank's credit card online in August 2016. He had opted out the use of his personal data in direct marketing during the application process. However, the complainant still received a direct marketing call from the Bank in October 2016 promoting its insurance services.

Outcome

The bank was charged with an offence under section 35G(3) of the PDPO for failing to comply with the requirement from a data subject to cease to use his personal data in direct marketing. The bank pleaded guilty to the charge and was fined HK$10,000.

個案三：一間拍賣公司在使用投訴人個人資料作直接促銷前沒有採取指明的行動通知投訴人，以及未有告知該人她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2017年11月於其住址收到一間拍賣公司具名致她的拍賣小冊子。投訴人過去與該公司沒有往來，這是她首次收到該公司的直接促銷資料。該公司在有關的直銷資料中亦沒有告知投訴人她有權要求該公司停止如此使用有關資料。

結果

該公司被控(1)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(2)在首次使用投訴人的個人資料作直接促銷時，未有告知她有權要求被告在不向其收費的情況下停止使用她的個人資料作促銷用途，違反了條例第35F(1)條。該公司承認上述兩項控罪，每項控罪分別被判罰款10,000元，共被判罰款20,000元。

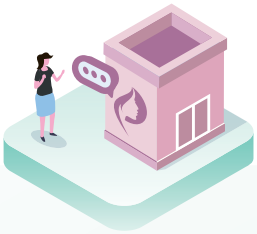
Case 3: An auction company convicted for using the complainant's personal data in direct marketing without taking specified actions and failing to notify the complainant of her opt-out right – sections 35C and 35F of the PDPO

The complaint

In November 2017, the complainant received at her address an auction booklet of an auction company addressed to her by her full name. She had no previous dealing with the company and that was the first time she received direct marketing material from it. No opt-out clause was provided to her on the direct marketing material.

Outcome

The auction company 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 PDPO; 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 PDPO. The company pleaded guilty to both charges and was fined HK$20,000 in total (HK$10,000 in respect of each charge).



個案四：一間美容產品公司在使用投訴人個人資料作直接促銷前沒有採取指明的行動通知投訴人–《私隱條例》第35C條

投訴內容

投訴人於2017年2月透過互聯網申請成為一間美容產品公司的會員，並向該公司提供了包括她公司地址在內的聯絡資料，及選擇了拒收該公司的直接促銷資訊。投訴人於2017年5月8日收到寄往其公司地址的該公司產品推廣來件。

結果

該公司被控在使用投訴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。該公司承認控罪，被判罰款HK$8,000。

Case 4: A beauty product company convicted for using the complainant's personal data in direct marketing without taking specified actions – section 35C of the PDPO

The complaint

In February 2017, the complainant registered online as a member of a beauty product company, by filling in her contact information including office address. The complainant also opted out of receiving direct marketing materials from the company. On 8 May 2017, the complainant received a mail at her office address from the company about their products.

Outcome

The company was charged with an offence of using the personal data of the complainant in direct marketing without taking specified actions, contrary to section 35C(2) of the PDPO. The company pleaded guilty to the charge and was fined HK$8,000.

個案五：一間電訊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

投訴人是一間電訊公司的客戶。2017年7月，投訴人曾透過電話向該公司提出拒收直銷訊息要求，但其後於2017年8月至12月（四個月內）收到該公司發出的23個直銷訊息或電郵。

結果

該公司被控違反23項《私隱條例》的罪行。所有23項控罪均指被告沒有依從資料當事人的拒收直銷訊息要求，而繼續使用其個人資料作直接促銷，違反了《私隱條例》第35G(3)條。該公司承認14項控罪，每項控罪分別被判罰款HK$6,000元，合共被判罰款HK$84,000。

Case 5: A telecommunications company convicted for failing to comply with an opt-out request – section 35G of the PDPO

The complaint

The complainant was a customer of a telecommunications company. In July 2017, she made her opt-out request by phone to the company relating to cessation of using her personal data in direct marketing. However, the complainant subsequently received 23 direct marketing text messages or emails from the company between August and December 2017 (within four months).

Outcome

The company faced 23 charges under section 35G(3) of the PDPO for failing to comply with the requirement from a data subject to cease to use her personal data in direct marketing. The Company pleaded guilty to 14 charges, and was fined HK$84,000 in total (HK$6,000 in respect of each charge).