合規
Compliance

公眾查詢

私隱專員公署在本報告年度接獲的查詢個案數目為15,293宗，比上年度減少了9.7%，平均每個月處理約1,300宗查詢個案，即每個工作天處理60宗查詢。大部分查詢個案(84%)屬電話查詢[1]，經書面及親臨公署提出的查詢分別佔13%及3%。(圖2.1)

大部份的查詢與收集及使用個人資料的情況有關(例如：香港身份證號碼及／或副本)(28%)，其他的主要查詢類別為僱傭關係的個人資料處理(7%)及《私隱條例》的應用(8%)。關於「起底」的查詢有所增加，由上年度的217宗增至本年度的325宗，增幅為49%。

有關電話行騙的查詢持續增加，由上年度的511宗增至本年度的732宗，增幅為43%。因應透過偽冒電話、電郵或短訊誘騙個人資料的個案呈上升趨勢，私隱專員公署於2022年9月設立「個人資料防騙熱線」(3423 6611)，處理懷疑誘騙個人資料的查詢或投訴。

[1] 包括透過私隱專員公署的一般查詢熱線(2827 2827)、中小型企業諮詢熱線(2110 1155)、有關「起底」查詢／投訴熱線(3423 6666)及個人資料防騙熱線(3423 6611)。

Public Enquiries

A total of 15,293 enquiry cases were received during the reporting year, a drop of 9.7% when compared to the previous year. On average, approximately 1,300 enquiry cases were handled per month, meaning 60 enquiries being handled per working day. The majority of the enquiries (84%) were telephone enquiries[1], while written and in-person enquiries accounted for 13% and 3% respectively. (Figure 2.1)

Most of the enquiries were related to the collection and use of personal data (e.g. Hong Kong Identity Card numbers and/or copies) (28%). Other enquiries included employment-issues (7%) and general enquiries on the application of the PDPO (8%). There was an increase in the number of enquiries related to doxxing, from 217 last year to 325 this year, representing an increase of 49%.

The number of enquiries concerning telephone scams continued to rise, from 511 last year to 732 this year, representing an increase of 43%. In response to the growing trend of personal data fraud cases through impersonating phone calls, emails or text messages, the PCPD set up a "Personal Data Fraud Prevention Hotline" (3423 6611) in September 2022 to handle enquiries or complaints about suspected personal data fraud cases.

[1] Including through the General Enquiries Hotline (2827 2827), Small and Medium Enterprises Hotline (2110 1155), Enquiry/Complaint Hotline about Doxxing (3423 6666) and Personal Data Fraud Prevention Hotline (3423 6611) of the PCPD.

查詢個案數目
Number of Enquiries Received

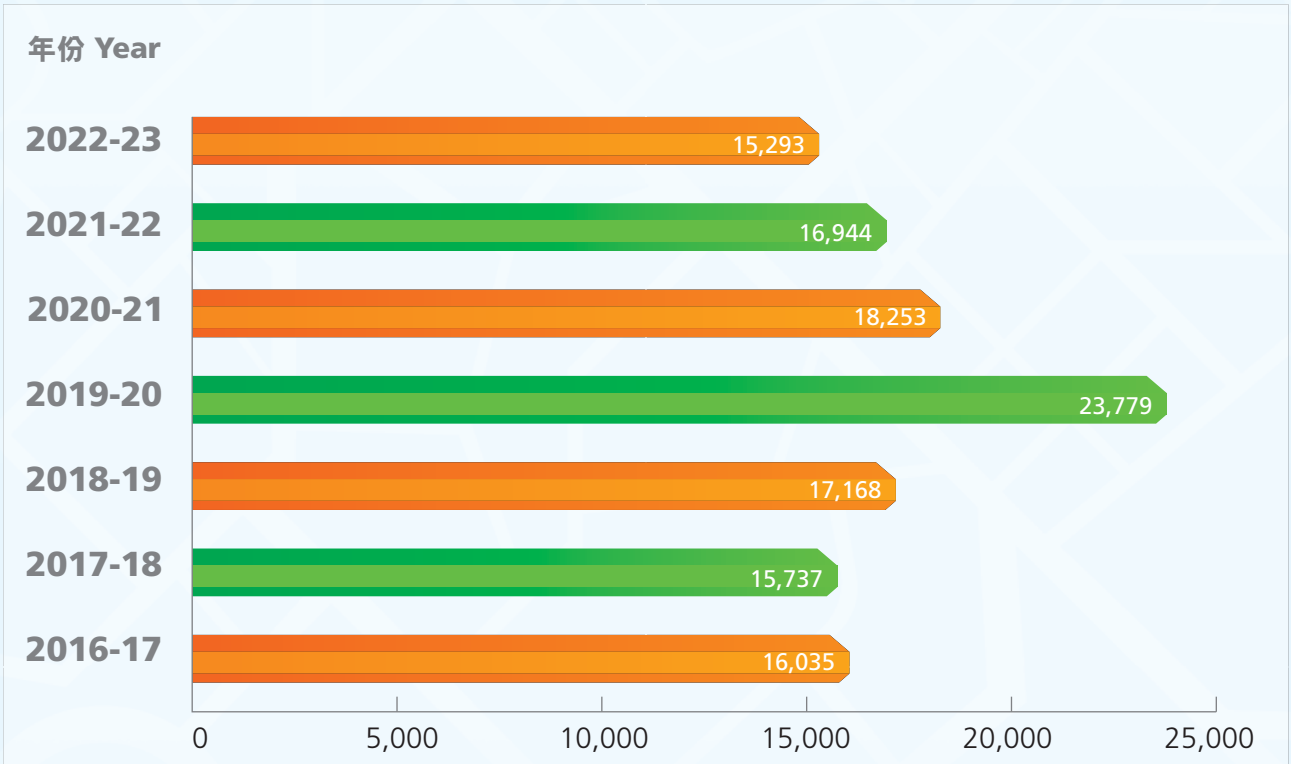


圖2.1
Figure 2.1

循規行動

當私隱專員公署發現有機構的行事方式與《私隱條例》規定不相符時，公署會展開循規審查或調查。在完成循規行動後，私隱專員一般會向機構指出與《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，糾正違規的情況和採取預防措施，避免同類事故再次發生。在報告年度內，私隱專員共進行了383次循規行動，數字與上一年度的382次循規行動相若。（圖2.2）

Compliance Actions

In cases where the PCPD finds that an organisation's practices do not comply with the requirements under the PDPO, the PCPD will initiate compliance checks or investigations. Upon completion of the compliance action, the Privacy Commissioner will generally point out any inconsistencies or deficiencies in relation to the requirements under the PDPO to the organisation, and advise the organisation to take remedial actions to correct the breaches and implement preventive measures to avoid the recurrence of similar incidents. During the reporting year, the Privacy Commissioner carried out 383 compliance actions, comparable to the 382 compliance actions carried out in the preceding year. (Figure 2.2)

循規行動數目
Number of Compliance Actions Carried Out

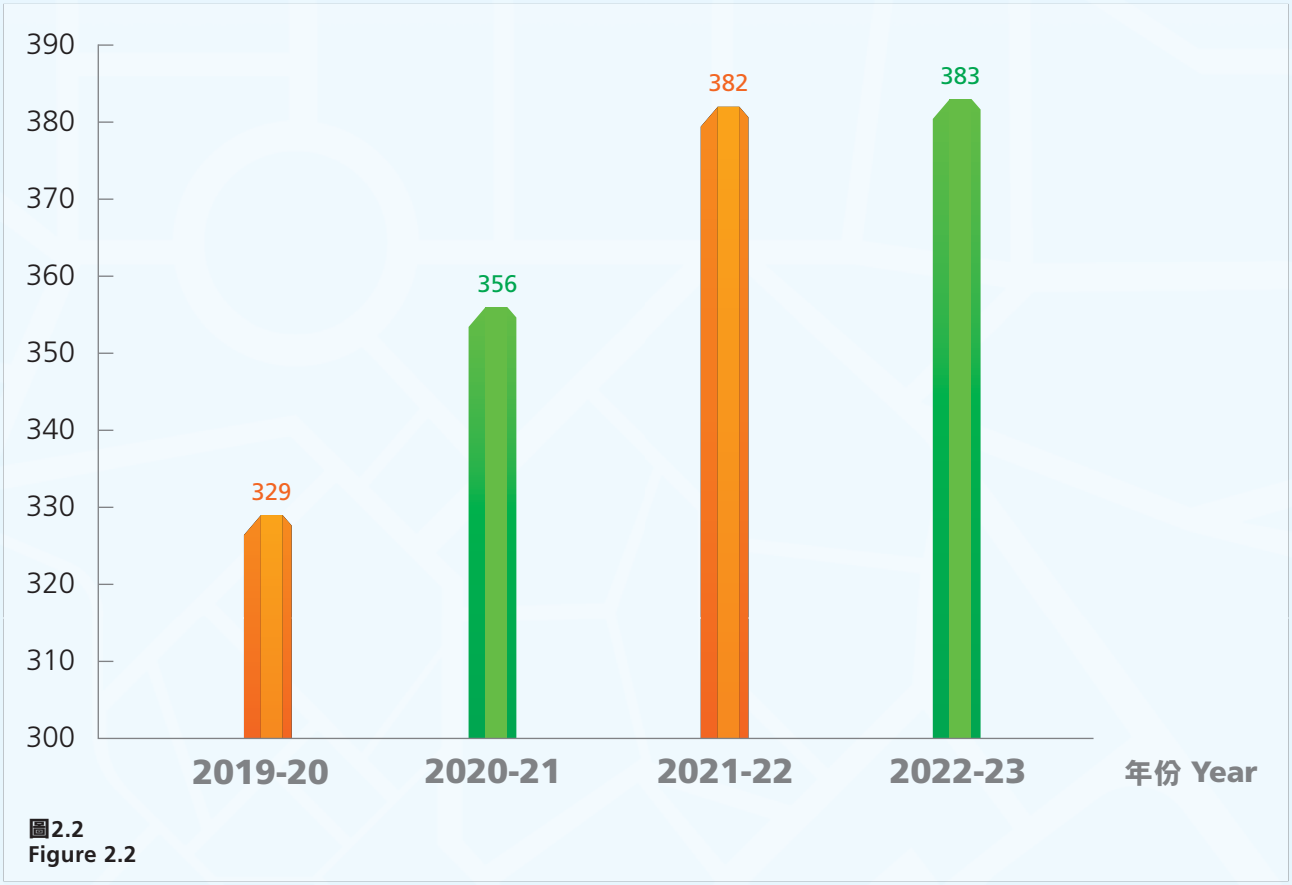


圖2.2
Figure 2.2

資料外洩事故通報

資料外洩事故一般指資料使用者持有的個人資料疑似或已經遭到外洩，令有關資料當事人的個人資料有被未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。資料外洩事故有可能構成違反《私隱條例》附表1的保障資料第4原則的規定。資料使用者在發現資料外洩事故時應盡快向私隱專員及受影響的資料當事人作出通報，尤其是當該資料外洩可能會給受影響的資料當事人帶來實際的傷害風險，以減低資料外洩事故的影響及妥善處理有關事故。

私隱專員公署在接獲資料外洩事故通報後，會仔細評估有關資料，以考慮是否有需要對有關機構展開循規審查或調查。在完成循規審查或調查後，私隱專員一般會指出資料使用者的不足之處，並建議他們採取補救措施以防止和避免同類事故重演。

在報告年度內，私隱專員公署接獲98宗資料外洩事故通報（39宗來自公營機構及59宗來自私營機構），共涉及約79萬名人士的個人資料。這些外洩事故涉及黑客入侵、遺失文件或便攜式裝置、經電郵、郵件或即時通訊軟件意外披露個人資料、僱員未經授權查閱，以及系統錯誤設定等。公署對這98宗事故均展開了循規審查或調查。（圖2.3）

Data Breach Notifications

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user, which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use. A data breach may amount to a contravention of Data Protection Principle (DPP) 4 in Schedule 1 in the PDPO. Data users should give a data breach notification to the Privacy Commissioner and the affected data subjects as soon as practicable after becoming aware of a data breach incident, in particular if the data breach is likely to result in a real risk of harm to those affected data subjects. This will minimise the impact of a data breach and ensure proper handling of such an incident.

Upon receiving a data breach notification, the PCPD would carefully assess the information provided and determine whether the situation warrants the initiation of a compliance check or investigation. Upon completing a compliance check or investigation, the Privacy Commissioner would generally point out deficiencies of the data user and suggest remedial actions to prevent and avoid the recurrence of similar incidents.

In the reporting year, the PCPD received 98 data breach notifications (39 from the public sector and 59 from the private sector), involving the personal data of about 790,000 individuals. These data breach incidents involved hacking, loss of documents or portable devices, inadvertent disclosure of personal data by email, post or instant messaging applications, unauthorised access to personal data by internal staff and system misconfiguration, etc. The PCPD conducted a compliance check or investigation for each of these 98 incidents. (Figure 2.3)

資料外洩事故通報數目
Number of Data Breach Notifications Received

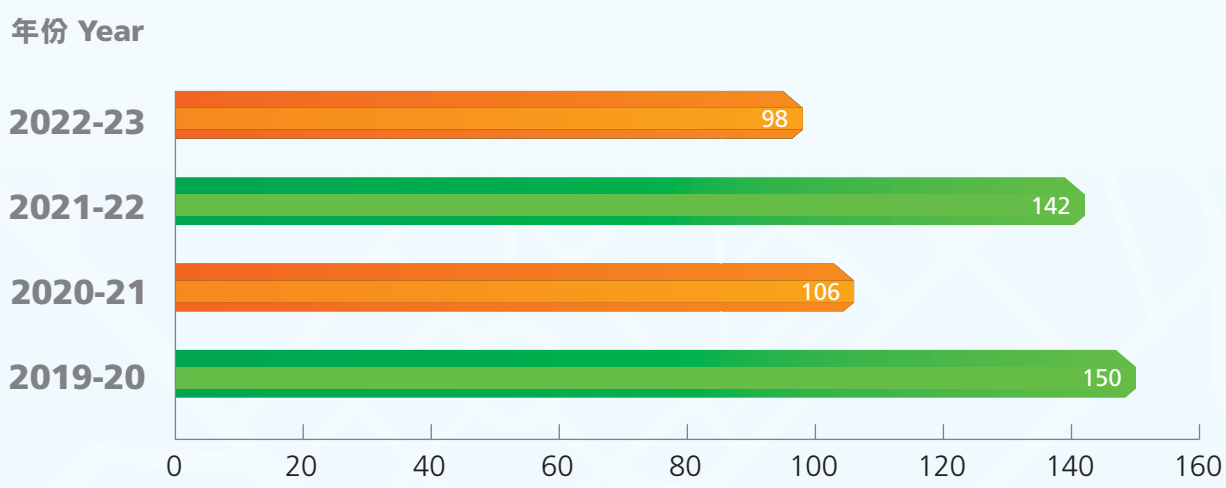


圖2.3
Figure 2.3

循規調查

在報告年度內，私隱專員公署就資料使用者作出的五宗資料外洩事故通報發表四份調查報告。

一間醫療機構外棄置病人醫療紀錄

一間醫療機構向私隱專員公署通報，指旗下一間醫務中心(該醫務中心)意外棄置一個載有病人醫療紀錄的紙箱(該紙箱)。事件涉及該醫務中心294名病人。

Compliance Investigations

During the reporting year, the PCPD published four investigation reports in relation to five data breach incidents reported by data users.

Accidental Disposal of Medical Records of Patients by a Medical Institution

A medical institution reported to the PCPD that one of its medical centres (Medical Centre) had accidentally disposed of a carton box (Carton Box) which contained patients' medical records. The incident affected a total of 294 patients at the Medical Centre.

根據調查所獲得的證據，私隱專員發現該醫療機構在以下方面存在嚴重不足，導致該紙箱在可避免的情況下遭意外棄置：

(1) 員工的個人資料保障意識欠奉；

(2) 欠缺有效的資料保障政策及程序；及

(3) 欠缺提供個人資料保障方面的員工培訓。

在這個案中，私隱專員發現該醫療機構在個人資料的保安方面存在嚴重不足，私隱專員認為該醫療機構沒有採取所有切實可行的步驟以確保涉事的醫療紀錄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，因而違反了《私隱條例》保障資料第 4(1)原則有關個人資料保安的規定。私隱專員已向該醫療機構送達執行通知，指示該醫療機構糾正以及防止有關違規情況再發生。

From the evidence collected in the investigation, the Privacy Commissioner found that the medical institution had the following serious deficiencies which contributed to the accidental yet avoidable disposal of the Carton Box:

(1) Lack of staff awareness of personal data protection;

(2) Lack of effective data protection policies and procedures; and

(3) Lack of staff training on personal data protection.

In the present case, the Privacy Commissioner found that the medical institution had serious deficiencies in ensuring the security of personal data. The Privacy Commissioner considered that the medical institution had not taken all practicable steps to ensure that the medical records in question be protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) concerning the security of personal data under the PDPO. The Privacy Commissioner issued an Enforcement Notice to the medical institution, directing it to remedy and prevent the recurrence of the contravention.

一間影像沖曬公司的數據庫遭勒索軟件攻擊

一間影像沖曬公司向私隱專員公署通報，指其網上商店的數據庫於2021年10月26日遭勒索軟件攻擊及惡意加密。事件合共影響544,862名會員及73,957名曾在2020年11月16日至2021年10月26日期間於該公司網上商店訂購產品及／或接受服務的客戶。

Ransomware Attack on the Database of a Photofinishing Company

A photofinishing company reported to the PCPD that its database of its online store (Database) had been attacked by ransomware and maliciously encrypted on 26 October 2021. A total of 544,862 members and 73,957 customers who had ordered products and/or accepted services from its online store between 16 November 2020 and 26 October 2021 were affected by the incident.

根據調查所獲得的證據，私隱專員發現該公司在以下方面存在嚴重不足，導致該數據庫在可避免的情況下被黑客利用保安漏洞入侵系統並存取個人資料：

(1) 錯誤評估保安漏洞的風險；

(2) 資訊系統管理有欠妥善；及

(3) 拖延啟用多重認證功能。

在這個案中，私隱專員發現該公司在個人資料風險意識及個人資料保安措施方面存在嚴重不足，導致公司的數據庫遭勒索軟件攻擊。私隱專員認為該公司沒有採取所有切實可行的步驟以確保涉事的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，因而違反了《私隱條例》保障資料第4(1)原則有關個人資料保安的規定。私隱專員已向該公司送達執行通知，指示該公司糾正違規情況以及防止違規情況再發生。

Based on the evidence collected in the investigation, the Privacy Commissioner found that the company had the following serious deficiencies, which contributed to the avoidable exploitation of a vulnerability and access to personal data in the Database by the hacker:

(1) Misevaluation of security vulnerability risks;

(2) Deficiencies in information system management; and

(3) Procrastinated implementation of multi-factor authentication.

In the present case, the Privacy Commissioner found that the company had serious deficiencies in risk awareness and personal data security measures, which led to the ransomware attack on the Database. The Privacy Commissioner considered that the company had not taken all practicable steps to ensure that the personal data involved was protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) concerning the security of personal data under the PDPO. The Privacy Commissioner issued an Enforcement Notice to the company, directing it to remedy the contravention and prevent its recurrence.

某政府部門兩宗個人資料外洩事故

個案(一):一員工錯誤地把載有選民資料的檔案以電郵發送至不明收件人

個案(一)發生之時正值本地第五波2019冠狀病毒病疫情肆虐,當時該政府部門作出特別在家工作安排,把職員分成不同組別交替在家工作,以減少社交接觸。涉案的文書主任(該文書主任)獲安排在某些日子在家工作。

該文書主任擬把兩個載有約15,000名選民登記資料(包括中英文姓名及住址資料)的試算表檔案(該兩個檔案)傳送至其私人電郵帳戶,以方便她翌日在家工作。然而該文書主任卻輸入了錯誤的電郵地址,導致該兩個檔案被傳送至不明收件人。該文書主任留意到她傳送的電郵在十多分鐘後仍未送達她的私人電郵帳戶,才發現出錯。該文書主任遂向助理選舉主任報告情況。

根據調查所獲得的證據,私隱專員認為以下原因導致個案(一)的發生:

(1) 職員沒有遵從該政府部門有關資訊科技保安的指引;

(2) 該政府部門職員的資料保障意識不足;及

(3) 該政府部門的資訊保安措施不足。

Two Personal Data Breach Incidents of a Government Department

Case (1): A Staff Member Wrongly Dispatched Files Containing the Data of Electors by Email to an Unknown Recipient

Case (1) occurred during the period when the fifth wave of COVID-19 ran rampant. At that time, the government department implemented special work-from-home arrangements by dividing staff into different teams to work from home alternately to reduce social contact. The clerical officer involved in the incident (Clerical Officer) was arranged to work from home on certain days.

The Clerical Officer intended to send two Excel files which contained the particulars of about 15,000 electors (including their Chinese and English names and residential addresses) (Two Excel Files) to her personal email account to facilitate her work from home the following day. However, she input an incorrect email address that the Two Excel Files were sent to an unknown recipient. She only realised the mistake when she noticed that she had not received the email in her personal email account after about 10 minutes. The Clerical Officer then reported the situation to the Assistant Electoral Officer.

According to the evidence obtained during the investigation, the Privacy Commissioner considered that the following reasons led to the occurrence of Case (1):

(1) Failure of the staff to comply with the guidelines issued by the government department on information technology security;

(2) Inadequate awareness of data protection among the staff of the government department; and

(3) Inadequate information security measures implemented by the government department.

私隱專員認為這宗個案主要涉及人為錯誤。資料外洩事故源於個別職員的疏忽和缺乏資料保障意識，以致違反該政府部門有關資訊科技保安的指引，包括「僅使用部門的電郵系統以電郵方式傳送保密資料」及「不可使用個人電郵帳戶處理公務或傳送保密資料或個人資料」。有關職員在沒有充分考慮所涉及的安全風險及未有仔細核對收件人的電郵地址的情況下，單純地為方便在家工作而將載有大量個人資料的電郵發送到該政府部門電郵系統以外的錯誤電郵地址。另一方面，私隱專員發現該政府部門在事發前並未設置適當的資訊保安措施，令職員可隨意將載有個人資料的檔案透過該政府部門的電郵系統發送到其電郵系統以外的私人電郵地址，亦是這宗個案發生的肇因。

The Privacy Commissioner considered that the incident was mainly caused by human errors. The data breach incident stemmed from the negligence and lack of awareness of data protection of the individual staff member, which led to the contravention of the relevant guidelines of the government department on information technology security, including "(staff should) only use the email system of the government department for transmission of classified information through email" and " (staff should not) use personal email accounts for official duties or for transmitting classified information or personal data". Simply for the convenience of working from home, the staff member sent an email containing a huge amount of personal data of electors to an incorrect email address outside the email system of the government department without sufficient consideration of the associated security risks and without carefully verifying the recipient's email address. On the other hand, the Privacy Commissioner also found that the government department had not put in place appropriate information security measures prior to the incident, which allowed staff to freely send files which contained personal data to personal email addresses outside the email system of the government department. This was another contributing factor of the incident.

<u>個案(二)：一員工錯誤地將一名選舉委員會委員送交的回條夾附在測試電郵內</u>

<u>Case (2): A Staff Member Wrongly Attached a Reply Slip Submitted by an Election Committee Member to a Test Email</u>

個案(二)在該政府部門準備舉行2022年行政長官選舉(該選舉)時發生。為準備該選舉，該政府部門計劃於2022年4月27日發送測試短訊及／或電郵給已提供流動電話號碼及／或電郵地址的選委及／或其助理，以確保他們能接收與選舉有關的資訊。

Case (2) occurred in the preparatory stage for the 2022 Chief Executive Election (Election). To prepare for the Election, the government department planned to issue test SMS and/or email messages on 27 April 2022 to Election Committee (EC) members and/or their assistants who had provided their mobile phone numbers and/or email addresses to ensure that they could receive information related to the Election.

該政府部門在收到選委及其助理提供的聯絡資料回條後，以人手將回條上涉及約1,800名選委及其助理的資料輸入至一份電腦資料總表(該資料總表)。可是，由於該資料總表仍存在不準確的資料，於是便要分批次核對電郵地址及發送測試電郵。

After receiving the reply slips which contained contact information provided by EC members and their assistants, the government department manually input the information related to about 1,800 EC members and their assistants onto a computer list (Master List). However, inaccuracies were spotted in the Master List, which led to the checking of the email addresses and the issuing of the test emails in batches.

為加快程序，一名高級主任指示自第四批次起省略第二次檢查。直至2022年4月28日早上，職員在覆核已發出的測試電郵時，發現一個於上午4時42分發送予38名選委及26名選委助理的電郵，錯誤夾附了附有一名選委及其助理個人資料的回條，當中載有該名選委及其助理的姓名、電郵地址、電話號碼，以及該名選委的簽署。

To speed up the process, a senior officer instructed that a second check process be removed starting from the fourth batch of test emails. In the morning of 28 April 2022, it was discovered while reviewing the issued test emails that an email sent to 38 EC members and 26 assistants at 4:42 a.m. had a reply slip containing the personal data of an EC member and his assistant wrongly attached. The personal data included the names, email addresses and phone numbers of the EC member and his assistant, as well as the signature of the EC member.

根據調查所獲得的證據，私隱專員認為以下原因導致個案(二)的發生：

According to the evidence obtained during the investigation, the Privacy Commissioner considered that the following reasons led to the occurrence of Case (2):

(1) 該政府部門的相關職員疏忽及資料保障的意識不足；

(1) Negligence and inadequate awareness of data protection among relevant staff of the government department;

(2) 該政府部門的工作流程明顯存有不足；及

(2) Deficiencies in the work process of the government department; and

(3) 相關工作欠缺書面程序。

(3) Absence of written procedures for the relevant work.

私隱專員認為這宗個案主要是由人為錯誤所引起。這事故源於相關職員的疏忽及缺乏資料保障意識，以及該政府部門相關工作流程的不足。在這宗個案中，不準確的資料總表明顯地導致了工作流程的突然改變，以致職員須在午夜後對測試電郵擬稿中的電郵地址與電子版回條進行核對。私隱專員認為如果該政府部門備有恰當的工作流程，以確保該資料總表能適時及準確地備妥，有關職員則毋須在時間緊迫下進行最後一刻的人手核對，亦毋須利用不穩妥的方式進行核對；同時，如果相關職員在核對的過程中更為謹慎，應可避免這宗個案發生。

The Privacy Commissioner attributed the incident to human errors. The incident stemmed from the negligence and lack of awareness of data protection among relevant staff and deficiencies in the relevant workflow of the government department. In this case, the inaccuracies in the Master List apparently led to a sudden change in the workflow. As a result, there was a need to manually cross-check email addresses in draft test emails against the reply slips well past mid-night. The Privacy Commissioner considered that if the government department had a proper workflow in place to ensure the Master List was promptly and accurately prepared, the staff members involved would not have to conduct last-minute manual checking under tight time constraints or use unreliable methods to conduct the checking. Meanwhile, if the staff members involved had been more cautious in the checking process, the incident could have been avoided.

再者，該政府部門沒有就發送測試電郵的機制制定任何書面程序，因而增加了人為偏差及未有依循所需步驟的風險。私隱專員理解該政府部門職員進行最後一刻的核對時所面對的壓力，但書面程序的欠缺無可避免地增加了人為錯誤的風險，尤其是考慮到當職員須長時間工作，以及為了加快整個工作流程而省略了第二次檢查，以致削弱了原先三層檢查機制的有效性。

In addition, the government department did not have any written procedures on the mechanism of sending test emails, thus increasing the risks of human errors and non-compliance with the necessary steps. The Privacy Commissioner understood that staff of the government department were working under huge pressure during last-minute checks. However, the lack of written procedures inevitably increased the risks of human errors, especially when the staff had to work prolonged hours, and the removal of the second checking to expedite the whole process undermined the effectiveness of the original three-tier checking mechanism.

綜合而言，私隱專員認為兩宗個案突顯該政府部門沒有採取所有切實可行的步驟以確保個人資料受到保障，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，因而違反了《私隱條例》保障資料第4(1)原則有關個人資料保安的規定。因此，私隱專員已向該政府部門送達兩份執行通知，指示該政府部門糾正以及防止有關違規情況再發生。

Overall, the Privacy Commissioner considered that the two incidents revealed that the government department had not taken all practicable steps to ensure that personal data was protected from unauthorised or accidental access, processing, erasure, loss or use, and therefore had contravened DPP 4(1) concerning the security of personal data under the PDPO. Consequently, the Privacy Commissioner served two Enforcement Notices on the government department directing it to remedy the contravention and prevent its recurrence.

一間非牟利學會遭勒索軟件攻擊

一間非牟利學會向私隱專員公署通報資料外洩事故，指其名下六台載有個人資料的伺服器遭勒索軟件攻擊及惡意加密，一名黑客威脅會將該些伺服器內的檔案上載至互聯網，並要求該學會支付贖金，為已被加密的檔案解鎖。事件導致超過13,000名會員及約10萬名非會員的個人資料外洩。

Ransomware Attack on the Servers of a Non-profit Institution

A non-profit institution reported to the PCPD that six servers containing personal data had been attacked by ransomware and maliciously encrypted. A hacker had threatened to upload the files in the servers to the internet and demanded a ransom from the institution to unlock the encrypted files. The personal data of over 13,000 members and about 100,000 non-members were leaked in the incident.

根據調查所獲得的證據，私隱專員認為該學會在資料保安風險意識及個人資料保安措施方面存在以下不足：

From the evidence collected in the investigation, the Privacy Commissioner found deficiencies in the institution's awareness of data security risks and its personal data security measures, namely:

(1) 資料保安風險管理欠佳；

(1) Inadequacies in the management of data security risks;

(2) 資訊系統管理有欠妥善；及

(2) Deficiencies in information system management; and

(3) 未適時啟用多重認證功能。

(3) Prolonged implementation of multi-factor authentication.

在這個案中，私隱專員發現該學會在資料保安風險管理及個人資料保安措施方面存在明顯不足，導致載有個人資料的伺服器遭勒索軟件攻擊。私隱專員認為該學會欠缺有效的資料保安風險管理機制，在保養關鍵的網絡設備上對服務提供者採取寬鬆態度，導致載有個人資料的資訊系統的保安措施無法有效應對網絡安全風險和威脅。私隱專員經調查後認為該學會沒有採取所有切實可行的步驟以確保涉事的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，因而違反了《私隱條例》保障資料第4(1)原則有關個人資料保安的規定。私隱專員已向該學會送達執行通知，指示該學會糾正以及防止有關違規情況再次發生。

In this case, the Privacy Commissioner found that there were apparent deficiencies in the data security risk management and personal data security measures of the institution, leading to the ransomware attack on its servers which contained personal data. The Privacy Commissioner considered that the institution lacked an effective data security risk management mechanism and adopted a lax approach towards service providers responsible for maintaining critical network infrastructure. As a result, the security measures of the information system which contained personal data were inadequate in addressing cybersecurity risks and threats. Upon the conclusion of the investigation, the Privacy Commissioner considered that the institution had not taken all practicable steps to ensure that the personal data involved was protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) concerning the security of personal data under the PDPO. The Privacy Commissioner served an Enforcement Notice on the institution, directing it to remedy the contravention and prevent its recurrence.

私隱專員透過上述調查個案向處理個人資料的機構提供以下建議：

Through these investigation cases, the Privacy Commissioner made the following recommendations to organisations which process personal data:

<u>機構性措施</u>

- 設立個人資料私隱管理系統，負責任地使用及保留個人資料；
- 委任保障資料主任，監察《私隱條例》的遵從並向高級管理層匯報；
- 就非常規的工作安排進行私隱風險評估並制訂具針對性的指引；

<u>Organisational Measures</u>

- Establish a Personal Data Privacy Management Programme (PMP) for the responsible use and retention of personal data;
- Appoint Data Protection Officer(s) to monitor compliance with the PDPO and report any issues to the senior management;
- Conduct privacy risk assessments and formulate specific guidelines for non-routine work;

- 向僱員提供全面的培訓，將個人資料保障滲入其日常工作之中，以減低因意識不足所引致的人為錯誤；及
- 妥善監督服務提供者。

- Provide employees with comprehensive training to incorporate personal data protection into their daily duties, with a view to reducing human errors caused by a lack of awareness; and
- Monitor service providers appropriately.

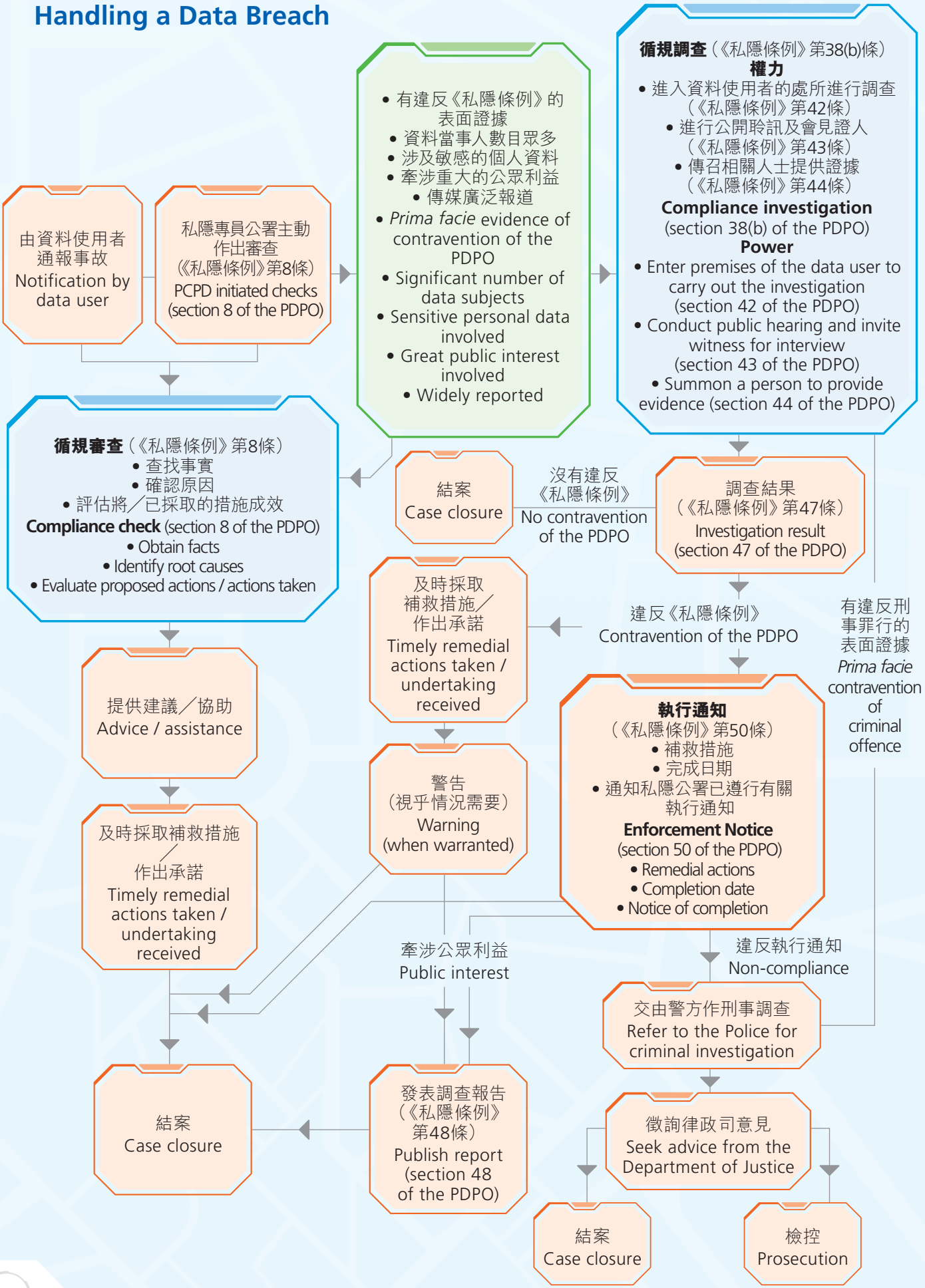
資訊保安措施

- 應時刻提高警覺以防止黑客攻擊，定時進行風險評估以檢視黑客攻擊對系統可能帶來的影響；
- 提升資訊系統管理，包括制訂有效的修補程式管理程序，盡早修補保安漏洞；及
- 確實執行數據備份，制訂數據備份政策，定期備份含有重要資料的系統。

Information Security Measures

- Stay vigilant to prevent hacker attacks by conducting regular risk assessments to review the potential impact of hacking on their systems;
- Enhance information systems management, including developing effective patch management procedures to patch security vulnerabilities as early as possible; and
- Conduct data backup conscientiously, including formulating a data backup policy and conducting regular backup for systems containing important data.

如何處理資料外洩事故
Handling a Data Breach



視察

視察原因

私隱專員公署一直致力就各界遵守《私隱條例》條文作出監察及監管，包括行使《私隱條例》第36條的權力，到持有大量市民個人資料的機構並對其資料系統進行實地視察。隨着數碼資訊科技急速發展，加上信貸資料服務機構的服務被廣泛地使用，社會對信貸資料庫的保安期望大大提升。在2022年，私隱專員依據《私隱條例》第36條對環聯資訊有限公司（環聯）進行視察，審視他們的個人資料系統。

視察結果及建議

視察結果顯示，環聯重視保障其持有的個人資料，採取了良好的行事常規，其個人信貸資料系統的保安措施符合國際標準。環聯已經接納私隱專員公署的意見建立個人資料私隱管理系統並委任專責人員作為保障資料主任，有系統地建立一套遵從《私隱條例》規定的制度，以收集、持有、處理及使用個人資料。私隱專員認為環聯在保障其持有的個人資料方面，符合《私隱條例》附表1的保障資料第4原則有關個人資料保安的要求。

Inspection

Reasons for Inspection

The PCPD is committed to monitoring and supervising compliance with the provisions of the PDPO, including exercising the powers under section 36 of the PDPO to carry out site inspections of the data systems of organisations handling vast amounts of personal data. With advancing technology and widespread use of credit reference agencies' services, public expectations on the data security measures adopted by credit reference agencies regarding their consumer credit databases have been increasing. In 2022, the Privacy Commissioner, pursuant to section 36 of the PDPO, carried out an inspection of the personal data system of TransUnion Limited (TransUnion).

Findings and Recommendations

The findings of the inspection reveal that TransUnion attached great importance to the personal data it holds and adopted good practices. The security measures of its consumer credit data system conformed to international standards. TransUnion accepted the advice of the PCPD to implement a PMP and appoint a designated Data Protection Officer to establish a proper system for collecting, handling, processing and using personal data in compliance with the PDPO. The Privacy Commissioner considered that in terms of protecting personal data, TransUnion had complied with the requirements in DPP 4 in Schedule 1 in the PDPO regarding the security of personal data.

視察期間，環聯因應私隱專員公署的建議推行免費「信貸提示服務」，當訂閱「信貸提示服務」人士的信貸報告出現重要變動（例如更改電話號碼或地址，出現申請查詢或帳戶開設），環聯會透過電郵通知該人士，讓該人士知悉其信貸報告的變動，並可以預早作出防範或跟進。此外，環聯亦因應私隱專員的建議推出一項服務，讓被「起底」或懷疑被「起底」的人士，可在其信貸報告中加入備註，讓使用環聯個人信貸資料服務的信貸提供者（即銀行或財務機構）查閱該名人士的信貸報告時得悉此事，在審核該人士的信貸申請時可作參考。

During the inspection, following the PCPD's advice, TransUnion launched a free "Credit Alert Service", alerting subscribers by email of crucial changes to their credit reports (e.g. changes to telephone numbers or addresses, or application enquiries or opening of accounts). The alerts allow individuals to be aware of changes in their credit reports and take early preventive measures or remedial action. TransUnion also launched a feature, on the advice of the Privacy Commissioner, to allow individuals who were victims or suspected victims of doxxing to add remarks to their credit reports. These remarks alert credit providers using TransUnion's consumer credit reference service (i.e. banks or financial institutions) when reviewing credit reports and assessing individuals' credit applications.

私隱專員透過視察結果，向需要處理大量客戶個人資料的機構作出數項建議，包括設立個人資料私隱管理系統及委任專責人員作為保障資料主任、制訂地區性政策及監控個人資料的查閱情況等，以確保符合《私隱條例》的規定。

Through the findings of the inspection, the Privacy Commissioner made several recommendations to organisations handling vast amounts of customers' personal data, including, for example, the implementation of a PMP, appointment of a designated Data Protection Officer, and development of local policies and monitoring access to personal data to ensure compliance with the PDPO.

核對程序申請

核對程序是指以自動化方法比較兩套因不同目的而收集的個人資料，每一項比較涉及10名或以上資料當事人的資料，而核對資料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。

Matching Procedure Requests

A data matching procedure automatically compares two sets of personal data collected for different purposes, each involving the personal data of 10 or more data subjects. The results of the comparison may be used to take adverse action against the data subjects concerned. A data user shall not carry out a matching procedure without the prescribed consent of all data subjects involved or the Privacy Commissioner.

在報告年度內，私隱專員公署共收到37宗來自政府部門的個人資料核對程序申請。經審閱後，私隱專員在附加條件的情況下批准了35宗申請，一宗申請因未有足夠資料而被拒，而另一宗則與之前一宗已獲批准的申請重疊而毋須再獲批准。

During the reporting year, the PCPD received 37 applications from government departments to carry out matching procedures. Upon examination, 35 applications were approved, subject to the conditions imposed by the Privacy Commissioner. One application was rejected due to insufficient information while another one was unnecessary as it repeated a previously approved application.

推廣合規

Promoting Compliance

發表《社交媒體私隱設定大檢閱》報告

Publication of Report on "Comparison of Privacy Settings of Social Media"

使用社交媒體及即時通訊軟件已成為香港人日常生活的一部分，近年公眾亦漸趨關注使用社交媒體的個人資料私隱風險。在2022年4月，私隱專員公署發表《社交媒體私隱設定大檢閱》報告，當中檢視和評估香港十大最常使用的社交媒體(即Facebook、Facebook Messenger、Instagram、LINE、LinkedIn、Skype、Twitter、WeChat、WhatsApp及YouTube)在私隱功能、私隱政策及私隱版面易用性的表現。

The use of social media and instant messaging applications is very much part of everyday life for Hong Kong people. In recent years, the public has become increasingly aware of the personal data privacy risks of using social media. In April 2022, the PCPD published a report on "Comparison of Privacy Settings of Social Media", which covered a review and assessment of the privacy functions, privacy policies and usability of privacy dashboards of the top 10 most commonly used social media platforms in Hong Kong (namely, Facebook, Facebook Messenger, Instagram, LINE, LinkedIn, Skype, Twitter, WeChat, WhatsApp and YouTube).

私隱專員公署基於檢視結果，向社交媒體營運者提供有關加強保護個人資料的具體建議，包括建議社交媒體營運者應持續採取「貫徹私隱的設計」，優化其服務，並向用戶提供更多私隱相關功能，增加用戶的選擇。另一方面，公署向社交媒體用戶提供建議，並提議社交媒體用戶如何更好地保障個人資料私隱，包括在註冊帳戶前細閱社交媒體的私隱政策、開設專為社交媒體而設的電郵帳戶，並只提供必須的個人資料。

Based on the review findings, the PCPD provided specific advice to the social media platform operators to enhance personal data protection. This includes continuously adopting "Privacy by Design" to enhance their services and provide more privacy-related functions to users so as to provide more choices to users. The PCPD also provided advice to social media users, including, for example, reading the privacy policy of the social media carefully before registering an account, opening an email account dedicated to social media and only providing the necessary personal data.