合規
Compliance

公眾查詢

在本報告年度，私隱專員公署接獲18,381宗查詢個案，較上報告年度增加14%，平均每個月處理約1,500宗查詢個案（圖3.1），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12%及4%。

大部分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）（25%）、私隱專員公署的投訴處理政策（12%）、《私隱條例》的應用（7%）、僱傭關係的個人資料處理（6%）、查閱與更正個人資料的權益（6%）及安裝與使用閉路電視設備情況（5%）。

有關誘騙個人資料的查詢不斷增加，由上報告年度的903宗增至本報告年度的1,094宗，增幅為21%。本報告年度私隱專員公署接獲1,143宗關於「起底」的查詢，較2023-24年度的942宗上升21%。

1 包括透過私隱專員公署的一般查詢熱線（2827 2827）、「AI安全」熱線、「數據安全」熱線及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）的查詢。

Public Enquiries

During the reporting year, the PCPD received a total of 18,381 enquiry cases, an increase of 14% compared to the preceding reporting year. On average, around 1,500 enquiry cases were handled each month (Figure 3.1). Enquiries made by telephone[1] accounted for the vast majority (84%) of these cases, while those made in writing and in person made up 12% and 4% of the total number respectively.

Key areas of enquiries included the collection and use of personal data (e.g. Hong Kong Identity Card numbers and/or copies) (25%), the PCPD's complaint handling policy (12%), the application of the PDPO (7%), the handling of personal data in the context of employment (6%), the rights to access and correct personal data (6%) and the installation and use of CCTV facilities (5%).

There was a continuous surge in the number of enquiries about personal data fraud, from 903 in the preceding reporting year to 1,094 in this reporting year, representing an increase of 21%. The number of enquiries related to doxxing in this reporting year was 1,143, a 21% increase from 942 in the year 2023-24.

1 Including enquiries made through the General Enquiries Hotline (2827 2827), "AI Security" Hotline, "Data Security" Hotline and 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

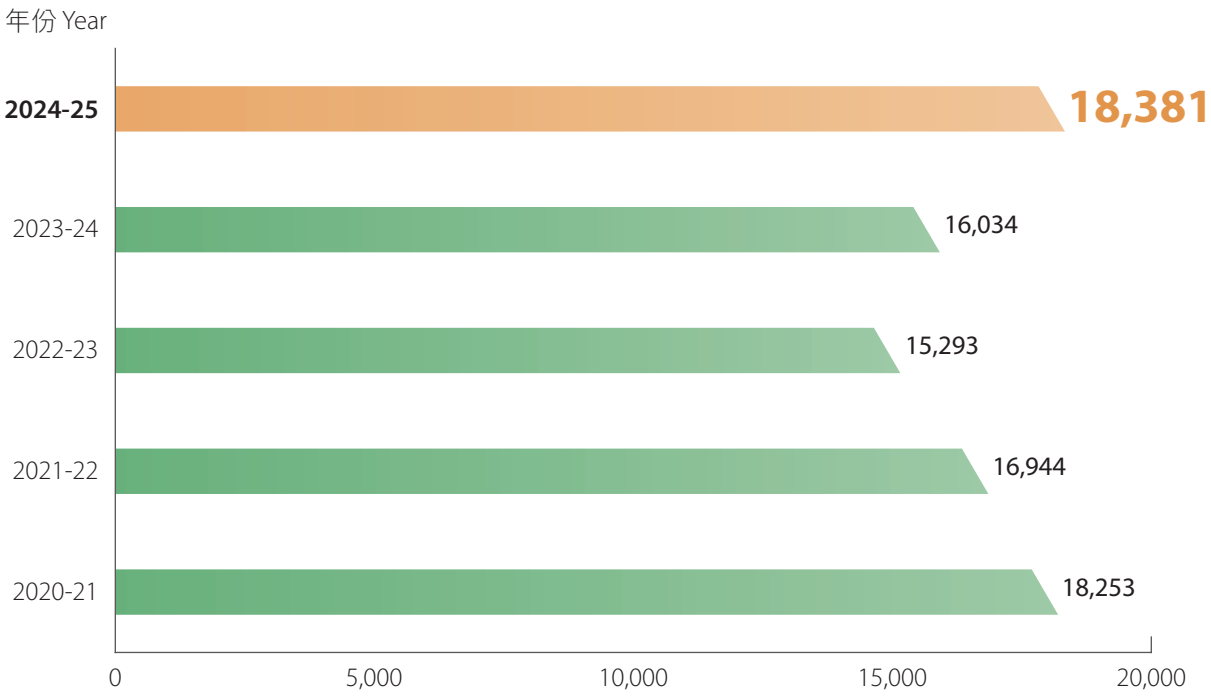


圖 Figure 3.1

循規行動

當私隱專員公署發現有機構的行事方式可能與《私隱條例》規定不相符時，公署會展開循規審查或調查。完成循規行動後，公署一般會向機構指出其行事方式與《私隱條例》規定不符之處，並促請有關機構採取適當的補救措施以糾正違規的情況，以依循《私隱條例》的規定。

私隱專員在本報告年度內一共進行443次循規行動，較上報告年度的410次多8%(圖3.2)。

Compliance Actions

When the PCPD identifies that an organisation's practices may not comply with the requirements under the PDPO, the PCPD would initiate a compliance check or investigation. Upon completion of a compliance action, the PCPD will, in the general case, inform the relevant organisation of any inconsistencies between the practices in question and the PDPO's requirements, and urge the relevant organisation to take appropriate remedial measures to rectify the contraventions, so as to comply with the requirements under the PDPO.

The Privacy Commissioner carried out 443 compliance actions during the reporting year, an 8% increase from 410 in the preceding reporting year (Figure 3.2).

循規行動數目
Number of Compliance Actions Carried Out

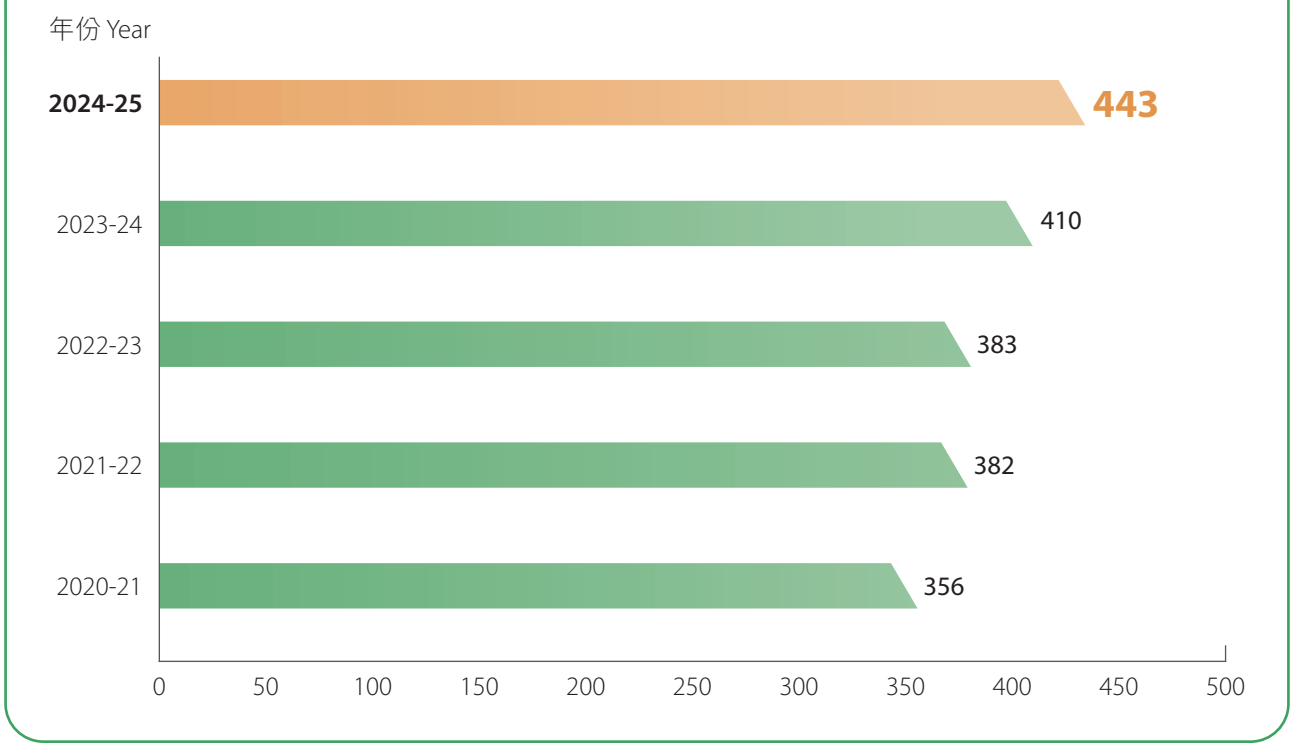


圖 Figure 3.2

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懷疑或已經外洩，面臨未經授權或意外地被查閱、處理、刪除、喪失或使用的風險。資料外洩事故可能違反《私隱條例》附表1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，私隱專員公署鼓勵資料使用者就事故通知受影響資料當事人、私隱專員和其他相關人士。

私隱專員公署在接獲資料外洩事故通報後，會仔細評估通報當中的資料，以考慮是否有需要對有關機構展開循規審查或調查。在完成循規行動後，私隱專員一般會向有關資料使用者具體指出其不足之處，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207宗資料外洩事故通報(71宗來自公營機構、136宗來自私營機構)，涉及約130萬名人士的個人資料。這些外洩事故的性質涉及黑客入侵、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、僱員未經授權查閱個人資料，以及系統錯誤設定等。公署對這207宗事故均展開了循規審查或調查(圖3.3)。

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 subjects to the risks of unauthorised or accidental access, processing, erasure, loss or use. The breach may be found to be in contravention of Data Protection Principle (DPP) 4 of Schedule 1 to the PDPO. To mitigate the impact of a data breach and rectify related security vulnerabilities, the PCPD calls on data users to notify the affected data subjects, the Privacy Commissioner and other relevant parties in the case of a data breach incident.

Upon receipt of a data breach notification, the PCPD would carefully assess the information provided to determine whether the situation warrants a compliance check on or an investigation into the organisation involved. Upon completion of the compliance action, the Privacy Commissioner would, in the general case, communicate the deficiencies found to the relevant data user and offer recommendations for remedial measures that help rectify the deficiencies and prevent its recurrence.

During the reporting year, the PCPD received a total of 207 data breach notifications (71 from the public sector and 136 from the private sector), concerning the personal data of around 1,300,000 individuals. The nature of these data breach incidents included hacking, loss of documents or portable devices, inadvertent disclosure of personal data by fax, email or post, unauthorised access to personal data by employees, and system misconfiguration, etc. The PCPD conducted a compliance check on or an investigation into each of these 207 incidents (Figure 3.3).

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

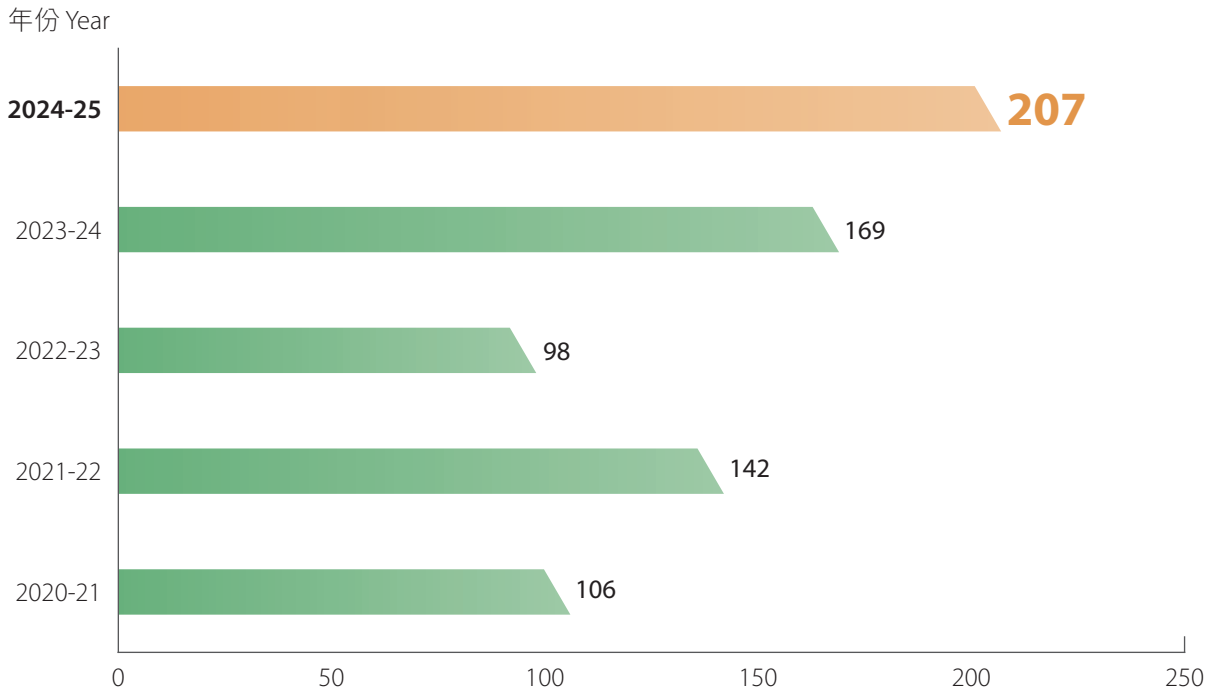


圖 Figure 3.3

循規調查

在本報告年度內，私隱專員發表了八份有關資料外洩事故的調查結果，當中六宗涉及違反《私隱條例》的規定：

Compliance Investigations

During the reporting year, the Privacy Commissioner published findings of eight investigations in relation to data breach incidents, six of which were found to be in contravention of the requirements of the PDPO:

一個學術團體的資訊系統遭勒索軟件攻擊

一個學術團體向私隱專員公署通報，指其電腦系統及檔案伺服器遭受勒索軟件攻擊。受事件影響的人士數目為8,122名，包括約7,200名電子通訊訂閱戶，另外約920名受影響人士包括青年科學家申請人、得獎者及其隨行人員、論壇大使或活動助理申請人、本地科學家及講者、評審員、活動助理，以及該團體的現職僱員、前僱員及委員。

根據調查所獲得的資料，私隱專員認為事件是由該團體以下的缺失導致：

（1）資訊系統管理有欠妥善；
（2）對服務供應商採取的資料保安措施缺乏監察；
（3）欠缺資訊保安政策及指引；及
（4）缺乏適當的數據備份方案。

基於上述情況，私隱專員認為該團體沒有採取所有切實可行的步驟，以確保涉事的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，因而違反了保障資料第4(1)原則有關個人資料保安的規定。私隱專員向該團體送達執行通知，指示其糾正以及防止有關違規情況再次發生。

Ransomware Attack on the Information Systems of an Academic Group

An academic group reported to the PCPD that its computer systems and file servers were attacked by ransomware. 8,122 individuals were affected, including approximately 7,200 e-newsletter subscribers. The other 920-odd individuals affected included applicants for young scientists, laureates and their retinues, forum ambassadors or event helper applicants, local scientists and speakers, reviewers, event helpers, current and former staff members of the academic group, as well as its board members.

From the information obtained during the investigation, the Privacy Commissioner considered that the incident was caused by the following deficiencies of the academic group:

(1) Deficiencies in information system management;
(2) Lax monitoring of the data security measures adopted by the service vendor;
(3) Lack of policies and guidelines on information security; and
(4) Lack of appropriate data backup solutions.

Based on the above, the Privacy Commissioner considered that the academic group failed to take all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) regarding the security of personal data. The Privacy Commissioner served an Enforcement Notice on the academic group to direct it to remedy the contravention and prevent its recurrence.

一個藝術團體的伺服器遭勒索軟件攻擊

一個藝術團體向私隱專員公署通報遭受勒索軟件攻擊，導致其資訊系統的四組實體伺服器受影響。根據該團體的估算，受外洩事件影響的人士數目可能為37,840名，包括該團體的僱員、求職者、門票訂購者、客席藝術家、活動參加者、捐款者、贊助者及供應商。

根據調查所獲得的資料，私隱專員認為事件是由該團體以下的缺失導致：

(1) 一組伺服器的運作軟件已過時；

(2) 相關伺服器在服務供應商進行系統遷移過程中被不必要地曝露於互聯網；

(3) 對服務供應商採取的資料保安措施缺乏監察；及

(4) 沒有對資訊系統進行保安評估及保安審計。

基於上述情況，私隱專員認為該團體沒有採取所有切實可行的步驟，以確保涉事的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，因而違反了保障資料第4(1)原則有關個人資料保安的規定。私隱專員向該團體送達執行通知，指示其糾正以及防止有關違規情況再次發生。

Ransomware Attack on the Servers of an Art Organisation

An art organisation reported to the PCPD that it suffered from a ransomware attack, which affected four physical servers of the information systems. Based on the art organisation's estimation, the number of the affected individuals might amount to 37,840, which included staff members, job applicants, ticket subscribers, guest artists, activity participants, donors, sponsors and vendors.

From the information obtained during the investigation, the Privacy Commissioner considered that the incident was caused by the following deficiencies of the art organisation:

(1) Outdated operating software of a server;

(2) Unnecessary exposure of the relevant server to the Internet during system migration performed by the service vendor;

(3) Lack of monitoring of the data security measures adopted by the service vendor; and

(4) Absence of security assessments and security audits of the information systems.

Based on the above, the Privacy Commissioner considered that the art organisation failed to take all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) regarding the security of personal data. The Privacy Commissioner served an Enforcement Notice on the art organisation to direct it to remedy the contravention and prevent its recurrence.

一個體育會的伺服器遭勒索軟件攻擊及惡意加密

一個體育會向私隱專員公署通報，表示其伺服器遭勒索軟件攻擊及惡意加密，當中涉及72,315名會員的個人資料。

根據調查所獲得的資料，私隱專員認為事件是由該體育會以下的缺失導致：

（1）相關伺服器被意外地曝露於互聯網；

（2）資訊系統欠缺有效的偵測措施；

（3）沒有為管理員帳戶啟用多重認證功能；

（4）欠缺資訊保安政策及指引；

（5）沒有定期進行風險評估及保安審計；及

（6）欠缺離線數據備份方案。

基於上述情況，私隱專員認為該體育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，因而違反了保障資料第4(1)原則有關個人資料保安的規定。私隱專員向該體育會送達執行通知，指示其糾正以及防止有關違規情況再次發生。

Ransomware Attack and Malicious Encryption on the Servers of a Sports Association

A sports association reported to the PCPD that its servers were attacked by ransomware and maliciously encrypted, which involved the personal data of 72,315 members of the association.

From the information obtained during the investigation, the Privacy Commissioner considered that the incident was caused by the following deficiencies of the sports association:

(1) Accidental exposure of the relevant server to the Internet;

(2) Lack of effective detection measures in the information systems;

(3) Failure to enable multi-factor authentication for administrator accounts;

(4) Lack of policies and guidelines on information security;

(5) Absence of regular risk assessments and security audits; and

(6) Lack of offline data backup solutions.

Based on the above, the Privacy Commissioner considered that the sports association failed to take all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) regarding the security of personal data. The Privacy Commissioner served an Enforcement Notice on the sports association to direct it to remedy the contravention and prevent its recurrence.

一個政府部門的資料外洩事故

一個政府部門於2024年5月1日向私隱專員公署通報，表示懷疑由其持有的市民個人資料外洩，當中涉及在2022年「限制與檢測宣告」行動(強檢行動)中受檢測人士的個人資料。為收集強檢行動中受檢測市民的資料，該政府部門向承辦商採購並使用一個雲端平台(該雲端平台)附設的電子表格平台(該電子表格平台)製作了14張電子表格作記錄，而相關的電子表格及資料會被儲存在該雲端平台數據儲存庫中。

該政府部門於2022年底知悉強檢行動告一段落後，隨即通知有關承辦商於2023年2月底合約屆滿後不再就該電子表格平台的服務續約。該政府部門認為在合約屆滿後，該電子表格平台的帳戶便會失效，而有關資料亦會被承辦商自動刪除。直至2024年4月30日，經私隱專員公署通知該政府部門，該政府部門才得知強檢行動中受檢測市民的個人資料可在無須輸入帳戶及密碼的情況下在該雲端平台的相關網址被瀏覽。

A Data Breach Incident of a Government Department

A government department reported to the PCPD on 1 May 2024 on a suspected data breach concerning the personal data of members of the public in its possession. It involved the personal data of individuals who had undergone testing in the "restriction-testing declaration" (RTD) operations conducted in 2022. To collect data of individuals subject to testing in the RTD operations, the government department procured and used the services of an e-form platform (the e-Form Platform) on a cloud platform (the Cloud Platform) to create 14 e-forms. The relevant e-forms and data were stored in the data repository of the Cloud Platform.

In late 2022, when the government department noted that the RTD operations had come to an end, it immediately notified the contractor of its decision not to renew the service contract after its expiry in late February 2023. The government department considered that the e-Form Platform account would be invalidated upon contract expiration, and that the relevant information would be automatically deleted by the contractor. It was not until its receipt of the PCPD's notification on 30 April 2024 that the government department learned that the personal data of individuals who had undergone testing in the RTD operations could be browsed on the relevant website of the Cloud Platform without logging into an account or entering a password.

根據調查所獲得的資料，私隱專員認為該政府部門的以下缺失是導致資料外洩事故的主因：

（1）沒有就強檢行動所收集的個人資料保存期限制定書面政策；

（2）未有清楚向承辦商提出刪除相關資料的要求；

（3）沒有自行主動刪除涉事的個人資料；及

（4）沒有適當跟進承辦商刪除資料。

基於上述情況，私隱專員認為該政府部門沒有採取所有切實可行的步驟，以確保涉事的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；及保存時間不超過使用該資料實際所需的時間，因而違反了保障資料第4(1)及2(2)原則有關個人資料保安及保留的規定。私隱專員向該政府部門送達執行通知，指示其糾正以及防止有關違規情況再次發生。

From the information obtained during the investigation, the Privacy Commissioner found that the following deficiencies of the government department were the main factors contributing to the data breach incident:

(1) Lack of written policies on the retention of personal data collected in the RTD operations;

(2) Failure to make unequivocal request to the contractor for deletion of the relevant data;

(3) Failure to take the initiative to delete the personal data involved; and

(4) Failure to properly follow up with the contractor on the deletion of data.

Based on the above, the Privacy Commissioner considered that the government department failed to take all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use; and not kept longer than was necessary for the fulfilment of the purpose for which the data was used, thereby contravening DPP 4(1) and DPP 2(2) regarding the security and retention of personal data. The Privacy Commissioner served an Enforcement Notice on the government department to direct it to remedy the contravention and prevent its recurrence.

一間非牟利機構的資訊系統遭受勒索軟件攻擊

一間非牟利機構向私隱專員公署通報，遭受勒索軟件攻擊，其資訊系統因而受到影響。黑客於2024年7月10日在該機構的資訊系統放置勒索軟件「DarkHack」，導致儲存在系統內的檔案及資料被加密及竊取。事件導致該機構共37台伺服器及24台工作電腦或手提電腦被入侵，大約550,000名資料當事人受影響。

根據調查所獲得的資料，私隱專員認為事件是由該機構以下的缺失導致：

（1）過時的防火牆存在嚴重漏洞；

（2）未有啟用多重認證功能；

（3）沒有對伺服器進行關鍵保安修補；

（4）資訊系統欠缺有效的偵測措施；

（5）對資訊系統進行的保安評估不足；

（6）資訊保安政策有欠具體；及

（7）過長地保存個人資料。

Ransomware Attack on the Information Systems of a Non-profit-making Organisation

A non-profit-making organisation reported to the PCPD that it suffered from a ransomware attack which affected its information systems. On 10 July 2024, the threat actor deployed "DarkHack" ransomware in the non-profit-making organisation's information systems, resulting in file encryption and data exfiltration. A total of 37 servers and 24 workstations or laptops belonging to the non-profit-making organisation were compromised in the incident, which potentially affected around 550,000 data subjects.

From the information obtained during the investigation, the Privacy Commissioner considered that the incident was caused by the following deficiencies of the non-profit-making organisation:

(1) Outdated firewalls with critical vulnerabilities;

(2) Failure to enable multi-factor authentication;

(3) Lack of critical security patches of servers;

(4) Ineffective detection measures in the information systems;

(5) Insufficient security assessments of information systems;

(6) Lack of specificity of its information security policy; and

(7) Prolonged retention of personal data.

基於上述情況，私隱專員認為該機構沒有採取所有切實可行的步驟，以確保涉事的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；及保存時間不超過使用該資料實際所需的時間，因而違反了保障資料第4(1)及2(2)原則有關個人資料保安及保留的規定。私隱專員向該機構送達執行通知，指示其糾正以及防止有關違規情況再次發生。

Based on the above, the Privacy Commissioner considered that the non-profit-making organisation failed to take all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use; and not kept longer than was necessary for the fulfilment of the purpose for which the data was used, thereby contravening DPP 4(1) and DPP 2(2) regarding the security and retention of personal data. The Privacy Commissioner served an Enforcement Notice on the non-profit-making organisation to direct it to remedy the contravention and prevent its recurrence.

一間品牌管理及分銷公司的伺服器遭勒索軟件攻擊

一間品牌管理及分銷公司於2024年5月31日向私隱專員公署通報，指其公司於2024年5月15日收到黑客的勒索訊息，聲稱竊取其資料並威脅出售相關資料。事件牽涉其公司營運的兩個會員計劃，合共影響127,268名人士的個人資料，包括127,254名兩個會員計劃的會員、14名該公司現職僱員及前僱員等。

根據調查所獲得的資料，私隱專員認為事件是由該公司以下的缺失導致：

（1）未有在修復系統故障後適時刪除臨時帳戶；

（2）使用已被終止支援的操作系統；

（3）資訊系統欠缺有效的偵測措施；及

（4）對資訊系統進行的保安風險評估及審計不足。

基於上述情況，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，因而違反了保障資料第4(1)原則有關個人資料保安的規定。私隱專員向該公司送達執行通知，指示其糾正以及防止有關違規情況再次發生。

Ransomware Attack on the Servers of a Brand Management and Distribution Company

A brand management and distribution company reported to the PCPD on 31 May 2024 that it received a ransom note from a threat actor on 15 May 2024, who claimed to have stolen and threatened to sell its data. The incident affected two loyalty programmes operated by the company. A total of 127,268 individuals were affected by the incident, which included 127,254 members of the two loyalty programmes, and 14 current and former employees of the company, etc.

From the information obtained during the investigation, the Privacy Commissioner considered that the incident was caused by the following deficiencies of the company:

(1) Failure to delete the temporary account timely after system troubleshooting;

(2) Use of end-of-support operating system;

(3) Ineffective detective measures for information systems; and

(4) Insufficient security risk reviews and audits for information systems.

Based on the above, the Privacy Commissioner considered that the company failed to take all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) regarding the security of personal data. The Privacy Commissioner served an Enforcement Notice on the company to direct it to remedy the contravention and prevent its recurrence.

私隱專員透過上述調查個案向持有個人資料的機構提供以下建議：

The Privacy Commissioner made the following recommendations to organisations in possession of personal data through the investigation cases:

機構性措施

- 建立重視數據安全的企業文化；
- 建立有效的培訓計劃，加強員工就數據安全及保障個人資料私隱方面的意識及能力，建立一道「人力防火牆」；及
- 設立穩健的網絡保安框架，在防範、偵測及應對網絡攻擊方面投放足夠資源及制定有效的策略及措施，以減低被攻擊的可能性及資料外洩風險。

Organisational Measures

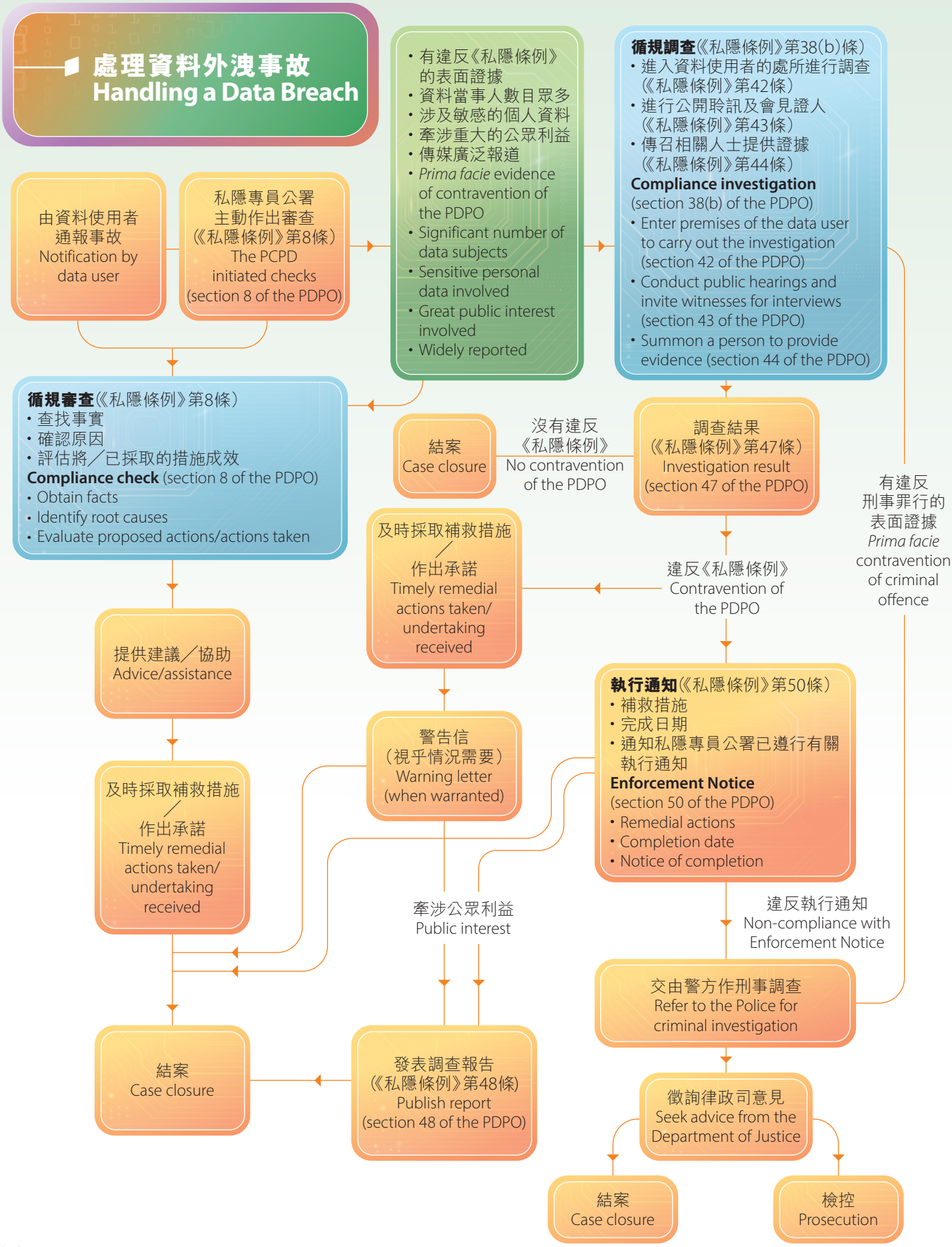
- Establish a corporate culture that values data security;
- Devise effective training plans to enhance staff awareness of and competence in data security and personal data privacy protection to build a "human firewall"; and
- Establish a robust cybersecurity framework, allocate sufficient resources and formulate effective strategies and measures to prevent, detect and respond to cyberattacks, thereby reducing the possibility of cyberattacks and the risk of data breach.

資訊保安措施

- 採用「最小權限」的原則及「角色為本」的存取管控機制，定期檢視帳戶權限及刪除不必要的帳戶；
- 對遙距登入資訊系統使用多重身分驗證；
- 定期對資訊系統進行全面的風險評估及保安審計；
- 使用防火牆等軟件保護電腦網絡；
- 停止使用已被終止支援的軟件，或適時更新軟件；
- 實施修補程式的管理；及
- 分開內部資料伺服器與網絡伺服器。

Information Security Measures

- Adopt the "least privilege" principle and "role-based" access control mechanisms, and regularly review access rights and delete unnecessary accounts;
- Adopt multi-factor authentication for remote access to information systems;
- Conduct regular and comprehensive risk assessments and security audits of information systems;
- Use firewalls and other software to protect computer networks;
- Cease the use of end-of-support software, or upgrade software timely;
- Implement patch management; and
- Separate internal database servers from web servers.


處理資料外洩事故
Handling a Data Breach
由資料使用者通報事故
Notification by data user
私隱專員公署主動作出審查（《私隱條例》第8條）
The PCPD initiated checks (section 8 of the PDPO)
• 有違反《私隱條例》的表面證據
• 資料當事人數目眾多
• 涉及敏感的個人資料
• 牽涉重大的公眾利益
• 傳媒廣泛報道
• Prima facie evidence of contravention of the PDPO
• Significant number of data subjects
• Sensitive personal data involved
• Great public interest involved
• Widely reported
循規調查《私隱條例》第38(b)條）
• 進入資料使用者的處所進行調查（《私隱條例》第42條）
• 進行公開聆訊及會見證人（《私隱條例》第43條）
• 傳召相關人士提供證據（《私隱條例》第44條）
Compliance investigation (section 38(b) of the PDPO)
• Enter premises of the data user to carry out the investigation (section 42 of the PDPO)
• Conduct public hearings and invite witnesses for interviews (section 43 of the PDPO)
• Summon a person to provide evidence (section 44 of the PDPO)
循規審查《私隱條例》第8條）
• 查找事實
• 確認原因
• 評估將／已採取的措施成效
Compliance check (section 8 of the PDPO)
• Obtain facts
• Identify root causes
• Evaluate proposed actions/actions taken
結案 Case closure
沒有違反《私隱條例》 No contravention of the PDPO
調查結果（《私隱條例》第47條） Investigation result (section 47 of the PDPO)
有違反刑事罪行的表面證據 Prima facie contravention of criminal offence
及時採取補救措施／作出承諾 Timely remedial actions taken/ undertaking received
違反《私隱條例》 Contravention of the PDPO
提供建議／協助 Advice/assistance
執行通知《私隱條例》第50條）
• 補救措施
• 完成日期
• 通知私隱專員公署已遵行有關執行通知
Enforcement Notice (section 50 of the PDPO)
• Remedial actions
• Completion date
• Notice of completion
警告信（視乎情況需要） Warning letter (when warranted)
及時採取補救措施／作出承諾 Timely remedial actions taken/ undertaking received
牽涉公眾利益 Public interest
違反執行通知 Non-compliance with Enforcement Notice
交由警方作刑事調查 Refer to the Police for criminal investigation
結案 Case closure
發表調查報告（《私隱條例》第48條） Publish report (section 48 of the PDPO)
徵詢律政司意見 Seek advice from the Department of Justice
結案 Case closure
檢控 Prosecution

視察

私隱專員公署一直積極監察及規管各界遵守《私隱條例》，包括行使《私隱條例》第 36 條的權力，派員前往持有及處理大量市民個人資料的機構，並對其資料系統進行實地視察。

Inspections

The PCPD is committed to monitoring and supervising compliance with the PDPO, including exercising the powers under section 36 of the PDPO to carry out site inspections of data systems of organisations which retain and handle a vast amount of personal data.

兩所教育機構的個人資料系統

在 2024 年，兩所教育機構向私隱專員公署通報資料外洩事故，兩宗事故均涉及資訊系統遭未經授權存取。公署已就有關教育機構的個人資料保安進行及完成循規行動。基於上述背景及針對教育機構的網絡攻擊風險增加，私隱專員依據《私隱條例》第 36 條對該兩所教育機構進行視察，審視他們的個人資料系統，以加強教育機構對其持有的個人資料之保障，防止類似事件再次發生，以及向整體教育界提供有關個人資料保安的建議，加強他們的資料保障架構。

Personal Data Systems of Two Educational Institutions

In 2024, two educational institutions reported data breach incidents to the PCPD, both involving unauthorised access to their information systems. The PCPD carried out and completed compliance actions against the educational institutions in relation to the security of personal data. Against this backdrop and the escalating risk of cyberattacks targeting educational institutions, the Privacy Commissioner, pursuant to section 36 of the PDPO, carried out inspections of the personal data systems of these two educational institutions. The inspections aimed to enhance the protection of personal data held by the educational institutions, prevent the recurrence of similar incidents, and provide recommendations to the entire education sector on enhancing data protection frameworks.

核對程序

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。資料使用者如無所有相關的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，私隱專員公署共收到33宗核對程序申請。

Matching Procedures

A 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. 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 from all data subjects involved or the consent of the Privacy Commissioner. During the reporting year, the PCPD received a total of 33 applications for carrying out matching procedures.

合規推廣

發表《實測十個網上旅遊平台收集個人資料的情況》報告

隨着網上旅遊平台及應用程式日見普及，私隱專員在2024年11月發表《實測十個網上旅遊平台收集個人資料的情況》報告，當中檢視了10個市民較常使用的網上旅遊平台（包括相關網站及應用程式），以了解有關平台收集及使用用戶個人資料的情況。該10個平台分別是（以英文字母順序排列）Agoda、東瀛遊、Expedia、金怡假期、美麗華旅遊、新華旅遊、專業旅運、Trip.com、永安旅遊及縱橫遊。

私隱專員根據檢視結果，向網上旅遊平台營運者提供良好行事方式及加強私隱保障的建議，包括實施個人資料私隱管理系統、委任保障資料主任、將保障私隱融入平台設計、只收集必須的個人資料、提供清晰易明的私隱政策、提高人工智能（AI）處理個人資料的透明度、提供便捷的刪除帳戶選項、謹慎使用第三方服務（例如付款平台）、提供足夠的用戶控制權，以及提供使用個人資料於直接促銷的選項。

另一方面，私隱專員亦建議網上旅遊平台的用戶閱讀私隱政策、調整私隱設定、注意有關直接促銷的設定、提供最少量的個人資料、留意AI的使用，以及刪除不再使用的帳戶。

Compliance Promotion

Release of Report on "A Study of the Collection of Personal Data by 10 Online Travel Platforms"

In the light of the growing popularity of online travel platforms and mobile applications, the Privacy Commissioner released a report on "A Study of the Collection of Personal Data by 10 Online Travel Platforms" in November 2024. 10 online travel platforms (including the relevant websites and mobile applications) commonly used by citizens were reviewed to understand how they collect and use the personal data of their users. The 10 platforms are (in alphabetical order) Agoda, EGL Tours, Expedia, Goldjoy Holidays, Miramar Travel, Sunflower Travel, Travel Expert, Trip.com, Wing On Travel and WWPKG.

According to the review results, the Privacy Commissioner offered recommendations to the operators of online travel platforms on the best practices and enhancement of privacy protection. They included implementing a Personal Data Privacy Management Programme, appointing a Data Protection Officer, incorporating privacy-protecting elements into the design of platforms, limiting collection of personal data to the extent that is necessary, providing a clear and easy-to-understand privacy policy, enhancing transparency in the processing of personal data by artificial intelligence (AI), providing an easily accessible option to delete accounts, using third-party services (e.g. payment systems) cautiously, providing sufficient user control, and providing options in relation to the use of personal data in direct marketing.

On the other hand, the Privacy Commissioner also advised users of online travel platforms to read the privacy policy, adjust privacy settings, pay attention to direct marketing settings, provide only the minimum amount of personal data, stay vigilant about the use of AI, and to delete unused accounts.