監察及監管符規
Monitoring and Supervising Compliance


INVESTIGATION
REPORT

回應公眾查詢

私隱公署在本報告年度接獲16,944宗公眾查詢個案，比上年度減少7%，平均每個月處理超過1,400宗查詢個案。（圖1.1）

查詢有關收集及使用個人資料（例如：香港身份證號碼及／或副本）的事宜佔整體查詢29%，而其他的主要查詢類別包括：處理與僱傭關係相關的個人資料(8%)及《私隱條例》的應用(7%)。私隱公署亦接獲與2019冠狀病毒病疫情有關的資料保障議題的查詢，主要涉及僱主收集及使用僱員的健康資料及在家工作安排下個人資料的保障。

隨着針對「起底」行為的《修訂條例》於2021年10月8日生效，市民查詢關於私隱公署處理投訴程序的個案有所增加(8%)。與「起底」及《私隱條例》相關條文的查詢共有217宗。

Responding to Public Enquiries

A total of 16,944 public enquiry cases were received during the reporting year, down 7% from that of the previous reporting year. On average, over 1,400 public enquiry cases were handled per month. (Figure 1.1)

The collection and use of personal data (e.g. Hong Kong Identity (HKID) Card numbers and/or copies) constituted 29% of total enquiries. The nature of other enquiries included the handling of personal data in employment relationships (8%) and the application of the PDPO (7%). The PCPD also received public enquiries on data privacy issues relating to the COVID-19 pandemic, mainly concerning the collection and use of employees' health data and the protection of personal data under work-from-home arrangements.

Following the implementation of the Amendment Ordinance targeting doxxing acts on 8 October 2021, there was an increase in public enquiries relating to the PCPD's complaint handling policy (8%). 217 enquiry cases were associated with doxxing and the related provisions of the PDPO.

查詢個案數目
Number of Enquiries Received

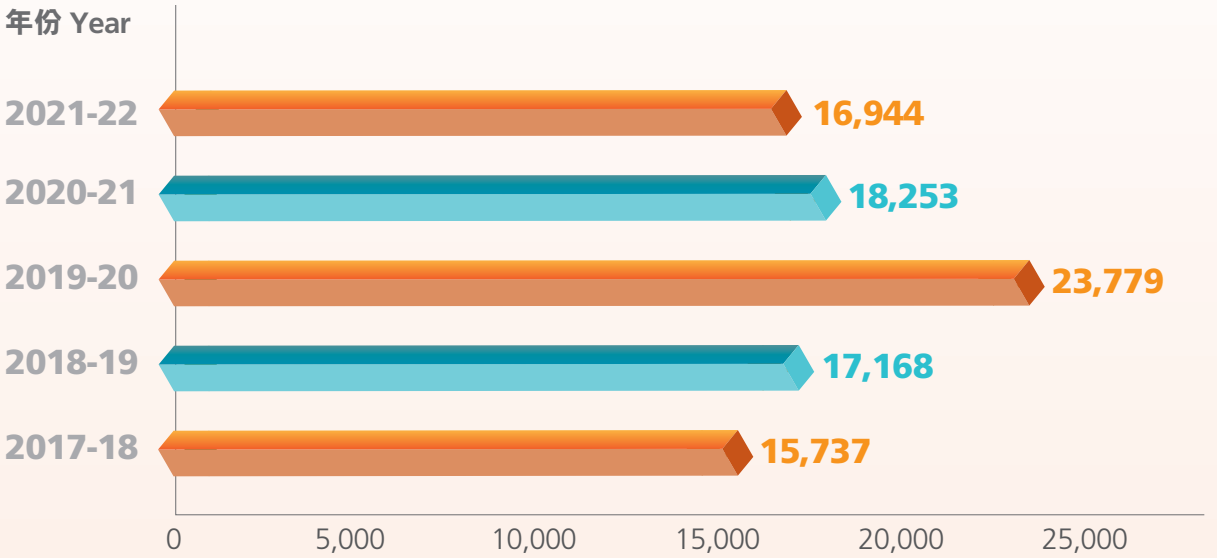


圖 Figure 1.1

監察及推廣遵守《個人資料(私隱)條例》的規定

當私隱公署發現有機構的行事方式與《私隱條例》規定不相符時，私隱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382次循規行動，較2020-21年度的356次上升7%。(圖1.2)

Monitoring and Promoting Compliance with the Personal Data (Privacy) Ordinance

In cases where the PCPD finds that there is an inconsistency between an organisation's practices and the requirements under the PDPO, the PCPD will initiate compliance checks or investigations. Upon completion of a compliance action, the Privacy Commissioner will generally point out any inconsistencies or deficiencies to the organisation, and advise the organisation to take remedial action to correct the breaches and preventive action to avoid recurrence of similar incidents.

During the reporting year, the Privacy Commissioner carried out 382 compliance actions, an increase of 7% compared to 356 in 2020-21. (Figure 1.2)

循規行動數目
Number of Compliance Actions Made

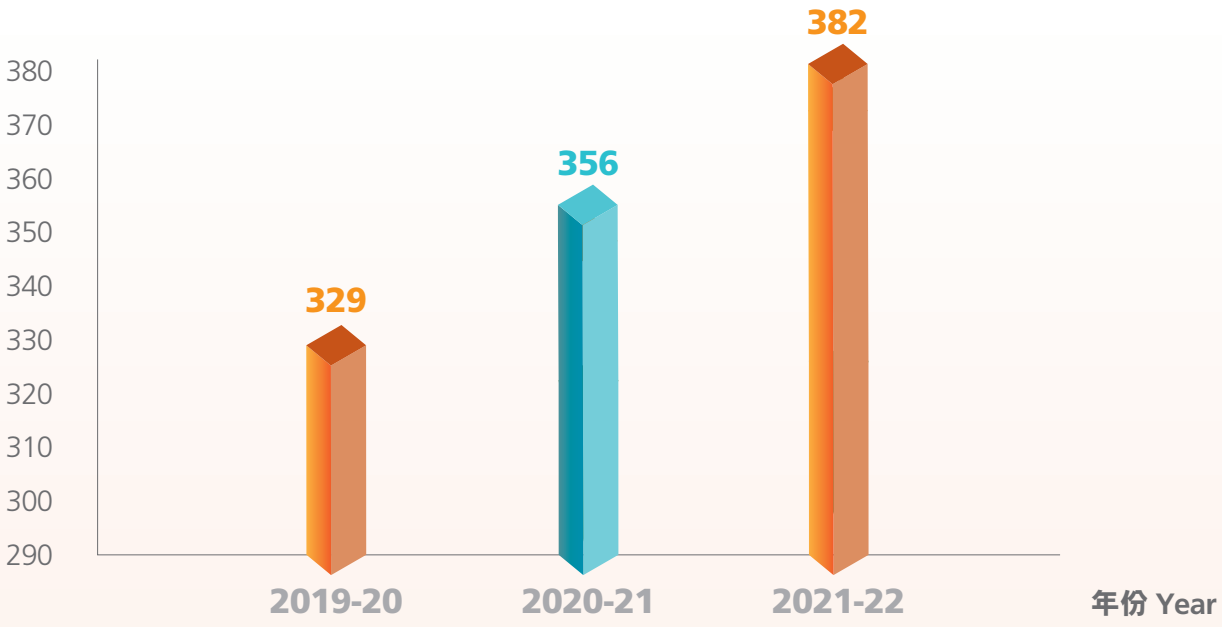


圖 Figure 1.2

視察

視察原因

私隱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。

公用事業公司在管理服務帳戶、處理帳單及客戶查詢的日常業務中處理大量客戶資料。在2021年，私隱專員依據《私隱條例》第36條對中華電力有限公司(中電)及香港電燈有限公司(港燈)進行視察，審視他們的客戶個人資料系統。

視察結果及建議

視察結果顯示，中電及港燈均實施了個人資料私隱管理系統，以及採取了良好的行事常規。兩間公司的客戶個人資料系統的保安措施符合國際準則，令人滿意。私隱專員認為兩間公司在保障客戶個人資料方面，符合《私隱條例》中附表1的保障資料第4原則有關個人資料保安的要求。

私隱專員透過上述視察結果，亦向處理大量個人資料的公用事業機構和組織作出數項建議，包括設立個人資料私隱管理系統及委任保障資料主任，以確保符合《私隱條例》的規定。

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 which handle a vast amount of personal data.

Public utility companies handle a vast amount of customers' data in their normal business of maintaining service accounts, processing bills and handling customer enquiries. In 2021, the Privacy Commissioner, pursuant to section 36 of the PDPO, carried out inspections of the customers' personal data systems of CLP Power Hong Kong Limited (CLP) and The Hongkong Electric Company, Limited (HKE).

Findings and Recommendations

The findings revealed that both CLP and HKE had implemented a Personal Data Privacy Management Programme and had adopted good practices. The security measures adopted by the two companies regarding their customers' personal data systems conformed with international standards and were found to be satisfactory. The Privacy Commissioner considered that in the protection of their customers' personal data, the two companies had complied with the requirements of Data Protection Principle (DPP) 4 of Schedule 1 to the PDPO as regards the security of personal data.

Through the findings of the inspection, the Privacy Commissioner also made several recommendations to public utility companies and organisations which handled a vast amount of personal data including, for example, the implementation of a Personal Data Privacy Management Programme and appointment of Data Protection Officers to ensure compliance with the requirements of the PDPO.

資料外洩事故通報

資料外洩事故一般是指因資料使用者的保安不足或存有漏洞，以致所持有的個人資料外洩，從而引致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。為減低資料外洩事故的影響及糾正相關保安漏洞，私隱公署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。

私隱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。私隱專員對相關資料使用者進行循規行動後，一般會指出明顯的不足之處，並建議他們採取補救措施，防止和避免同類事故重演。

在報告年度內，私隱公署接獲142宗資料外洩事故通報（42宗來自公營機構及100宗來自私營機構），涉及約68萬名人士的個人資料。這些外洩事故涉及黑客入侵、遺失文件或便攜式裝置、經傳真、電郵或郵件意外披露個人資料、僱員未經授權查閱、意外銷毀個人資料，以及系統錯誤設定等。私隱公署對這142宗事故均展開了循規審查或調查。（圖1.3）

Data Breach Notifications

In general, a data breach occurs when inadequate security or vulnerabilities of personal data held by a data user exist, thereby exposing the data to the risks of unauthorised or accidental access, processing, erasure, loss or use. The breach may be found to be in contravention of DPP 4 of Schedule 1 to the PDPO. To minimise the impact of a data breach and rectify the relevant security vulnerabilities, data users are encouraged to give a data breach notification to the affected data subjects, the Privacy Commissioner, and other relevant parties after a data breach has occurred.

Upon receipt of a data breach notification, the PCPD would carefully assess the information provided and decide whether the situation warrants the initiation of a compliance check or an investigation. When the compliance action is completed, the Privacy Commissioner would generally advise on the particular deficiencies of the data user and make suggestions for remedial action to prevent and avoid further breaches of a similar nature in future.

During the reporting year, the PCPD received 142 data breach notifications (42 from the public sector and 100 from the private sector), involving the personal data of around 680,000 individuals. The data breach incidents included hacking, loss of documents or portable devices, inadvertent disclosure of personal data by fax, email or post, unauthorised access of personal data by internal staff, accidental erasure of personal data and system misconfiguration, etc. The PCPD conducted a compliance check or an investigation into each of these 142 incidents. (Figure 1.3)

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

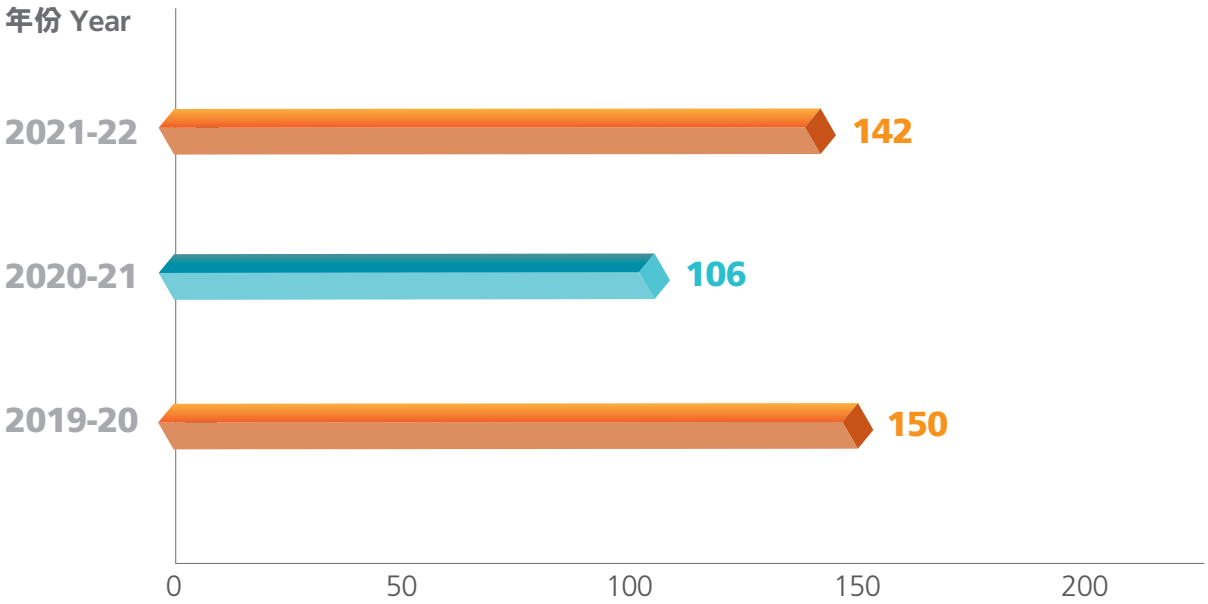


圖 Figure 1.3

循規調查

在報告年度內，私隱公署發表了一份資料外洩事故的調查報告。

一間公司向私隱公署通報，指其六個員工的電郵帳戶曾遭黑客入侵，導致發送至該些電郵帳戶的電郵被轉發至兩個不明的電郵地址。事件導致超過1,600名客戶的個人資料外洩，包括他們的姓名、電郵地址、公司名稱、電話號碼及信用卡資料。私隱公署就事件展開調查。

Compliance Investigation

During the reporting year, the PCPD published an investigation report in relation to a data breach incident.

A company reported to the PCPD that a hacker had intruded into the email accounts of six staff members and forwarded the emails therein to two unknown email addresses. The incident resulted in the leakage of 1,600 customers' personal data, including their names, email addresses, company names, telephone numbers and credit card information. The PCPD initiated an investigation into the incident.

私隱公署發現該公司的電郵系統於事故發生時在保安方面明顯地存在以下四項不足：

(1) 薄弱的密碼管理；

(2) 保留已過時的電郵帳戶；

(3) 公司的電郵系統欠缺針對遠端存取的保安措施；及

(4) 欠缺針對其資訊系統的保安措施。

The PCPD found that the following four deficiencies existed in the security of the company's email system at all material times:

(1) Weak password management;

(2) Retention of obsolete email accounts;

(3) Lack of security controls for remote access to the company's email system; and

(4) Inadequate security controls on its information system.

私隱公署經調查後認為該公司未有採取所有切實可行的步驟，以確保其持有的客戶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。私隱公署向該公司送達執行通知，指示該公司糾正以及防止有關違規情況再發生。

The PCPD considered, upon conclusion of the investigation, that the company had failed to take all practicable steps to ensure that its customers' personal data was protected against unauthorised or accidental access, processing or use, thereby contravening DPP 4(1) as regards the security of personal data under the PDPO. The PCPD issued an Enforcement Notice to the company to direct it to remedy and prevent recurrence of the contravention.

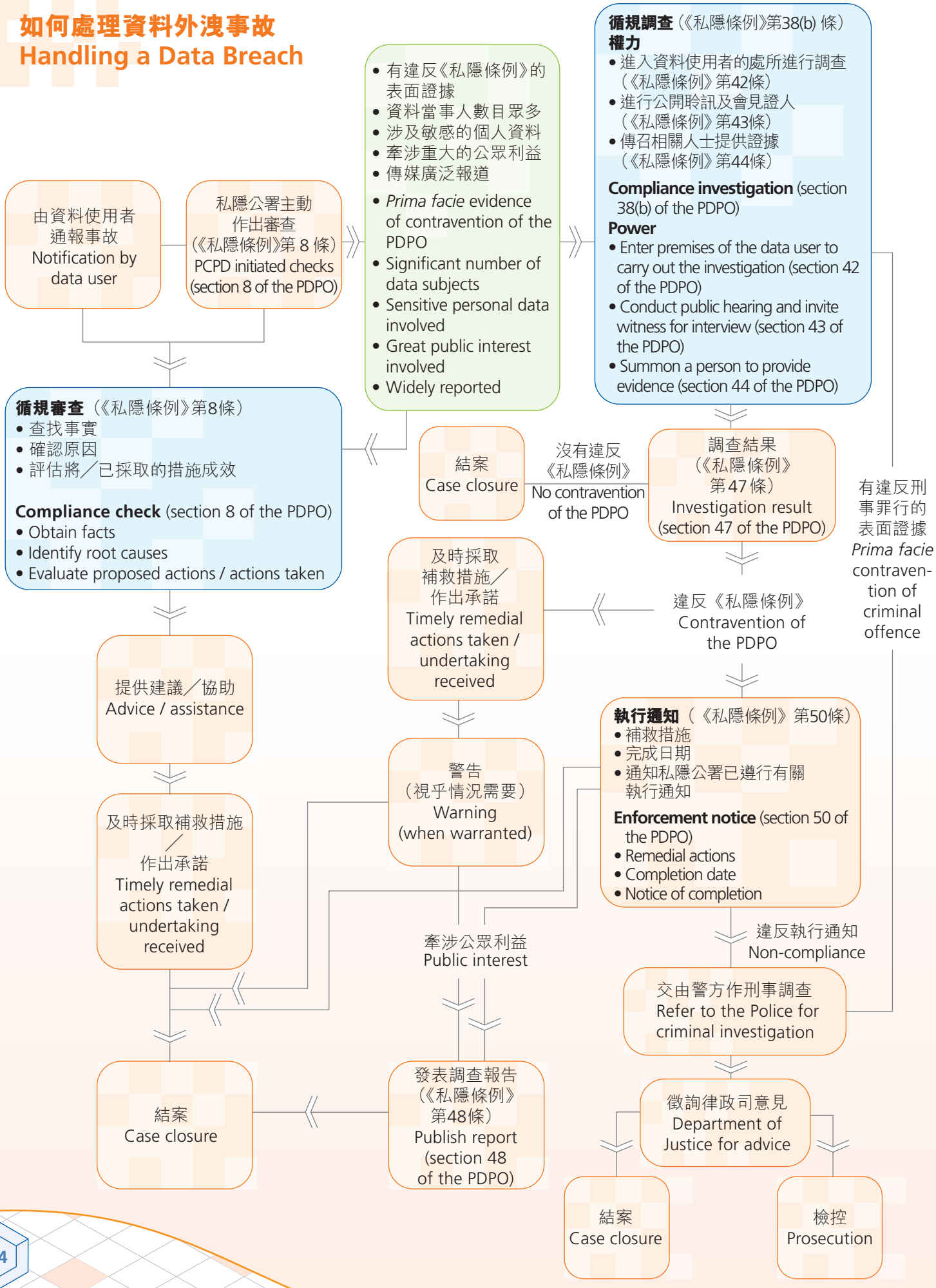
私隱公署提醒設有客戶個人資料電郵系統的機構需加強警惕，以防止網絡攻擊影響其電郵系統。機構應制定適當的系統安全政策、措施和程序，並涵蓋以下領域：

The PCPD reminded organisations with email systems which handled customers' personal data to be vigilant about cyberattacks targeting their email systems. Adequate policies, measures and procedures covering system security should be put in place, and should cover the following areas:

- 設立個人資料私隱管理系統；
- 委任保障資料主任；
- 訂定電郵通訊政策；
- 制定足夠保安措施；及
- 培養工作場所的私隱友善文化。

- Establishing a Personal Data Privacy Management Programme;
- Appointing Data Protection Officer(s);
- Devising policy on email communications;
- Implementing adequate security measures; and
- Instilling a privacy-friendly culture in the workplace.

如何處理資料外洩事故
Handling a Data Breach



處理核對程序申請

核對程序是指以電子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，私隱公署共收到43宗個人資料核對程序申請，全部來自政府部門及公營機構。經審閱後，私隱專員在附加條件的情況下批准了上述所有申請。

Handling Requests for Matching Procedure

A data matching procedure involves the electronic comparison of two sets of personal data, each of which is collected for different purposes. Each comparison involves the personal data of 10 or more data subjects. The result of the comparison may be used for taking adverse action against the data subjects concerned. A data user shall not carry out a matching procedure without the prescribed consent from all data subjects involved or the Privacy Commissioner.

During the reporting year, the PCPD received a total of 43 applications from government departments and public-sector organisations to carry out matching procedures. After vetting, the Privacy Commissioner approved all of these applications, with conditions imposed.