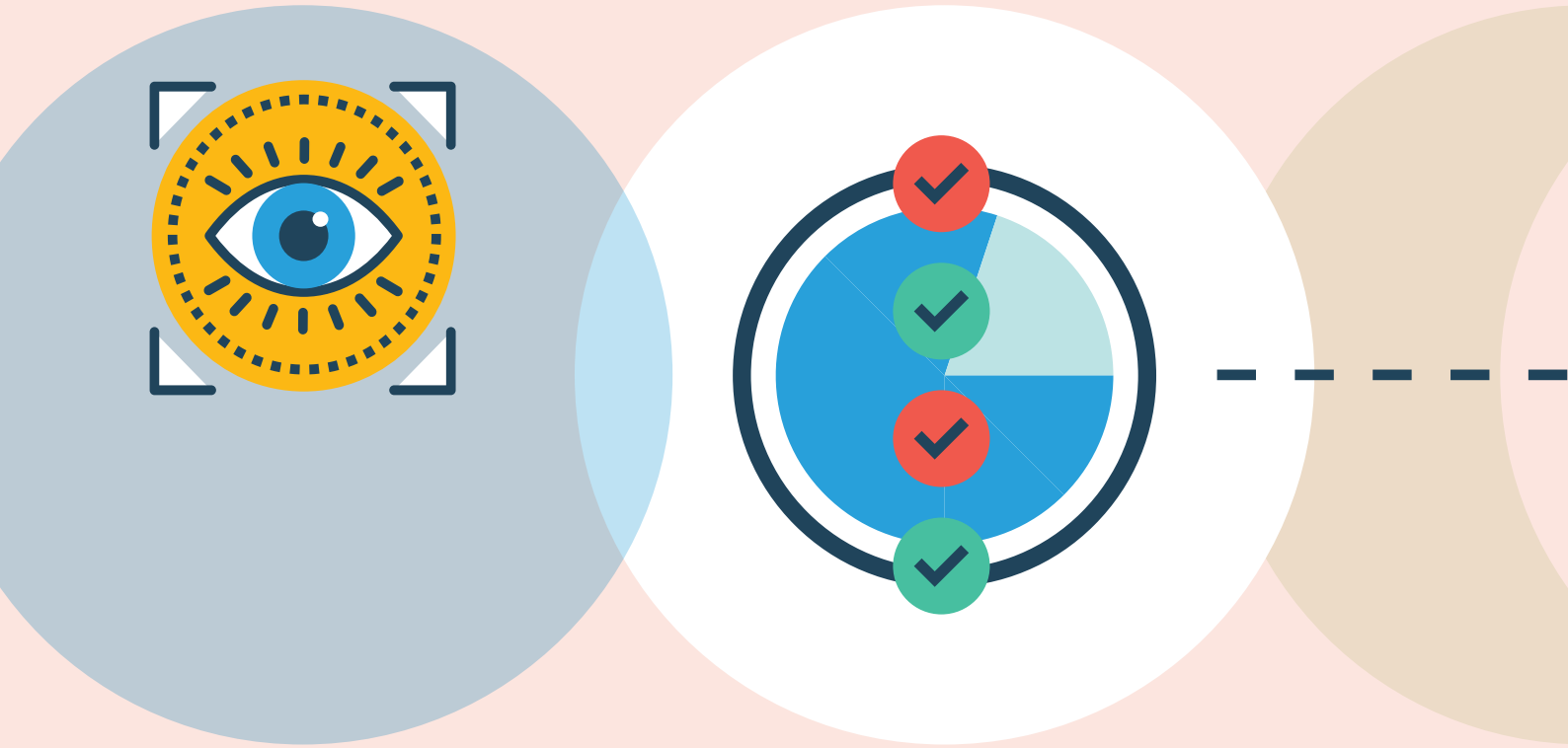
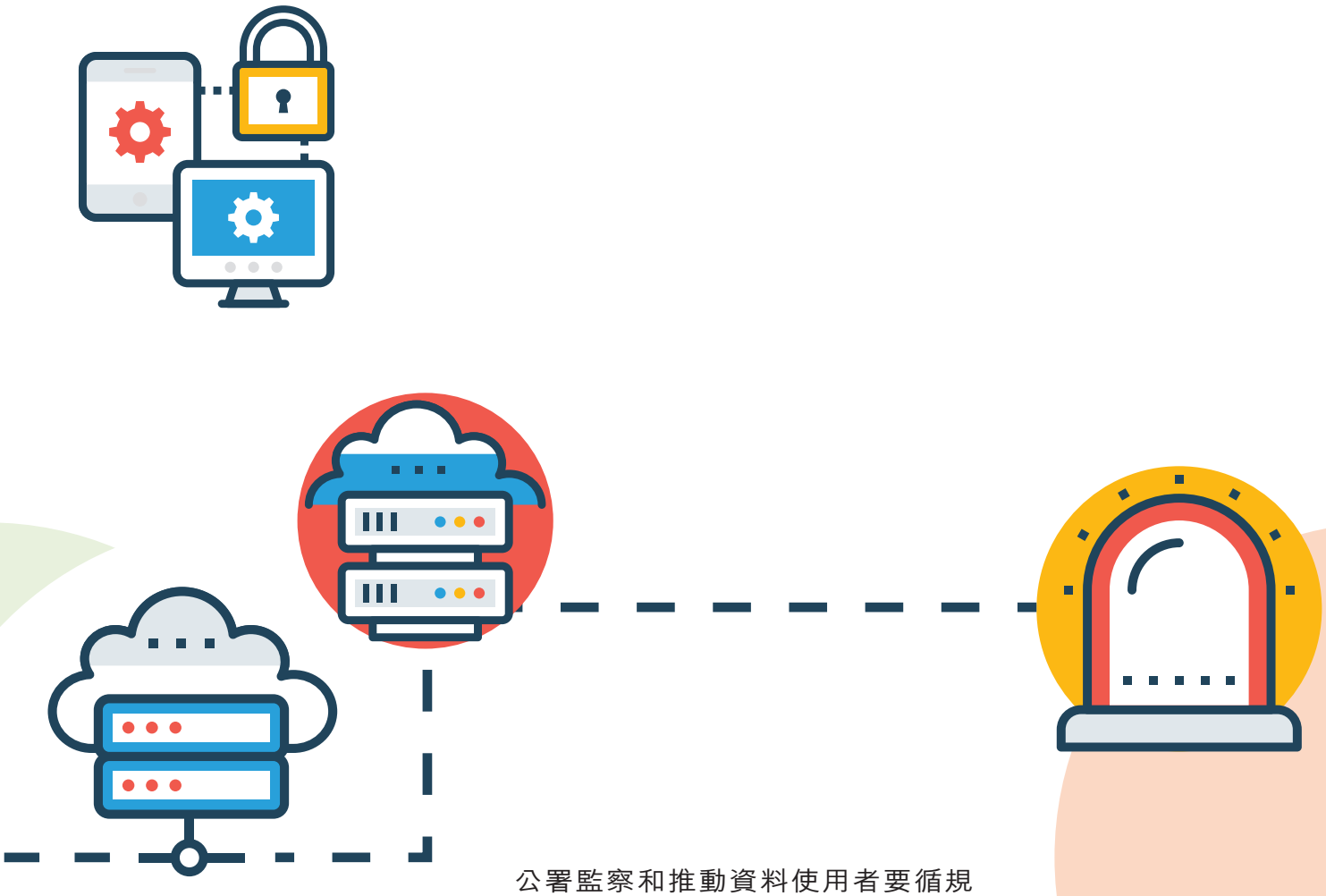
MONITORING COMPLIANCE EMBRACING CHALLENGES

監督符規　擁抱挑戰





公署監察和推動資料使用者要循規以符合《私隱條例》的規定。隨著資訊科技急速發展而衍生的私隱風險，公署鼓勵和支援機構採取措施保障個人資料，並尊重消費者的個人資料私隱。

The PCPD monitors and promotes compliance with the provisions of the Ordinance. In view of the privacy risks brought about by the rapid advancement in information and communication technology, we encourage and facilitate organisations to adopt measures to ensure personal data protection and respect consumers' personal data privacy.

2017 年抽查報告：顧客獎賞計劃

公署連續第五年參與全球私隱執法機關網絡（Global Privacy Enforcement Network）的抽查行動。本年抽查行動的主題是「用戶對其個人資料的掌控程度」。包括公署在內共 24 個來自世界各地的私隱執法機關參與了抽查行動，透過檢視個人資料收集表格、私隱政策及收集個人資料聲明等，評估不同行業在私隱方面的實務措施。

公署的抽查行動在 2017 年 5 月 22 日至 26 日期間進行，檢視了六個不同行業（即零售、酒店、餐飲、航空、戲院及汽油）的 30 個顧客獎賞計劃。

全球方面，各私隱執法機關檢視了不同行業共 455 個資料使用者的私隱政策及實務措施，包括零售、金融及銀行、旅遊、社交媒體、遊戲／博彩、教育及健康護理。

主要觀察所得

公署的抽查結果大致與全球抽查結果一致。公署在抽查行動的主要觀察所得包括：

1. **普遍備有私隱政策：**大部分顧客獎賞計劃均備有私隱政策供顧客參閱。

2. **欠缺透明度：**大多數政策均使用空泛及含糊的字眼，欠缺透明度。

3. **沒有具意義的同意：**大部分計劃在登記時向顧客取得「綑綁式同意」，以便將他們的資料用於多項用途。顧客通常沒有真正的選擇。

4. **欠缺對個人資料的控制：**這些獎賞計劃沒有向顧客提供適當的途徑以提出要求刪除其個人資料、反對分享其個人資料，以及反對利用其個人資料進行個人概況彙編等，顧客因而不能對其個人資料作有效的控制。數據中介行業的興起令人更難掌握資料最終會落在何人手中。

PRIVACY SWEEP 2017 - CUSTOMER LOYALTY AND REWARD PROGRAMMES

The PCPD participated in the Privacy Sweep of the Global Privacy Enforcement Network (GPEN) for the fifth consecutive year. The theme of the global Privacy Sweep 2017 was "User Control over Personal Information". 24 privacy enforcement authorities from around the world, including the PCPD, participated in the Privacy Sweep to evaluate the privacy practices of various sectors by conducting desktop review of the personal information collection forms, privacy policies and personal information collection statements of the industry players, etc.

During the Sweep period between 22 and 26 May 2017, the PCPD examined 30 customer loyalty and reward programmes selected from six sectors, namely retail, hotel, catering, airlines, cinema and gasoline.

Globally, the privacy practices of 455 data users in various sectors (including retail, finance and banking, travel, social media, gaming/gambling, education and health) were examined by the privacy enforcement authorities.

Key observations

The PCPD's observations were largely in line with the global ones. The key observations of the PCPD included:

1. **Privacy policies were generally available.** The majority of the customer loyalty and reward programmes provided privacy policies to customers.

2. **Lack of transparency.** The privacy policies generally lacked transparency because the terms used were too broad and vague.

3. **No meaningful consent.** The majority of the programmes obtained "bundled consent" from customers during registration to use their data for multiple purposes. The customers usually did not have genuine choice.

4. **Lack of control over personal data.** Customers could not exercise effective control over their personal data because they were usually not provided with the means to request data deletion and to object to data sharing and profiling. The rise of the data broker industry cast further doubt about where the data would end up.

5. **涉及大數據分析及個人概況彙編的私隱風險：**很多計劃在其私隱政策中表明有意使用個人資料作大數據分析、個人概況彙編及／或自動化決策，這些做法會增加私隱風險，例如：
   - 過度收集個人資料；
   - 從匿名資料中重新識別個人的身份；及
   - 揭露個人私密生活的詳情。

建 議

公署建議顧客獎賞計劃的營運商從多方面改善其私隱實務措施：

1. **透明度：**提供精確易明的私隱政策；避免使用含糊語言及法律措辭。

2. **避免令顧客感到驚訝：**坦誠及清楚地向顧客解釋收集的資料種類；表明收集的目的；清楚指明個人資料會與何人分享。

3. **尊重：**向顧客提供有關收集及使用其個人資料的分項選擇（即非綑綁式同意）。如可能，容許顧客拒絕其個人資料被用於某些用途（包括個人概況彙編）或分享。

4. **問責及道德：**在決定使用（包括披露）顧客的個人資料時，考慮顧客的合理期望、私隱風險及對顧客造成的潛在傷害（包括身體、財務及心理上的傷害）。

公署亦提醒消費者，在參加顧客獎賞計劃前，應小心閱讀私隱政策，了解其資料可能被使用及分享的情況，以及評估相關的私隱風險。

5. **Privacy risks relating to big data analytics and profiling.** Many programmes indicated in their privacy policies the intention to use personal data for big data analytics, profiling and/or automated decision making, which would amplify the privacy risks, such as:
   - excessive collection of personal data;
   - re-identification of individuals from anonymous data; and
   - revelation of details about an individual's intimate life.

Recommendations

The PCPD recommended operators of customer loyalty and reward programmes to improve their privacy practices in the following ways:

1. **Transparency.** Provide a privacy policy which is precise, concise and easy to understand; avoid using obscure and legalese language.

2. **Avoidance of surprises.** Explain to the customers frankly and clearly the types of data to be collected; specify the purposes of collection; clearly identify the parties with whom the personal data may be shared.

3. **Respect.** Provide customers with granular options (as opposed to bundled consent) regarding the collection and use of their personal data. If possible, allow customers to opt out of certain use (including profiling) or sharing of their personal data.

4. **Accountability and ethics.** When deciding on the use (including disclosure) of customers' personal data, take into account the reasonable expectations of the customers, as well as the privacy risks and potential physical, financial and psychological harm.

The PCPD also reminded customers of loyalty and reward programmes to read the privacy policy carefully to understand the possible use and sharing of their data, and assess the related privacy risks before joining such programmes.

循規行動

當有足夠理由相信有機構的行事方式與《私隱條例》規定不相符時，私隱專員會展開循規審查或調查。在完成循規審查或調查後，私隱專員會書面告知有關機構，指出與《私隱條例》規定不符或不足之處，並促請有關機構採取適當的補救措施，糾正可能違規的情況和採取預防措施。

在報告年度內，私隱專員共進行了273次循規審查及調查行動。80%的循規審查對象為私營機構，其餘20%則為政府部門或公營機構（包括法定機構、非政府機構及政府資助教育機構）。

下文重點介紹在年內進行的部分循規審查行動。

(i) Facebook披露用戶個人資料予第三方應用程式開發商及「劍橋分析」

2018年3月，Facebook帳戶個人資料疑被濫用一事被傳媒廣泛報道。事件涉及劍橋大學教授Dr. Aleksandr Kogan及Global Science Research於2013年透過一個性格測驗的應用程式「thisisyourdigitallife」（該應用程式）收集得的Facebook帳戶的個人資料。根據有關報道，約有270,000用戶透過Facebook安裝該應用程式，並容許該應用程式取得他們的個人資料，包括：建立個人檔案的所在城市，讚好的內容及他們朋友的資料等。多達8,700萬名Facebook帳戶的個人資料其後被轉移至一間名為「劍橋分析」的英國數據處理及分析公司，藉以影響2016年美國總統大選中選民的投票意向。

2018年3月28日，公署基於以下原因對Facebook Hong Kong Limited（Facebook HK）展開了循規審查：

(i) 香港有超過500萬名活躍Facebook帳戶；

(ii) 立法會議員莫乃光先生對事件提出關注；及

(iii) 事件引起本地傳媒的關注。

COMPLIANCE ACTIONS

The Privacy Commissioner conducts compliance checks or investigations of practices that he has sufficient grounds to take the view that they may be inconsistent with the requirements under the Ordinance. Upon completion of a compliance check or investigation, the Privacy Commissioner alerts an organisation in writing, pointing out the apparent inconsistency or deficiency, and advising the organisation, if necessary, to take remedial actions to correct any breaches and prevent further breaches.

During the reporting year, the Privacy Commissioner carried out 273 compliance checks and investigation. Of these, 80% were conducted on private sector organisation, while the remaining 20% were on government departments or public organisations (i.e. statutory bodies, non-government organisations and government-funded educational institutions).

Below are the highlights of some of the compliance actions conducted during the year.

(i) Disclosure of Facebook users' personal data to third-party app developer and Cambridge Analytica

In March 2018, media widely reported an incident of suspected unauthorised use of the data of Facebook users relating to Cambridge University Professor Aleksandr Kogan and Global Science Research, collecting Facebook users' data, through a personality test application called "thisisyourdigitallife" in 2013. Reportedly, around 270,000 people installed the aforementioned application through Facebook and allowed it to access their information, including the city they set on their profile, content they liked, and information of their friends. As a result, data of up to 87 million Facebook users collected had been passed to Cambridge Analytica, a data processing and analytics company in UK, to manipulate voters' behavior in President Trump's 2016 election campaign.

On 28 March 2018, PCPD initiated a compliance check against Facebook Hong Kong Limited (Facebook HK) for the reasons that:–

(i) there are over 5 million Facebook Hong Kong users;

(ii) Legislative Councilor Hon Charles MOK raised his concern on this incident; and

(iii) the incident attracted local media's concern.

根據公署在循規審查所取得的資料：

(1) Facebook在香港設立的辦事處（即Facebook HK）並不控制香港帳戶資料的收集、持有、處理或使用；所有Facebook的香港帳戶的資料是由Facebook Ireland Limited（Facebook Ireland）所控制。而Facebook Ireland聲稱，有關的第三方應用程式開發商未曾將Facebook的香港帳戶的個人資料披露予「劍橋分析」及其母公司。

(2) 現階段沒有資料顯示Facebook的香港帳戶牽涉於事件當中。

任何社交媒體或社交網絡服務營運商作為「資料使用者」（即控制者），在香港控制有關個人資料的收集、持有、處理或使用（包括披露和轉移），或能夠從香港行使該項控制，必須遵從《私隱條例》的規定及相關的保障資料原則。Facebook HK並不控制香港帳戶資料的收集、持有、處理或使用，所以不能被視為《私隱條例》下的「資料使用者」；雖然Facebook Ireland是香港帳戶的「資料使用者」，但沒有香港帳戶向公署表示受影響，故《私隱條例》相關規管條文未能適用於是次事件。

儘管如此，Facebook已因應是次事件採取一系列補救行動，包括限制第三方應用程式存取用戶的資料，向帳戶提供更方便的私隱設定，以及符合歐盟《通用數據保障條例》規定的一些措施。

公署其後發新聞稿公布完成循規審查。私隱專員表示，贏取客戶信任是社交媒體營運商最重要的一環。不當地處理或未有妥善保障帳戶的資料不單構成客戶變節，亦會失去商譽及公眾信任。私隱專員亦建議社交媒體的營運商應採取措施建構一個保障及尊重個人資料私隱的文化：

According to the information obtained in the compliance check:

(1) the office of Facebook in Hong Kong (Facebook HK) did not control the collection, holding, processing or use of all the data of Facebook's Hong Kong account holders, which was controlled by Facebook Ireland Limited (Facebook Ireland). Facebook Ireland also claimed that its third party application (app) developer had not disclosed the personal data of Facebook's Hong Kong account holders to Cambridge Analytica and its parent company.

(2) there is no evidence showing that Facebook's account holders in Hong Kong were involved in the incident.

As data users, social media or social network service operators must comply with the relevant requirements and Data Protection Principles of the Ordinance if they control the collection, holding, processing or use (including disclosure and transfer) of personal data in Hong Kong or exercise such control from Hong Kong. Facebook HK did not control the collection, holding, processing or use of data of its Hong Kong account holders, so Facebook HK could not be regarded as "data user" under the Ordinance. Although Facebook Ireland was the "data user" of Facebook's Hong Kong account holders, no account holders in Hong Kong complained to the PCPD that they had been affected. The relevant regulatory provisions in the Ordinance are therefore not applicable in this incident.

Nevertheless, in response to the scandal, Facebook has taken a series of remedial actions, including restriction on data to be accessed by third party app, providing more convenient controls on privacy settings to users, as well as measures to comply with GDPR.

The PCPD later issued a media statement announcing the completion of the compliance check case. In the media statement, the Privacy Commissioner commented that building trust with account holders is vital to social media operators. Improper processing or inadequate protection of data causes not only deflection of customers, but also the damage of goodwill and public confidence. The Privacy Commissioner also recommended that social media operators should adopt the following measures to nurture the culture of "protect and respect personal data privacy":

- 將資料保障提升為機構的管治責任；
- 以淺白易明的形式向帳戶解釋該社交媒體平台收集個人資料的目的、其私隱政策，以及條款及細則，並考慮以概要形式輔以圖像解釋；
- 這類政策的通知必須放置於網頁或應用程式當眼的位置；
- 向帳戶提供實質的選擇，並向其獲取明確的同意。不應與接受私隱政策綑綁；及
- 以合約或其他明確形式規範合作的第三方可存取及使用帳戶資料的情況，並必須從帳戶獲取授權。

- to embrace data protection as part of their corporate governance responsibilities;
- to explain the purposes of collecting personal data, the privacy policy, terms and conditions to users in an easily readable and understandable manner, and may consider supplementing a summary with infographics;
- to place the notification of such policies conspicuously on their websites or apps;
- to provide users with real choices and obtain their express consent. The choices should not be bundled with acceptance of the privacy policy;
- to use contractual or other explicit means to restrict the access and use of users' data by third parties, and must obtain users' authorisation.

(ii) 旅行社的客戶數據庫遭黑客入侵

在年內發生的數家旅行社的數據庫遭黑客入侵的個案當中，其中一間旅行社的客戶數據庫遭黑客加密，被勒索贖金以換取解密鑰匙。該客戶數據庫涉及約20萬名自2014年3月起的客戶的個人資料，包括姓名、身份證號碼、護照號碼、電話、電郵地址、信用卡資料、郵寄地址及／或購買紀錄。該旅行社拒絕交付贖金並報警。公署從傳媒得悉事件後主動展開循規審查。

事發後，該旅行社聘請了兩間網絡保安公司分別調查黑客入侵系統的方法和提供加強網絡安全的建議。為減低受到網絡攻擊的風險，該旅行社提升其整體的網絡保安，包括加設網絡應用防火牆、於遙距存取採用雙重認證、為客戶數據庫進行加密和離線備份、定期進行滲透測試和漏洞掃描等。

該旅行社亦檢視了其資料收集和保留的做法，停止收集信用卡保安碼和身份證號碼，及將信用卡號碼的保留期限由一年縮短至半年，以減低外洩敏感個人資料的風險。

(ii) Travel agencies' customer databases being hacked

Several travel agents were cyber-attacked and got their databases hacked during the year. In one of the cases, a travel agency's customer database was encrypted by a hacker who demanded a ransom in exchange for decryption key. The database contained personal data of about 200,000 customers who had made purchases with the travel agency since March 2014. Personal data involved included customers' names, Hong Kong Identity Card numbers, passport numbers, phone numbers, email addresses, credit card information, mailing addresses and/or purchase histories. The travel agency refused to pay the ransom and reported the incident to the Police. The PCPD initiated a compliance check after noting the incident from the media.

After the incident, the travel agency engaged two cybersecurity companies to investigate how the systems had been compromised and to advise how to strengthen its cybersecurity respectively. To reduce the risk of cyberattack, the travel agency enhanced its overall cybersecurity by enabling Web Application Firewall, adopting two-factor authentication for remote access, encrypting the customer database and creating an offline backup, conducting penetration testing and vulnerability scanning regularly, etc.

The travel agency also reviewed its data collection and retention practices. It ceased collecting credit cards' CVV numbers and Hong Kong Identity Card numbers, and shortened the retention period of credit card numbers from one year to six months to reduce the risk of leakage of sensitive personal data.

(iii) 沒有安全傳輸個人資料的網站

公署抽查了不同行業涉及收集個人資料的大約660個本地網站，以評估有關的資料使用者在透過互聯網傳輸個人資料的過程中是否採取足夠保障措施。根據抽查結果，公署對68個未有使用安全通訊端層（SSL）或其他科技以加密所需要傳送資料的資料使用者展開循規審查。

循規行動顯示大部分有問題的資料使用者不是沒有意識到需要保障在互聯網上傳輸的個人資料，便是擁有很少甚或根本沒有資訊科技方面的知識以確保他們的網站安全。

因應公署的建議，上述68間公司已在其網站實施SSL加密技術，以保障個人資料不受未獲准許的截取或查閱。基於是次循規行動的正面成效，公署將繼續相關行動。

視察行動

視察原因

近年香港的物業市場交投持續活躍，而地產代理需要處理的個人資料數量龐大，種類繁多，私隱專員遂根據《私隱條例》第36條對一間在市場具領導地位的地產代理公司（「該公司」）的個人資料系統進行視察，就業界處理個人資料方面作出建議，藉以加強他們依從《私隱條例》規定的認知。

視察結果及建議

視察結果顯示，該公司已採取合理措施致力確保顧客的個人資料得到妥善管理，未有發現有嚴重缺失。私隱專員滿意該公司最高管理層支持個人資料私隱保障的承諾，委任高級行政人員以監察其個人資料系統符合《私隱條例》的規定，並將個人資料私隱保障納入其企業管治之中。在技術層面方面，私隱專員欣賞該公司審慎地分割及監控其資料庫系統的權限，並按「有需要知道」的原則設置使用權限，以減少未獲授權查閱或洩露顧客個人資料的風險。

(iii) Websites without secure transmission of personal data

The PCPD examined around 660 local websites from various sectors which involved the collection of personal data, to evaluate whether the data users concerned provided sufficient security measures for personal data transmitted through their websites. Subsequently, the PCPD initiated compliance checks against 68 of those data users who did not enable Secure Sockets Layer (SSL) or other technical means on their websites to encrypt the data transmitted.

The compliance actions revealed that most of the problematic data users involved were either not aware of the need of security during personal data transmission through Internet or they did not have sufficient knowledge of information technology to make their websites secure.

With the PCPD's advice, the 68 data users had implemented SSL encryption on their websites in order to protect the transmitted personal data against unauthorised interception or access. In view of the positive outcome, the PCPD will continue to carry out similar exercises.

INSPECTION

Reasons for Inspection

Given the continuous boom of the property market in Hong Kong and the vast volume and broad range of personal data handled by estate agents, the Privacy Commissioner conducted an inspection of the personal data system of a leading estate agency (the Agency) pursuant to section 36 of the Ordinance. Through the inspection exercise, we made recommendations to this class of data users in relation to the handling of personal data so as to promote compliance with the provisions of the Ordinance.

Findings and Recommendations

The inspection showed that the Agency did make reasonably good efforts to ensure proper management of customers' data. No material deficiencies were found on the part of the Agency in privacy protection matters. The Privacy Commissioner was satisfied that the Agency had top management commitment to data privacy protection by designating a senior management officer to oversee and monitor the compliance of the personal data system and integrating the idea of data privacy protection into the organisation's governance. On the technical side, the Privacy Commissioner appreciated that the Agency prudently segmented the authorities and controlled the access rights of its database systems on a need-to-know basis, which would minimise the risk of unauthorised access to or leakage of customers' data.

私隱專員參照一個全面的私隱管理系統的要求，在報告內提出多項建議及良好行事方式供業界作參考，包括制定全面的私隱政策、合規審核機制、資料外洩事故通報機制及指引、資訊科技保安政策，規範個別地產代理收集及處理買賣雙方顧客的個人資料的方式，以及積極提供培訓及教育予員工等，以協助地產代理業界遵從《私隱條例》的規定。

Based on the elements of a comprehensive privacy management programme, the Privacy Commissioner made a number of recommendations and provided examples of the best practices in the report, including the formulation of comprehensive privacy policies, compliance audit system, data breach reporting mechanism and guidelines, IT security policies, controls on the handling of vendors' and purchasers' personal data by estate agents and the provision of training and education to staff members in a proactive approach etc., to assist the industry in ensuring compliance with the requirements under the Ordinance.

私隱專員於報告內亦指出，機構若要有效管理及執行個人資料保障的政策，則不可只視有關政策為法律循規的事宜，而是應由董事會做起，將個人資料保障視為其企業管治責任、建立自己的私隱管理系統，並將之納入處理業務中不可或缺的一環。

The Privacy Commissioner also stated in the report that personal data protection could not be managed effectively if an organisation treats it merely as a legal compliance issue. Instead, organisations should embrace personal data protection as part of their corporate governance responsibilities, formulate a comprehensive privacy management programme and apply them as a business imperative, starting from the boardroom.

資料外洩通報

DATA BREACH NOTIFICATIONS

資料外洩事故一般是指資料使用者懷疑其持有的個人資料保安不足，以致洩露資料，令資料可能被人未經授權或意外地查閱、處理、刪除、喪失或使用。資料外洩事故可能構成違反保障資料第4原則。雖然《私隱條例》並未有規定資料使用者就資料外洩事故作出通報，但為符合數據道德標準，公署一直鼓勵資料使用者一旦發生資料外洩事故，須通知受影響的資料當事人、私隱專員和其他相關人士。

A data breach is a breach of security of personal data held by a data user, which results in exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. The breach may amount to a contravention of Data Protection Principle 4. Although the Ordinance does not require data users to give data breach notification (DBN), the PCPD has always encouraged data users to give such notification to the affected data subjects, the Privacy Commissioner, and other relevant parties when a data breach has occurred.

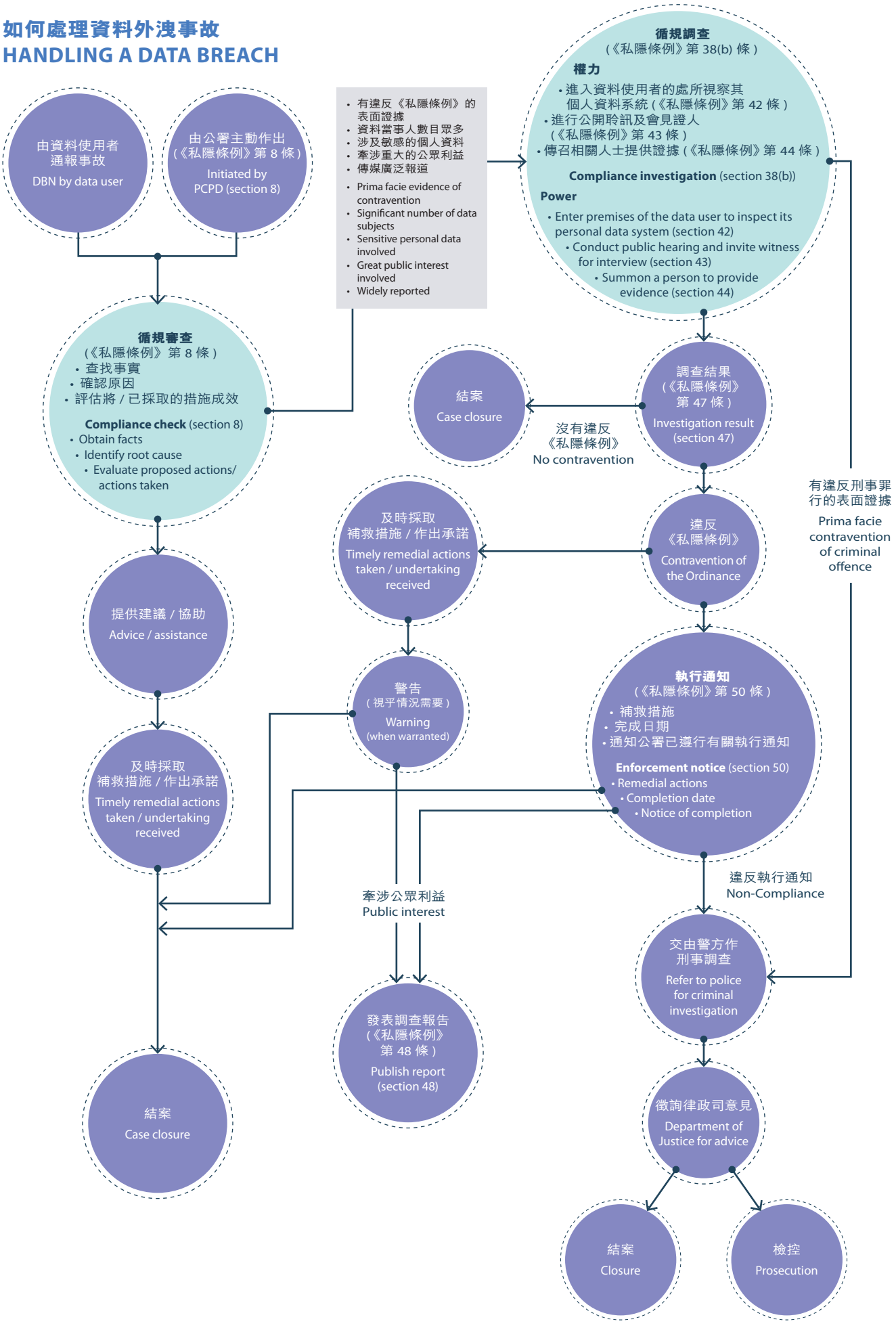
公署在接獲資料外洩事故通報（可用公署的指定表格或其他方式呈報）後，會評估有關資料，以考慮是否有需要對有關機構展開循規審查。私隱專員對相關資料使用者進行循規審查後，會書面指出明顯的不足之處，並建議他們採取補救措施，防止同類事故重演。

Upon receipt of a DBN from a data user (which could be submitted through the PCPD-designed DBN form or other means of communication), the PCPD would assess the information provided in the DBN and decide whether a compliance check is warranted. On completion of a compliance check, the Privacy Commissioner would point out the apparent deficiency and suggest the data user, where appropriate, to take remedial actions to prevent recurrence of the incident.

在報告年度內，公署接獲 116 宗資料外洩事故通報（37 宗來自公營機構；79 宗來自私營機構），牽涉 765,834 名人士的個人資料。公署對所有肇事機構均展開循規審查行動。

During the reporting year, the PCPD received 116 DBNs (37 from the public sector and 79 from the private sector), involving personal data of 765,834 individuals. The PCPD conducted a compliance check in each of these 116 incidents.

如何處理資料外洩事故
HANDLING A DATA BREACH



個人資料的核對程序

核對程序是指以電子方法比較因不同目的而收集的個人資料，從中得出的結果可用作對有關資料當事人採取不利行動的程序。資料使用者如無資料當事人的訂明同意或私隱專員的同意，不得進行核對程序。

在報告年度內，私隱專員共收到 20 宗個人資料核對程序申請，全部來自政府部門或公營機構。

經審閱後，私隱專員在有條件的情況下批准了 18 宗申請，餘下兩宗申請則不屬《私隱條例》釋義所指的核對程序。以下是私隱專員批准進行個人資料核對程序的部分個案：

DATA MATCHING PROCEDURE

A data matching procedure is a process by which personal data collected for one purpose is compared electronically with personal data collected for other purposes with an aim of taking adverse action against the data subjects concerned. A data user shall not carry out a matching procedure unless it has obtained the data subjects' prescribed consent or the Privacy Commissioner's consent.

During the reporting year, the Privacy Commissioner received a total of 20 applications for carrying out matching procedures. All of these applications came from government departments or public-sector organisations.

Upon examination, 18 applications were approved, subject to conditions imposed by the Privacy Commissioner; and the remaining two applications were found not to be matching procedures as defined under the Ordinance. The following are some of the matching procedures approved by the Privacy Commissioner:

提出要求者 Requesting Parties	核准的資料核對程序詳情 Details of the Approved Data Matching Procedures
政府資訊科技總監辦公室 Office of the Government Chief Information Officer	把政府資訊科技總監辦公室從「上網學習支援計劃」申請人及其配偶和子女收集的個人資料，與社會福利署從「綜合社會保障援助計劃」下與就學有關的選定項目定額津貼受助人收集的個人資料互相比較，以核實申請人的資格。 Comparing the personal data collected by the Office of the Government Chief Information Officer from the applicants of the Internet Learning Support Programme and their spouses and children with the personal data collected by the Social Welfare Department from the beneficiaries of the flat-rate grant for selected items of school-related expenses under the Comprehensive Social Security Assistance Scheme, so as to assess the eligibility of the applicants.
在職家庭及學生資助事務處 Working Family and Student Financial Assistance Agency	把在職家庭及學生資助事務處從「低收入在職家庭津貼計劃」（2018 年 4 月 1 日易名為「在職家庭津貼計劃」）受助人收集的個人資料，與社會福利署從「綜合社會保障援助計劃」受助人收集的個人資料互相比較，以辨識符合領取《2017-18 年度財政預算案》中提及的一次性額外款項的受助人。 Comparing the personal data collected by the Working Family and Student Financial Assistance Agency from the beneficiaries of the Low-income Working Family Allowance Scheme (renamed as Working Family Allowance Scheme from 1 April 2018) with the personal data collected by the Social Welfare Department from the beneficiaries of the Comprehensive Social Security Assistance Scheme, in order to identify beneficiaries eligible for the one-off extra payment introduced in the 2017-18 Budget.

香港房屋協會 Hong Kong Housing Society	把香港房屋協會從「資助出售房屋項目 2017」申請人及其家庭成員收集的個人資料，與香港房屋委員會從資助房屋業戶、租戶及申請人收集的個人資料互相比較，以避免公共房屋資源遭到濫用。 Comparing the personal data collected by the Hong Kong Housing Society from the applicants of the Subsidised Sale Flats Projects 2017 and their family members with the personal data collected by the Hong Kong Housing Authority from the owners, tenants and applicants of subsidised housing, so as to prevent abuse of public housing resources.
選舉事務處 Registration and Electoral Office	把選舉事務處從申請更新住址資料的登記選民收集的個人資料，與房屋署從公共房屋業戶、租戶及認可成員收集的個人資料互相比較，以核實選民的住址資料。 Comparing the personal data collected by the Registration and Electoral Office from electors applying for change of registered addresses with the personal data collected by the Housing Department from the owners, tenants and authorised members of public housing, in order to verify the addresses of electors.