

PCPD



H K

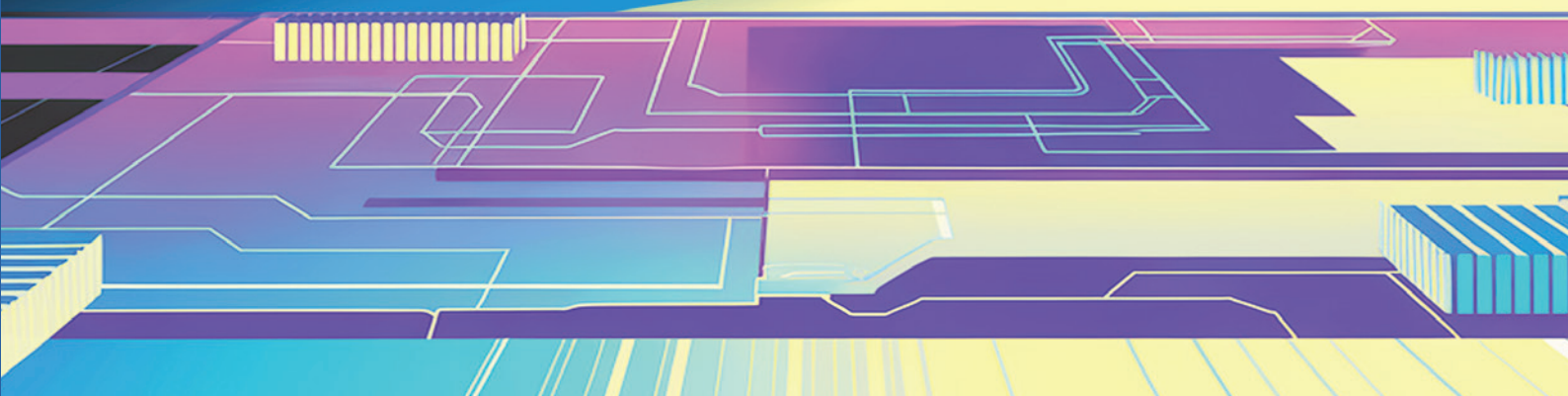
PCPD.org.hk

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

善用人工智能 構建數碼私隱新時代

LEVERAGING ARTIFICIAL INTELLIGENCE for a New Digital Privacy Era

2024-25 年報 Annual Report



目錄

Contents

2 ■ 私隱專員的話 Privacy Commissioner's Message

12 ■ 私隱專員公署簡介 About PCPD

數字回顧 A Year in Numbers
願景、使命及價值 Vision, Mission and Values
大事紀要 Key Moments of the Year
企業管治 Corporate Governance

40 ■ 構建數碼私隱新時代 Building a New Digital Privacy Era

提升人工智能安全 Enhancing Artificial Intelligence Security
加強數據安全 Fostering Data Security
打擊「起底」 Combatting Doxxing
進行調查 Conducting Investigations
提防個人資料詐騙 Preventing Personal Data Fraud
推動數據跨境流動 Promoting Cross-boundary Data Flows

72 ■ 合規 Compliance

公眾查詢 Public Enquiries
循規行動 Compliance Actions
資料外洩事故通報 Data Breach Notifications
視察 Inspections
核對程序 Matching Procedures
合規推廣 Compliance Promotion

92 ■ 投訴及上訴 Complaints and Appeals

投訴處理 Complaint Handling
向行政上訴委員會提出的上訴 Appeals Lodged with the Administrative Appeals Board

112 ■ 宣傳與教育 Promotion and Education

與不同界別聯繫 Engagement with Different Sectors
媒體拓展及宣傳 Media Outreach and Publicity
青少年教育 Youth Education

132 ■ 內地及國際聯繫 Mainland and International Connections

與內地聯繫 Connections with the Mainland
全球及地區性私隱保障網絡 Global and Regional Privacy Protection Networks

146 ■ 財務報表 Financial Statements

178 ■ 附錄 Appendices

保障資料原則 Data Protection Principles
服務承諾 Performance Pledge
上訴個案簡述 Appeal Case Notes
投訴個案選錄・以作借鑑 Summaries of Selected Complaint Cases – Lessons Learnt
定罪個案選錄・以作借鑑 Summaries of Selected Conviction Cases – Lessons Learnt
循規行動個案選錄・以作借鑑 Summaries of Selected Compliance Action Cases – Lessons Learnt

私隱專員的話

Privacy Commissioner's Message



鍾麗玲, SBS Ada CHUNG Lai-ling, SBS

個人資料私隱專員
Privacy Commissioner
for Personal Data

善用人工智能 構建數碼私隱新時代

歡迎大家參閱個人資料私隱專員公署(私隱專員公署)2024-25年度的年報。今年年報的主題圍繞着兩種「AI」——分別是**成果及影響**(Accomplishments and Impacts)，以及**人工智能**(Artificial Intelligence，AI)。

Leveraging Artificial Intelligence for a New Digital Privacy Era

Welcome to the 2024-25 Annual Report of the Office of the Privacy Commissioner for Personal Data (PCPD). The year covered by this report was defined by the dual themes of AI – **Accomplishments and Impacts**, as well as **Artificial Intelligence** (AI).

私隱專員公署過去一年工作的成果及影響碩果纍纍。年內我們在循規行動方面創下了前所未有的成績，亦主動調查多宗備受關注的案件，足證我們在執法行動上的決心，並對違反《個人資料(私隱)條例》《私隱條例》的行為採取零容忍的態度。在數碼私隱的新時代，面對數據安全及網絡安全風險日益增加，公署成功推出多項推廣數據安全的措施，提升大眾對數據安全重要性的認知。

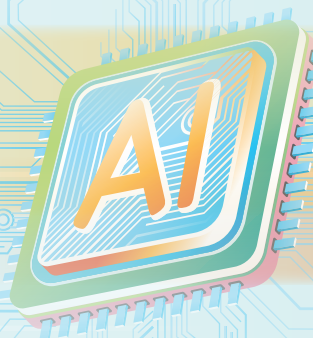
在AI領域方面，私隱專員公署採取的措施在本地以至國際間均引起不少迴響。我們出版了香港首份有關AI的個人資料保障模範框架，引導香港業界及機構在使用AI時負責任地保障個人資料。與此同時，我們聯同環球私隱或資料保障監管機構，在AI領域尋求創新與安全的微妙平衡。

本年報充分反映私隱專員公署一直堅守的價值，同時展示公署作為「改革者」的決心和發展，以及我們如何在瞬息萬變的數碼世界中識變、應變及求變。

The accomplishments and impacts can be seen through our work over the year, during which we achieved record-breaking results in compliance actions and proactively commenced investigations into multiple high-profile cases, demonstrating our commitments to enforcement actions and zero tolerance of breaches of the Personal Data (Privacy) Ordinance (PDPO). In the face of escalating data security and cybersecurity risks, we successfully launched a multitude of data security initiatives to drive home the importance of safeguarding data security in this new digital privacy era.

In the realm of AI, our initiatives have created impacts both locally and globally. We published the city's inaugural model personal data protection framework for AI to steer Hong Kong's industries and organisations towards the responsible protection of personal data in using AI, while spearheading efforts to strike a delicate balance between innovation and security in AI among global privacy or data protection regulators.

This Annual Report reflects the long-standing values of my Office that shone through the year – a year marked by determination and growth as a reformer for the PCPD, showcasing our drive to proactively identify, respond to and steer changes in the rapidly evolving digital landscape.



2024-25的主要數字

作為個人資料私隱的守護者，私隱專員公署於2024-25年度致力在各方面履行職能，保障個人資料私隱。報告年度內，我們：

Notable Figures in 2024-25

As the guardian of personal data privacy, we are dedicated to upholding the protection of individuals' personal data privacy by fulfilling our responsibilities on all fronts in 2024-25. During the reporting year, we:

- 接獲**3,450**宗投訴個案；
Received **3,450** complaints;
- 處理**370**宗「起底」個案；
Handled **370** doxxing cases;
- 展開**134**次調查；
Commenced **134** investigations;
- 接獲**207**宗資料外洩事故通報；
Received **207** data breach notifications;
- 接獲**18,381**宗公眾查詢；
Received **18,381** public enquiries;
- 進行**443**次循規行動；
Conducted **443** compliance actions;
- 展開**88**次刑事調查；
Initiated **88** criminal investigations;
- 採取**20**次拘捕行動並拘捕**21**人；
Mounted **20** arrest operations and arrested **21** persons;
- 發布**62**篇新聞稿；
Issued **62** media statements;
- 回應**225**宗傳媒查詢；
Responded to **225** media enquiries;
- 各媒體發布了**3,024**則與私隱專員公署工作相關的新聞；
Noted **3,024** news reports relating to the PCPD's work across various media channels;
- 錄得每月平均**344,610**人次瀏覽私隱專員公署網站；
Logged an average of **344,610** visits to the PCPD's website each month;
- 於社交媒體發表**671**篇帖文；及
Published **671** social media posts; and
- 錄得**57,900**人次參加私隱專員公署的講座、研習班及工作坊。
Recorded **57,900** attendances at the PCPD's talks, seminars and workshops.

2024-25年度重點工作

果斷執法 監管符規

一如既往，私隱專員公署堅決果斷地採取執法行動。2021年10月8日生效的《2021年個人資料(私隱)(修訂)條例》賦予公署的全方位機制，對簡化及加快針對「起底」案件的執法和檢控行動而言十分關鍵，我們年內的傑出成果亦充分反映此機制的成效。

與2022-23報告年度(即「起底」新條文生效後首年)相比，經私隱專員公署主動網上巡查發現的「起底」個案下跌92%，由2022-23年度的841宗下跌至本報告年度的65宗。與「起底」相關的投訴亦下跌55%，由676宗下跌至305宗。

同時，我們展開了88次刑事調查並採取了20次拘捕行動，拘捕人數達21人。私隱專員公署亦發出多份停止披露通知，成功移除3,482則「起底」訊息，「起底」訊息移除率達98.3%，情況令人鼓舞。

至於處理投訴及循規行動方面，我們於報告年內發表多份調查報告，包括一個加密貨幣項目在香港運作的調查結果，以及有關八間機構透過一個網上招聘平台刊登匿名招聘廣告的調查結果。此外，經檢視10個本港市民較常使用的網上旅遊平台收集及使用個人資料的情況後，我們在2024年11月發表《數碼時代的私隱保障：實測十個網上旅遊平台收集個人資料的情況》報告。

Highlights of Our Work in 2024-25

Proactive Enforcement and Compliance Supervision

As with previous years, my Office spared no effort to take enforcement actions. Effective from 8 October 2021, the Personal Data (Privacy) (Amendment) Ordinance 2021 has empowered the PCPD to adopt a holistic approach that has been instrumental in streamlining and expediting enforcement and prosecution actions against doxxing cases, as highlighted by the outstanding results we accomplished over the year.

When compared to the 2022-23 reporting year (i.e. the first year after the commencement of the new anti-doxxing regime), the number of doxxing cases uncovered by the PCPD's proactive online patrols dropped by 92%, from 841 cases in 2022-23 to 65 cases in the reporting year. The number of doxxing complaints also decreased by 55%, from 676 to 305.

Furthermore, we initiated 88 criminal investigations and mounted 20 arrest operations, resulting in the arrest of 21 individuals. By serving cessation notices on online platforms and removing as many as 3,482 doxxing messages, we achieved a very satisfactory removal rate of over 98.3% of doxxing messages.

As regards our work on complaints handling and compliance actions, we released multiple investigation reports during the reporting year, including one covering investigation findings on the operation of a cryptocurrency project in Hong Kong, and another regarding the act of placing "blind" recruitment advertisements on an online recruitment platform by eight organisations. In addition, we published our flagship report titled "Privacy Protection in the Digital Age: A Study of the Collection of Personal Data by 10 Online Travel Platforms" in November 2024 after reviewing the collection and use of personal data by 10 online travel platforms commonly used by citizens in Hong Kong.

多管齊下 構建數據安全堅固防線

隨着 21 世紀走入數碼轉型的年代，不論本地抑或國際間的數據安全威脅亦見增加，而且手法越趨精密。保障數據安全對維護個人資料私隱及推動可持續發展的數字經濟而言至關重要。報告年度內，我們多管齊下，透過採取不同措施及與各界協作，在各個領域推廣保障數據安全的重要性。這些措施包括提供數據安全工具、舉辦關注私隱的活動及與業界夥伴合作。

特別是，有鑑於資料外洩事故呈上升趨勢，尤其是涉及學校、非牟利機構及中小企的資料外洩事故，私隱專員公署推出了「數據安全」套餐。機構在完成「數據安全快測」評估其數據安全措施是否足夠後，可獲免費名額參加由公署舉辦的研習班及講座。機構亦可透過公署的「數據安全」專題網頁及「數據安全」熱線查閱相關資訊並尋求協助，為應對網絡安全威脅作好準備。

除了提供工具協助業界主動預防資料外洩事故，我們亦舉辦多項宣傳活動，包括在 2024 年 5 月舉辦以「數據安全保私隱」為主題的旗艦活動「關注私隱週 2024」。除了舉辦有關數據安全的研討會以及為不同機構舉辦內部培訓講座，私隱專員公署亦與業界加強合作，在推廣數據安全方面發揮協同效應。

Multi-pronged Approach to Building a Strong Data Security Defence

As the 21st century ushers in an era of digital transformation, we are simultaneously witnessing data security threats ramping up and becoming more intricate, both domestically and internationally. Safeguarding data security is critical for both upholding personal data privacy and driving a sustainable digital economy. Throughout the reporting year, we adopted a multi-pronged approach characterised by diverse initiatives and collaborative engagement to promote the importance of safeguarding data security across different sectors. These efforts included offering data security tools, launching awareness programmes and collaborating with industry partners.

In particular, owing to the upward trend in data breach incidents, particularly those involving schools, non-profit-making organisations, and small and medium-sized enterprises, we launched the “Data Security” Package, providing free quotas for participating organisations to join our professional workshops and seminars upon completion of an assessment by the “Data Security Scanner”, which assesses the adequacy of their data security measures. Organisations can also access relevant information and seek assistance via the “Data Security” thematic webpage and the “Data Security” Hotline provided by us to better equip themselves against cybersecurity threats.

Beyond equipping industries with tools to proactively prevent data breaches, we organised various promotional activities, including the flagship event “Privacy Awareness Week 2024” under the theme “Safeguard Data Security • Safeguard Privacy” in May 2024. In addition to organising seminars on data security and conducting in-house training sessions for different organisations, we also strengthened our collaboration with the industry to create synergy in promoting data security.

繼往開來 揭開人工智能安全新一頁

推廣人工智能安全一直是私隱專員公署的重點工作。繼2021年出版《開發及使用人工智能道德標準指引》及2023年出版《使用AI聊天機械人「自保」十招》單張這兩份廣受好評的指引後，公署於2024年6月適時發布亞太區在保障私隱領域其中一份最早出版且具領導地位的AI指引——《人工智能(AI)：個人資料保障模範框架》(《模範框架》)，並在2025年3月發布《僱員使用生成式AI的指引清單》(《指引》)。年內，生成式AI引發了廣泛討論，而如何在創新與安全之間取得平衡亦成為焦點議題。《模範框架》提供國際認可及切實可行的建議和最佳行事常規，以協助機構在採購、實施及使用AI，包括生成式AI時，遵從《私隱條例》的相關規定，而《指引》則着重協助機構制定僱員在工作時使用生成式AI的內部政策或指引。

《模範框架》自推出以來，廣獲本地社會各界的認同和支持，更於亞太區 GovMedia Conference & Awards 中榮獲「2025 年度香港公營機構倡議——監管組別」的獎項。這項國際級的肯定，印證私隱專員公署出版的指引在本地及國際層面均具高度參考價值與影響力。

A New Chapter in AI Security

Promoting AI security has always been a priority for my Office. Building on prior success in publishing the “Guidance on the Ethical Development and Use of Artificial Intelligence” in 2021 and the “10 TIPS for Users of AI Chatbots” leaflet in 2023, we timely issued the “Artificial Intelligence: Model Personal Data Protection Framework” (Model Framework) – one of the first leading guides on AI in the privacy landscape in the Asia-Pacific region – in June 2024, and the “Checklist on Guidelines for the Use of Generative AI by Employees” (Guidelines) in March 2025. This year was marked by intense discussions on generative AI and ongoing debates about balancing innovation and safety. The Model Framework provides internationally recognised and practical recommendations and best practices, with a view to assisting organisations in procuring, implementing and using AI, including generative AI, in compliance with the relevant requirements of the PDPO, while the Guidelines focus on assisting organisations in developing internal policies or guidelines on the use of generative AI by employees at work.

Since the publication of the Model Framework, it has garnered widespread recognition and support across various sectors of the society. My Office has won the “2025 Hong Kong Public Sector Initiative of the Year – Regulatory” award in the Asia Pacific GovMedia Conference & Awards for the Model Framework. This international accolade underscores the high reference value and impacts of our published guidance both locally and globally.

私隱專員公署委託香港生產力促進局進行有關網絡保安準備的調查，並於2024年11月發表「香港企業網絡保安準備指數及AI安全風險」調查報告結果。調查發現，大部分受訪企業（近七成）認為在營運中使用AI會帶來顯著的私隱風險，反映機構極需採用適當的指引，例如公署的《模範框架》，以緩減實施AI所帶來的私隱風險。

AI相關的風險與日俱增，已成為迫在眉睫的全球性問題。就此，私隱專員公署積極應對，與國際夥伴攜手合作。自2024年10月起，公署擔任環球私隱議會轄下的人工智能的道德與數據保障工作分組聯席主席。基於環球私隱議會是集合全球超過130個私隱或資料保障機構且具領導地位的國際平台，這標誌着我們在積極參與全球性AI管治討論方面一個重要的里程碑。

另一方面，私隱專員公署繼續擔任環球私隱議會轄下的國際執法合作工作分組聯席主席，持續關注全球數據擷取問題，包括在網上大規模擷取個人資料作訓練AI模型的情況。建基於2023年8月發表的首份聯合聲明，公署在2024年10月聯同全球15個私隱或資料保障機構，向主要社交媒體平台及公開網站發出環球聯合聲明，就保障個人資料免遭非法數據擷取向業界提供進一步指引。

My Office commissioned the Hong Kong Productivity Council to conduct a survey on cyber security readiness and released the results of the “Hong Kong Enterprise Cyber Security Readiness Index and AI Security” survey in November 2024. The survey revealed that a significant majority (around 70%) of the surveyed enterprises perceived that using AI in their operations posed significant privacy risks. This underscores the need for organisations to adopt appropriate guidelines, such as my Office’s Model Framework, to mitigate privacy risks associated with the implementation of AI.

The surge in AI-related risks has become a pressing global issue. In response, my Office has stepped up to the plate, joining forces with international partners. Since October 2024, we have taken on the role of co-chair in the Ethics and Data Protection in Artificial Intelligence Working Group under the Global Privacy Assembly (GPA). Since the GPA is a leading international forum for over 130 privacy or data protection authorities worldwide, this marks a significant milestone in our active participation in the discussions on global AI governance.

As my Office remained the co-chair of the International Enforcement Cooperation Working Group of the GPA, we continued to look into the worldwide data scraping issue, including mass extraction of personal data online for training AI models. Riding on an initial joint statement from August 2023, my Office and 15 other privacy or data protection authorities around the world issued a concluding statement to major social media platforms and public websites in October 2024, providing the industry with further guidance on protecting personal data against unlawful data scraping.

與時俱進 推廣私隱保障

個人資料保障領域瞬息萬變，私隱專員公署的推廣策略亦要因時制宜、與時俱進。其中，公署不斷優化防騙宣傳策略，以應對不斷演變的挑戰，例如AI深度偽造騙案的出現。在2024-25年度，我們繼續走進社區，在社交媒體平台、屋邨及醫院播放防騙宣傳短片、在學校舉辦防騙講座，並於中秋節及聖誕節探訪「老友記」，加強他們的防騙意識，向他們介紹公署的「防騙六招」。

Moving with the Times in Promoting Privacy Protection

Given the dynamic nature of the personal data protection landscape, our promotional efforts must also adapt and advance. In particular, we have constantly refined our anti-fraud promotional efforts to keep pace with evolving challenges, such as the emergence of AI deepfake scams. In 2024-25, we continued to reach out to the community by broadcasting anti-fraud videos on social media platforms, housing estates and hospitals, organising anti-fraud talks at schools and visiting the elderly during the Mid-Autumn Festival and Christmas periods to enhance anti-fraud awareness, featuring our "Six Tips to Prevent Fraud".



促進大灣區個人資料跨境流動

有見數據跨境流動對推動香港發展為數據中心，以及促進粵港澳大灣區（大灣區）發展數字經濟所擔當的重要角色，在報告年度內，私隱專員公署與香港政府及內地當局繼續緊密合作，促進個人信息在大灣區內安全有序跨境流動。

隨着《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同》便利措施於2024年11月擴展至全港各行各業，私隱專員公署積極投入不同宣傳及教育活動，進一步推動各界採用便利措施。

Facilitating Cross-boundary Flows of Personal Data within the Greater Bay Area

Recognising the crucial role of cross-boundary data flows in driving the development of Hong Kong as a data centre and fostering the development of digital economy within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA), my Office has continued to work closely with the Hong Kong Government and Mainland authorities to facilitate the safe and orderly cross-boundary flows of personal information within the GBA during the reporting year.

With the extension of the facilitation measures of the Standard Contract for Cross-Boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) to all sectors in Hong Kong in November 2024, we enthusiastically engage in different publicity and educational activities to further promote the adoption of the facilitation measures across industries and sectors.



展望未來

這年報涵蓋的時期見證人類歷史上AI的崛起，猶如發現「新電力」。這個變革性的時代為所有人，包括私隱專員公署帶來挑戰。展望將來，我們會繼續在瞬息萬變的數碼世界中識變、應變及求變，我與公署同事將繼續上下一心，竭力求進、守正創新，做好「改革者」的本分，以高水平安全護航國家及香港的高質量發展，推廣人工智能安全及數據安全，構建尊重個人私隱的和諧社會，改善民生，令東方之珠綻放更璀璨的輝煌。

最後，本人衷心感謝香港特別行政區政府政制及內地事務局，以及私隱專員公署兩個諮詢委員會（個人資料（私隱）諮詢委員會和科技發展常務委員會）的委員，一直支持公署的工作，推動我們取得持續的工作成果及影響。我亦感激公署敬業樂業的所有同事，他們展現專業認真的精神，群策群力、孜孜不倦地為服務市民而努力。

**讓我們同心協力，
擔當「改革者」，
共創數碼私隱新時代。**

鍾麗玲, SBS

大律師

個人資料私隱專員

2025年9月

Looking Ahead

This Annual Report covers an unprecedented period in human history marked by the rise of AI as the “new electricity”. This transformative era has brought challenges to all of us, and my Office was of no exception. Looking ahead, we would continue to proactively identify, respond to and steer changes in the constantly evolving digital privacy landscape. We would strive to embrace the role of a reformer in our innovative journey, seeking to facilitate the high quality development of the Country and Hong Kong while safeguarding a high level of security, including data security and AI security. In tandem, we would continue to promote the building of a harmonious society that respects personal privacy for the betterment of the society, a society that emits the dazzling radiance of the Pearl of the Orient.

Last but not least, I wish to extend my heartfelt gratitude to the Constitutional and Mainland Affairs Bureau of the Hong Kong SAR Government, as well as members of my Office's two advisory committees, the Personal Data (Privacy) Advisory Committee and the Standing Committee on Technological Developments. Their unwavering support has been integral to our continuous accomplishments and impacts. I would also like to acknowledge and thank the dedicated professionals of my Office for their exceptional contributions. Their collective expertise, coupled with tireless commitment, has been of profound benefit to the public good.

**Let us Embrace the Role of a Reformer to
Usher in a New Digital Privacy Era.**

Ada CHUNG Lai-Ling, SBS

Barrister

Privacy Commissioner for Personal Data

September 2025

私隱專員公署簡介

About PCPD



數字回顧 (2024年4月 — 2025年3月)

A Year in Numbers (April 2024 – March 2025)



3,450

接獲3,450宗投訴個案
Received 3,450 complaints



370

處理370宗「起底」個案
Handled 370 doxing cases



134

展開134次調查
Commenced 134 investigations



207

接獲207宗資料外洩事故通報
Received 207 data breach notifications



443

進行443次循規行動
Conducted 443 compliance actions



18,381

接獲18,381宗公眾查詢
Received 18,381 public enquiries



88

展開88次刑事調查
Initiated 88 criminal investigations



20

採取20次拘捕行動，拘捕21人
Mounted 20 arrest operations
and arrested 21 persons



225

回應225宗傳媒查詢
Responded to 225
media enquiries



62

發布62篇新聞稿
Issued 62
media statements

3,024

各媒體發布了3,024則與
私隱專員公署工作相關的新聞
Noted 3,024 news reports relating to the
PCPD's work across various media channels



344,610

錄得每月平均344,610人次
瀏覽私隱專員公署網站
Logged an average of 344,610 visits
to the PCPD's website each month



671

於社交媒體
發表671篇帖文
Published 671 social
media posts



57,900

錄得57,900人次參加私隱專員公署
的講座、研習班及工作坊
Recorded 57,900 attendances at the
PCPD's talks, seminars and workshops

願景、使命及價值

Vision, Mission and Values



願景 Vision

培養及推廣保障與尊重個人資料私隱的文化

To develop and promote a culture of protection of and respect for individual's privacy in relation to personal data

使命 Mission

透過宣傳和教育，推廣保障及尊重個人資料私隱

To promote the protection of and respect for personal data privacy through publicity and education

透過提供指引和最佳行事常規，促進合法及負責任地使用個人資料

To facilitate lawful and responsible use of personal data by providing guidance and best practices

透過有效執法，監察及監管循規情況

To monitor and supervise compliance through effective enforcement

透過持續檢視和優化，並參考全球個人資料私隱保障的標準，維持監管機制的效能

To maintain the efficacy of the regulatory regime through continuous review and enhancement, taking into account global standards for the protection of personal data privacy



價值 Values

尊重

尊重他人的個人資料私隱

Respect

Respect others' personal data privacy

誠信

行事公正專業

Integrity

Act fairly and professionally

創新

緊貼科技、社會與經濟的發展

Innovation

Embrace technological, social and economic developments

獨立

獨立於政府和其他機構

Independence

Independent from the Government and other bodies

卓越

致力追求最佳成績及最高標準

Excellence

Strive for the best results and highest standards

大事紀要

Key Moments of the Year

4月
Apr
2024

發表一宗公營機構資料外洩事故的調查結果
Released investigation findings on the data breach incident of a public organisation



舉辦「粵港澳大灣區個人信息跨境流動」研討會，吸引超過130名人士參加
Organised a seminar on “Cross-boundary Flow of Personal Information Within the Greater Bay Area”, attracting more than 130 participants



政制及內地事務局局長曾國衛, GBS, IDSM, JP與私隱專員出席立法會財務委員會特別會議，解答立法會議員的問題。私隱專員亦於立法會政制事務委員會會議上簡報公署在數碼時代保障個人資料私隱的工作

The Secretary for Constitutional and Mainland Affairs, Mr Erick TSANG Kwok-wai, GBS, IDSM, JP, and the Privacy Commissioner attended the special meeting of the Legislative Council Finance Committee to answer questions raised by Legislative Council members. The Privacy Commissioner also briefed members on the PCPD's initiatives for protecting personal data privacy in the digital age at a meeting of the Legislative Council Panel on Constitutional Affairs

5月
May
2024

發表一宗公營機構資料外洩事故的調查結果
Released investigation findings on the data breach incident of a public organisation



舉辦年度旗艦活動「關注私隱週 2024」，以「數據安全保私隱」為主題，展開一連串推廣及教育活動

Organised the annual flagship event “Privacy Awareness Week 2024” themed “Safeguard Data Security • Safeguard Privacy”, and launched a series of promotional and educational activities

5月
May
2024

完成對Worldcoin(世界幣)項目的調查並發表調查結果

Completed the investigation into the Worldcoin project and published the investigation findings

舉辦「資料外洩個案及數據安全措施分享」研討會，反應熱烈。研討會於7月再度舉辦，共吸引超過1,700名人士參加

Organised a seminar on “Lessons from Data Breach Cases and Recommended Data Security Measures”, which received an overwhelming response. The seminar was held again in July, drawing more than 1,700 participants in total



私隱專員出席其中一場反「起底」學校教育巡迴講座，向超過170名中學生講解「起底」罪行及保障網上私隱的重要性

The Privacy Commissioner attended a talk as part of the School Touring of Anti-doxxing Education Talks, and explained to more than 170 secondary school students the doxxing offences and the importance of protecting privacy online

6月
Jun
2024

發布《人工智能(AI)：個人資料保障模範框架》(《模範框架》)，提供國際認可及切實可行的建議和最佳行事常規，以協助機構在採購、實施及使用AI(包括生成式AI)時遵從《私隱條例》的相關規定

Issued “Artificial Intelligence (AI): Model Personal Data Protection Framework” (Model Framework) to provide internationally recognised and practical recommendations and best practices to assist organisations in procuring, implementing and using AI, including generative AI, in compliance with the relevant requirements of the PDPO



「私隱之友嘉許獎2023」在GovMedia Conference & Awards 2024中榮獲「香港年度最佳活動—監管組別」獎項

“Privacy Friendly Award 2023” received the “Hong Kong Campaign of the Year – Regulatory” award in the GovMedia Conference & Awards 2024



大事紀要

Key Moments of the Year

6月
Jun
2024

出席第61屆亞太區私隱機構論壇，並介紹私隱專員公署發出的《模範框架》
Attended the 61st Asia Pacific Privacy Authorities Forum and introduced the Model Framework issued by the PCPD

7月
Jul
2024

參與全球私隱執法機構網絡聯合行動，針對「誘導性設計模式」完成全球性保障私隱抽查並發表環球聯合報告
Joined the Global Privacy Enforcement Network to conduct the global privacy protection sweep on “Deceptive Design Patterns” and issued a global joint report subsequent to its completion



舉辦中學生AI實踐工作坊，讓他們認識AI所帶來的私隱風險及學習如何負責任地使用AI，吸引100名同學參加。活動亦包括參觀Microsoft微軟香港總部

Organised an AI practical workshop for secondary school students to understand the privacy risks associated with AI and learn how to use AI responsibly, attracting 100 students. The Workshop also included a visit to Microsoft Hong Kong's headquarters

舉辦「人工智能與私隱保障：發展與安全並重」研討會，吸引近1,000名人士參加

Organised a seminar on “AI and Privacy Protection: Balancing Innovation and Safety”, attracting nearly 1,000 participants



8月
Aug
2024



拍攝短片親身示範透過深度偽造技術實時換臉，提醒市民在AI時代，有相、有片也未必有真相

Produced a short video to demonstrate instant face swapping through deepfake technology, with a view to illustrating that it is easy to produce fake videos in the AI era

8月
Aug
2024

發表兩宗機構資料外洩事故的調查結果
Released investigation findings on the data breach incidents of two organisations



發布新版《身份證號碼及其他身份代號實務守則：資料使用者指引》及《身份證號碼與你的私隱》資料單張

Issued new versions of "Code of Practice on the Identity Card Number and other Personal Identifiers: Compliance Guide for Data Users" and information leaflet titled "Your Identity Card Number and Your Privacy"

9月
Sep
2024

私隱專員公署關愛義工隊上門探訪長者，送上中秋福袋並分享防騙貼士及影片，以加強長者的防騙意識

The PCPD Volunteer Team made home visits to the elderly, distributed Mid-Autumn Festival gift bags, and shared anti-fraud tips and videos to enhance awareness of fraud prevention among the elderly



出版英文新書“Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”(香港個人資料(私隱)法例的符規實務指南(第三版))，並舉辦新書發布會

Published a new book titled "Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)" and organised a book launch

分別出席2024年國家網絡安全宣傳周——香港及澳門分論壇，並於澳門分論壇上發表演講

Attended the Hong Kong and Macao sub-forums of 2024 China Cybersecurity Week respectively, and delivered a keynote speech at the Macao sub-forum



大事紀要

Key Moments of the Year

9月
Sep
2024

主動啟動對五間刊登匿名招聘廣告的機構之調查，並呼籲求職者就匿名招聘廣告提高警惕

Proactively initiated investigations against five organisations that had placed “blind” recruitment advertisements (Blind Ads) and appealed to job seekers to stay vigilant about Blind Ads



10月
Oct
2024

與香港互聯網註冊管理有限公司合作推出一系列宣傳短片，協助機構提高員工對網絡安全及保障個人資料私隱的意識

Jointly launched a series of promotional videos with the Hong Kong Internet Registration Corporation Limited to assist organisations in raising employees' awareness of cybersecurity and personal data privacy protection



政制及內地事務局局長曾國衛, GBS, IDSM, JP 與私隱專員出席立法會政制事務委員會政策簡報會，解答立法會議員的問題

The Secretary for Constitutional and Mainland Affairs, Mr Erick TSANG Kwok-wai, GBS, IDSM, JP, and the Privacy Commissioner attended the Policy Briefing meeting of the Legislative Council Panel on Constitutional Affairs to answer questions raised by Legislative Council members

發表一宗體育會資料外洩事故的調查結果，以及為學校、非牟利機構及中小企推出「數據安全」套餐

Released investigation findings on the data breach incident of a sports association and launched the “Data Security” Package for schools, non-profit-making organisations (NGOs) and small and medium-sized enterprises (SMEs)



出席香港網絡安全高峰會2024並發表題為「人工智能與保障個人資料：挑戰及管治上的建議」的主題演講

Attended the Cyber Security Summit Hong Kong 2024 and delivered a keynote speech titled “AI and Personal Data Protection: Challenges and Recommendations on Governance”

聯同全球 15 個私隱或資料保障機構共同就數據擷取及私隱保障向社交媒體平台發表環球聯合聲明

Issued a global joint statement with 15 privacy or data protection authorities worldwide on data scraping and the protection of privacy to social media platforms

11月
Nov
2024



於香港國際電腦會議 2024 發表題為「在 AI 時代保障個人資料私隱：管治上的建議」的主題演講

Delivered a keynote speech titled "Safeguarding Personal Data Privacy in the Age of AI: Governance Recommendations" at the Hong Kong International Computer Conference 2024

舉辦「保障私隱學生大使・學校夥伴嘉許計劃 2024」暨「AI 新世代保障私隱領袖培訓計劃」嘉許典禮，表揚 67 間中學成為「學校夥伴」，向合共超過 17,000 名學生推動私隱友善的校園文化

Organised the Award Presentation Ceremony for "Student Ambassador for Privacy Protection Programme – Partnering Schools Recognition Scheme 2024" cum "Future Leaders of AI and Privacy Protection Training Programme" to commend 67 secondary schools as "Partnering Schools" in promoting a privacy-friendly culture to over 17,000 students on campus



發表《數碼時代的私隱保障：實測十個網上旅遊平台收集個人資料的情況》報告

Released a report on "Privacy Protection in the Digital Age: A Study of the Collection of Personal Data by 10 Online Travel Platforms"

發表「香港企業網絡保安準備指數及 AI 安全風險」調查報告

Released the "Hong Kong Enterprise Cyber Security Readiness Index and AI Security" survey report



大事紀要

Key Moments of the Year

11月
Nov
2024

出席第62屆亞太區私隱機構論壇，並參與題為「亞太區人工智能及新興科技的治理：觀點與措施」的專題討論

Attended the 62nd Asia Pacific Privacy Authorities Forum and participated in a panel discussion titled "Governance of AI and Emerging Technologies in the Asia Pacific Region: Perspectives and Initiatives"



12月
Dec
2024

發表一宗政府部門資料外洩事故及八間機構透過一個求職平台刊登匿名招聘廣告的調查結果

Released investigation findings on the data breach incident of a government department and the Blind Ads posted by eight organisations on an online job-seeking platform

於《粵港澳大灣區(內地、香港)個人信息跨境流動標準合同》便利措施簡介會上發表演講

Spoke at the Briefing for Facilitation Measures on the "Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)"

1月
Jan
2025



發表一宗公營機構資料外洩事故的調查結果及發布新版《雲端運算指引》

Released investigation findings on the data breach incident of a public organisation and issued the new "Guidance on Cloud Computing"

發表2024年工作報告及一宗非牟利機構資料外洩事故的調查結果

Reported on the PCPD's work in 2024 and released investigation findings on the data breach incident of an NGO



2月
Feb
2025

出席應用科技高峰會，並在題為「確保生成式人工智能的可信度 — 挑戰與解決方案」的專題討論中擔任嘉賓講者

Attended the Tech Applied Summit and spoke as a panellist at a thematic session titled "Ensuring Trustworthiness in Generative AI – Challenges and Solutions"



私隱專員向立法會政制事務委員會報告2024年的工作

The Privacy Commissioner briefed the Legislative Council Panel on Constitutional Affairs on the work of the PCPD in 2024

3月
Mar
2025

舉辦「防騙有法」講座，吸引超過740名人士參加

Organised a seminar on "Protecting Personal Data to Prevent Fraud", attracting over 740 participants



與香港生產力促進局聯手推出「中小企數據安全培訓系列」，協助中小企加強保障數據安全，首場研討會吸引近400名人士參加

Jointly launched the "Data Security Training Series for SMEs" with the Hong Kong Productivity Council to assist SMEs in enhancing data security, attracting nearly 400 participants at the first seminar

發表《僱員使用生成式AI的指引清單》及一宗機構資料外洩事故的調查結果

Issued the "Checklist on Guidelines for the Use of Generative AI by Employees" and released investigation findings on the data breach incident of an organisation



企業管治

Corporate Governance

組織架構

香港個人資料私隱專員公署(私隱專員公署)是一個獨立機構，負責監察香港法例第486章《個人資料(私隱)條例》(《私隱條例》)的實施及符規情況。私隱專員公署致力透過監察及監管各界人士遵從《私隱條例》的規定，執行《私隱條例》及推廣保障和尊重個人資料私隱的文化，確保市民的個人資料私隱得到保障。

私隱專員公署於1996年8月成立，由個人資料私隱專員(私隱專員)領導轄下多個部門，包括投訴部、刑事調查部、合規及查詢部、法律部、環球事務及研究部、企業傳訊部及企業支援部。

Organisational Structure

The Office of the Privacy Commissioner for Personal Data (PCPD) is an independent body set up to oversee the implementation of and compliance with the Personal Data (Privacy) Ordinance (PDPO) (Chapter 486 of the Laws of Hong Kong). The PCPD strives to ensure the protection of the privacy of individuals in relation to personal data through monitoring and supervising compliance with the PDPO, enforcing its provisions, and promoting a culture of protecting and respecting personal data privacy.

Established in August 1996, the PCPD is headed by the Privacy Commissioner for Personal Data (Privacy Commissioner). It comprises several functional units, including the Complaints Division, Criminal Investigation Division, Compliance and Enquiries Division, Legal Division, Global Affairs and Research Division, Corporate Communications Division, and Corporate Support Division.



個人資料私隱專員

Privacy Commissioner for Personal Data

助理個人資料私隱專員(企業傳訊及營運)
Assistant Privacy Commissioner for Personal Data
(Corporate Communications and Operations)

助理個人資料私隱專員(投訴及刑事調查)
Assistant Privacy Commissioner for Personal Data
(Complaints and Criminal Investigation)

助理個人資料私隱專員(合規、環球事務及研究)
Assistant Privacy Commissioner for Personal Data
(Compliance, Global Affairs and Research)

署理助理個人資料私隱專員(法律)
Acting Assistant Privacy Commissioner for Personal Data
(Legal)

投訴 Complaints

刑事調查 Criminal Investigation

合規及查詢 Compliance and Enquiries

法律 Legal

環球事務及研究 Global Affairs and Research

企業傳訊 Corporate Communications

企業支援 Corporate Support

個人資料(私隱)諮詢委員會

個人資料(私隱)諮詢委員會(委員會)是根據《私隱條例》第11條成立，目的是就保障個人資料私隱及《私隱條例》運作的相關事宜，向私隱專員提供意見。

Personal Data (Privacy) Advisory Committee

The Personal Data (Privacy) Advisory Committee (PDPAC) was established pursuant to section 11 of the PDPO to advise the Privacy Commissioner on matters relating to personal data privacy protection and the operation of the PDPO.

主席 Chairperson



鍾麗玲 女士, SBS
Ms **Ada CHUNG Lai-ling**, SBS

個人資料私隱專員
Privacy Commissioner for Personal Data

成員 Members (按姓氏英文字母排序 in alphabetical order of last name)



陳嘉賢 女士, JP
Ms **Karen CHAN Ka-yin**, JP

德國寶集團有限公司
執行董事
Executive Director,
German Pool Group Company Limited



鄒錦沛 博士
Dr **CHOW Kam-pui**

香港大學計算機科學系副教授
Associate Professor,
Department of Computer Science,
The University of Hong Kong



簡慧敏 議員, JP
The Hon **Carmen KAN Wai-mun**, JP

中國銀行(香港)有限公司
總法律顧問
General Counsel,
Bank of China (Hong Kong) Limited



羅輝 先生
Mr **LAW Fai**

香港商業廣播有限公司
新聞及公共事務部總監
Director, News and Public Affairs, Hong Kong
Commercial Broadcasting Company Limited

委員會每年舉行定期會議，討論私隱專員公署的運作表現報告，並就公署的運作及政策事宜向私隱專員提供意見，包括推廣公眾對《私隱條例》的認識、理解及遵從的活動，以及可能影響個人資料私隱的現行及擬議的法例等。

委員會主席為私隱專員，而委員會成員則由政制及內地事務局局長委任，成員來自不同界別，各具豐富經驗和專業知識。

The PDPAC holds regular meetings each year to discuss reports on the operational performance of the PCPD and advise the Privacy Commissioner on operational and policy matters of the PCPD, including, among others, activities to promote awareness, understanding, and compliance with the PDPO, as well as existing and proposed legislation that may affect individuals' personal data privacy.

The Privacy Commissioner is the chairperson of the PDPAC, and members of the PDPAC are appointed by the Secretary for Constitutional and Mainland Affairs. The members come from diverse sectors, each bringing a wealth of experience and professional expertise.



連浩民先生, MH
Mr **Joseph**
LIN Ho-man, MH

HKE Holdings Limited
執行董事兼主席
Executive Director and Chairman,
HKE Holdings Limited



黃敏華女士
Ms **Nikki**
NG Mien-hua

信和集團
非執行董事
Non-Executive Director,
Sino Group



黃志光博士
Dr **Patrick**
WONG Chi-kwong

嶺南大學諮議會主席；
香港生產力促進局前副主席
Chairman, The Court of Lingnan University;
Former Deputy Chairman, Hong Kong
Productivity Council

政制及內地事務局副秘書長或
首席助理秘書長
Deputy Secretary for Constitutional
and Mainland Affairs or
Principal Assistant Secretary for
Constitutional and Mainland Affairs

科技發展常務委員會

私隱專員公署設立科技發展常務委員會，旨在協助私隱專員更有效地執行《私隱條例》第8(1)(f)條指明的法定職能，即對可能會影響個人資料私隱的資料處理進行研究及監察其發展。委員會就數據處理及資訊科技的發展對個人資料私隱的影響等議題向私隱專員提供意見。委員會成員由資訊及通訊技術行業的傑出人士，包括資訊安全、網絡安全和人工智能等領域的專家組成。

科技發展常務委員會由私隱專員及助理私隱專員擔任聯席主席，每年舉行定期會議。

Standing Committee on Technological Developments

The Standing Committee on Technological Developments (SCTD) was established to assist the Privacy Commissioner in better performing the statutory functions under section 8(1)(f) of the PDPO, namely researching into and monitoring technological developments that may affect personal data privacy. The SCTD advises the Privacy Commissioner on, among other things, the impact of the developments in the processing of data and information technology on the privacy of individuals in relation to personal data. It comprises distinguished individuals from the information and communications technology industry, including experts in the fields of information security, cybersecurity and AI.

The SCTD, co-chaired by the Privacy Commissioner and the Assistant Privacy Commissioner, holds regular meetings each year.

聯席主席 Co-Chairpersons



鍾麗玲女士, SBS
Ms Ada CHUNG Lai-ling, SBS

個人資料私隱專員
Privacy Commissioner for Personal Data

王雅媛女士
Ms Joanne WONG

助理個人資料私隱專員(合規、環球事務及研究)
Assistant Privacy Commissioner for Personal Data
(Compliance, Global Affairs and Research)



成員 Members (按姓氏英文字母排序 in alphabetical order of last name)



陳仲文工程師
Ir **Alex CHAN**

香港生產力促進局
網絡安全及數碼轉型部總經理
General Manager,
Digital Trust and Transformation Division,
Hong Kong Productivity Council



張偉倫博士
Dr **Alan CHEUNG**

香港應用科技研究院
人工智能及可信技術部門首席總監
Chief Director,
Artificial Intelligence and Trust Technologies,
Hong Kong Applied Science and Technology
Research Institute



劉偉經特邀教授
Adjunct Professor
Jason LAU

國際信息系統審計會 (ISACA)
全球董事會成員
Director,
ISACA International Board of Directors



李嘉樂博士
Dr **Gregg LI**

創星匯(香港)
創會主席兼總裁
Founding Director and President,
Orion Astropreneur Space Academy



黃錦輝議員, MH
Professor the Hon
**William WONG
Kam-fai, MH**

香港中文大學工程學院
副院長(外務)
Associate Dean (External Affairs),
Faculty of Engineering,
The Chinese University of Hong Kong



楊熾仁教授
Professor
Dit-yan YEUNG
(任期由2024年7月1日起)
(Appointment from 1 July 2024)

香港科技大學計算機科學及工程學系
講座教授
Chair Professor,
Department of Computer Science and Engineering,
Hong Kong University of Science and Technology



姚兆明教授
Professor **S M YIU**

香港大學計算機科學系
教授及副系主任
Professor and Deputy Head,
Department of Computer Science,
The University of Hong Kong

高級管理團隊

Senior Management Team

■ **鍾麗玲女士, SBS**
Ms Ada CHUNG Lai-ling, SBS

個人資料私隱專員
Privacy Commissioner for Personal Data



■ **王雅媛女士**
Ms Joanne WONG

助理個人資料私隱專員
(合規、環球事務及研究)
Assistant Privacy Commissioner
for Personal Data
(Compliance, Global Affairs
and Research)

■ **黎智敏女士**
Ms Joyce LAI

助理個人資料私隱專員
(企業傳訊及營運)
Assistant Privacy Commissioner
for Personal Data
(Corporate Communications
and Operations)

■ **何芹若女士**
Ms Rebecca HO

助理個人資料私隱專員
(投訴及刑事調查)
Assistant Privacy Commissioner
for Personal Data
(Complaints and Criminal
Investigation)

■ **賴皓茵女士**
Ms Fiona LAI

署理助理個人資料私隱專員
(法律)
Acting Assistant Privacy
Commissioner for Personal
Data (Legal)

郭正熙先生
Mr Brad KWOK

首席個人資料主任(合規及查詢)
Chief Personal Data Officer
(Compliance and Enquiries)

廖雅欣女士
Ms Joyce LIU

高級律師
(環球事務及研究)
Senior Legal Counsel
(Global Affairs and Research)

黃寶漫女士
Ms Clemence WONG

署理高級律師
Acting Senior Legal Counsel



胡慧雅女士
Ms Terri WU

署理首席個人資料主任(投訴)
Acting Chief Personal
Data Officer (Complaints)

庾燕青女士
Ms Gloria YU

首席個人資料主任(刑事調查)
Chief Personal Data Officer
(Criminal Investigation)

潘潔霖女士
Ms Natalie POON

高級個人資料主任(企業支援)
Senior Personal Data Officer
(Corporate Support)

高級人員

Senior Officers

盧浩榮先生
Mr John LO

高級個人資料主任
(合規及查詢)
Senior Personal Data Officer
(Compliance and Enquiries)

陳鐵威先生
Mr William CHAN

高級個人資料主任
(資訊科技)
Senior Personal Data Officer
(Information Technology)



文靄怡女士
Ms Ayee MAN

高級個人資料主任
(合規及查詢)
Senior Personal Data Officer
(Compliance and Enquiries)

鄭楚英女士
Ms Kimmy CHENG

高級個人資料主任
(合規及查詢)
Senior Personal Data Officer
(Compliance and Enquiries)

周映彤女士
Ms Phoebe CHOW

企業傳訊總監
Head of Corporate
Communications

譚嘉榮先生
Mr Tamson TAM

署理高級個人資料主任
(資訊科技)
Acting Senior Personal Data
Officer (Information Technology)

■ **陳世皓先生**
Mr Kevin CHAN

律師
Legal Counsel

■ **盧迪凡先生**
Mr DF LO

高級個人資料主任
(刑事調查)
Senior Personal Data Officer
(Criminal Investigation)

■ **黎淑芬女士**
Ms Addy LAI

高級個人資料主任(投訴)
Senior Personal Data Officer
(Complaints)



■ **馮學晴女士**
Ms Dorothy FUNG

署理律師
Acting Legal Counsel

■ **周沅瑩女士**
Ms Stephanie CHAU

律師
Legal Counsel

■ **李凱寧女士**
Ms Joyce LI

高級個人資料主任(投訴)
Senior Personal Data Officer
(Complaints)

高級管理團隊

私隱專員公署設立了高級管理團隊，負責訂立公署的策略方向和工作計劃、制定政策及管理公署的運作，以維持高水平的企業管治及有效執行《私隱條例》，確保市民的個人資料私隱獲得保障。高級管理團隊由私隱專員領導，成員包括首長級人員及部門主管。為確保有效管理，高級管理團隊每月舉行會議，匯報、討論及檢討公署各個部門的工作進度及成效。

企業策略計劃

維持高水平的企業管治對私隱專員公署的可持續發展和保障市民的個人資料私隱權利極為重要。根據公署的願景、使命及價值，公署制定了企業策略計劃，作為履行其法定職責的原則及目標，同時維持高水平的企業管治(圖1.1)。

Senior Management Team

The PCPD has set up a Senior Management Team (Team) tasked with envisioning strategic directions and work plans, formulating policies and managing operations of the PCPD, with a view to maintaining high standards of corporate governance and effectively enforcing the PDPO to ensure the protection of the personal data privacy of individuals. The Team is headed by the Privacy Commissioner and constitutes directorate officers and division heads of the PCPD. To ensure effective management, the Team meets monthly to report, discuss and review the work progress and performance of each division of the PCPD.

Corporate Strategic Plan

Maintaining high standards of corporate governance is of fundamental importance to the sustainability of the PCPD and the protection of personal data privacy rights of members of the public. In keeping with its vision, mission and values, the PCPD formulated the Corporate Strategic Plan as the principles and goals in performing its statutory duties while maintaining high standards of corporate governance (Figure 1.1).





圖 Figure 1.1

企業社會責任

私隱專員公署自2022年起成立「關愛義工隊」，透過舉辦不同義工活動向社會展示關懷，例如在新冠疫情期間向社福機構捐贈抗疫物資、在節日為長者舉辦防騙講座暨送暖行動，以及為有需要人士製作膳食餐盒等，為社會作出貢獻。

此外，私隱專員公署視員工為重要的資產。除了為員工提供各方面的培訓和發展機會，令員工持續增值外，公署亦舉辦不同的員工活動讓他們舒展身心，並定期舉行員工會議，以關懷及了解員工的需要。

Corporate Social Responsibility

The PCPD Volunteer Team, set up in 2022, shows care to the community through organising different volunteering activities. For example, the Volunteer Team donated medical supplies to social welfare organisations during the COVID-19 pandemic, arranged talks on fraud prevention while visiting the elderly during festivals to send joy and good wishes, and prepared meal boxes for the needy, etc., so as to contribute to the betterment of the community.

In addition, the PCPD values its employees as an important asset. With this in mind, the PCPD organises a wide range of staff activities to support its employees' physical and mental well-being, in addition to providing various training and development opportunities to equip them for continuous growth. Regular staff meetings are also held to care for and understand the needs of employees.





構建數碼私隱 新時代

Building a New Digital
Privacy Era



提升人工智能安全

隨着人工智能(AI)的使用與日俱增，不同規模的企業均開始研究在營運中應用這項技術。為協助機構在採用AI的同時亦保障個人資料私隱，私隱專員公署積極在本港推出一系列措施，並與世界各地的私隱或資料保障機構合作，在瞬息萬變的數碼時代中推廣AI安全的重要性。

Enhancing Artificial Intelligence Security

With the rapidly increasing use of artificial intelligence (AI), businesses of all sizes are set to explore the potential of adopting the technology in their operations. To assist organisations in adopting AI while safeguarding the personal data privacy of individuals, the PCPD has acted proactively to launch an array of initiatives in Hong Kong and collaborate with privacy or data protection authorities from around the globe to promote the importance of AI security amidst the ever-evolving digital era.

發布《人工智能(AI)：個人資料保障模範框架》

2024年6月，私隱專員公署發布了《人工智能(AI)：個人資料保障模範框架》(《模範框架》)，提供國際認可及切實可行的建議和最佳行事常規，以協助機構在採購、實施及使用AI，包括生成式AI時，遵從《私隱條例》的相關規定，確保機構在善用AI之餘，亦保障個人資料私隱。

Issuing “Artificial Intelligence: Model Personal Data Protection Framework”

In June 2024, the PCPD issued the “Artificial Intelligence: Model Personal Data Protection Framework” (Model Framework) to provide internationally recognised and practical recommendations and best practices, with a view to assisting organisations in procuring, implementing and using AI, including generative AI, in compliance with the relevant requirements of the PDPO, thereby harnessing the benefits of AI while safeguarding personal data privacy.

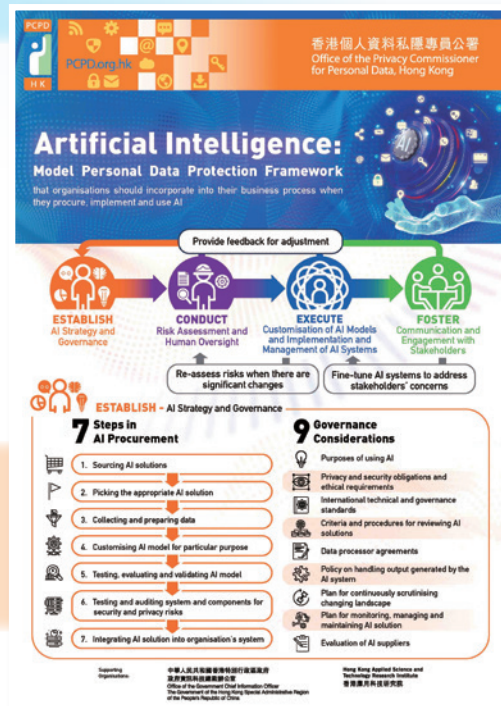
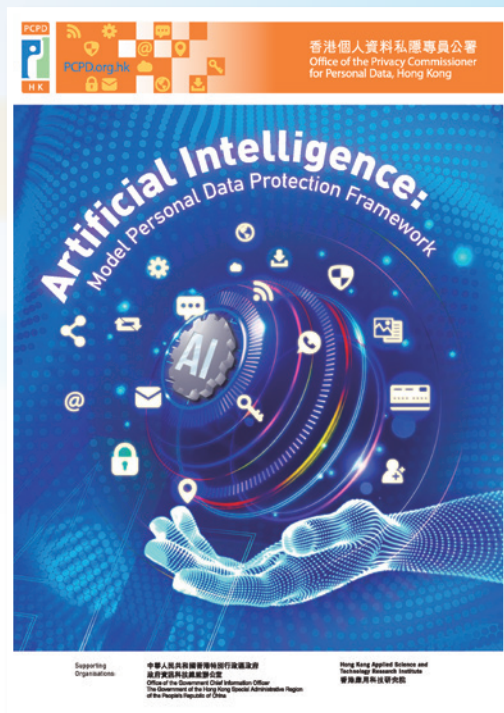


《模範框架》建基於一般業務流程，就「AI策略及管治架構」、「風險評估及人為監督」、「實行AI模型的定製與AI系統的實施及管理」，以及「促進與持份者的溝通及交流」等範疇，提供建議及最佳行事常規。

此外，為協助機構了解《模範框架》，私隱專員公署出版了一份介紹《模範框架》的懶人包，摘錄當中的重點建議。

The Model Framework, premised on general business procedures, covers recommendations and best practices in the areas of “AI strategy and governance”, “risk assessment and human oversight”, “customisation of AI models and implementation and management of AI systems”, and “communication and engagement with stakeholders”.

Furthermore, to assist organisations in understanding the Model Framework, the PCPD has published a leaflet which provides an extract of the key recommendations in the Model Framework.

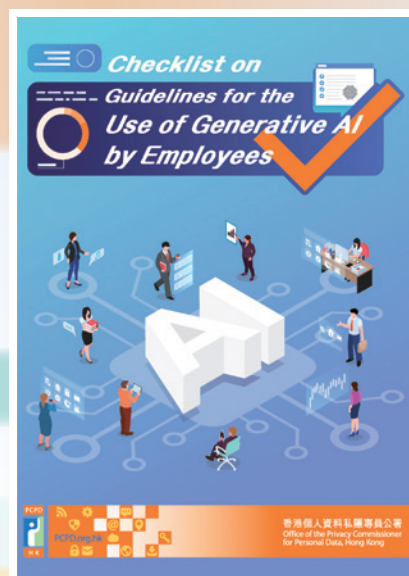


發布《僱員使用生成式AI的指引清單》

2025年3月，私隱專員公署發布了《僱員使用生成式AI的指引清單》（《指引》），協助機構制定僱員在工作時使用生成式AI的內部政策或指引，以及遵從《私隱條例》的相關規定。

Issuing “Checklist on Guidelines for the Use of Generative AI by Employees”

In March 2025, the PCPD issued the “Checklist on Guidelines for the Use of Generative AI by Employees” (Guidelines) to assist organisations in developing internal policies or guidelines on the use of generative AI by employees at work while complying with the requirements of the PDPO.



《指引》建議機構在制定其僱員使用生成式AI的內部政策或指引時涵蓋以下內容：「獲准使用生成式AI的範圍」、「保障個人資料私隱」、「合法及合乎道德的使用及預防偏見」、「數據安全」，以及「違反政策或指引可引致的後果」。

《指引》同時就支援僱員使用生成式AI工具提供了實用貼士，包括提高政策或指引的透明度、提供僱員使用生成式AI工具的培訓及資源、委派支援隊伍，以及建立反饋機制。

The Guidelines recommend that organisations cover the following aspects when developing their internal policies or guidelines on the use of generative AI by employees: “scope of permissible use of generative AI”, “protection of personal data privacy”, “lawful and ethical use and prevention of bias”, “data security”, and “possible consequences of violations of the policies or guidelines”.

The Guidelines also provide practical tips on supporting employees in using generative AI tools, which include enhancing transparency of the policies or guidelines, providing training and resources for employees’ use of generative AI tools, setting up a support team and establishing a feedback mechanism.

此外，為協助機構在採用AI時確保個人資料私隱得到充分保障，私隱專員公署推出了「AI安全」熱線(2110 1155)，以便機構查詢。

In addition, to assist organisations in adopting AI while ensuring the protection of personal data privacy of individuals, the PCPD has launched the “AI Security” Hotline (2110 1155) for organisations to make enquiries.

積極深入社區向各界宣傳推廣

報告年度內，私隱專員公署積極推廣《模範框架》及《指引》，以提高公眾對AI安全的意識。公署分別於2024年7月及9月舉辦兩場關於AI與個人資料私隱保障的專題研討會，講解機構在採購、實施及使用AI系統時處理個人資料的最佳行事常規，反應熱烈，合共吸引逾1,300人參加。此外，公署代表亦於不同的會議和研討會上發表演講，推廣AI安全。

Proactive Publicity and Promotion Efforts for Community Outreach

During the reporting year, the PCPD made concerted efforts in promoting the Model Framework and the Guidelines as a means of raising public awareness of AI security. The PCPD organised two topical seminars on AI and personal data privacy protection in July and September 2024 respectively, to elucidate the best practices for organisations to procure, implement and use AI systems that involve the handling of personal data. The seminars were well-received, attracting over 1,300 participants. In addition, representatives of the PCPD also spoke at an array of conferences and workshops to promote AI security.



年輕人使用AI已蔚然成風，私隱專員公署主動走入校園，向中學生推廣AI安全。公署於2024年4月舉辦「AI新世代保障私隱領袖培訓計劃」，透過專題講座、與保障資料主任交流及在Microsoft微軟香港總部舉辦的AI實踐工作坊等多項活動，向參與活動的學生解釋個人資料私隱管理系統的重要性，以及符合道德的AI應用標準。

In the light of the widespread use of AI among youngsters, the PCPD took the initiative to reach out to secondary school students to promote AI security. The PCPD launched the “Future Leaders of AI and Privacy Protection Training Programme” in April 2024 to explain the importance of personal data privacy management programmes and the standards of ethical use of AI to the participating students through various activities, including a topical seminar, exchanges with data protection officers, and an AI interactive workshop organised at Microsoft Hong Kong’s headquarters.



除了舉辦研討會，私隱專員亦在不同報章及專業期刊發表文章，包括香港律師會會刊《香港律師》及香港會計師公會的官方季度雜誌《A Plus》等，藉此向社會各界人士推廣AI安全在數碼時代的重要性。

In addition to hosting seminars, the Privacy Commissioner published articles in various newspapers and professional journals, such as “Hong Kong Lawyer”, the journal of The Law Society of Hong Kong, and “A Plus”, the official quarterly magazine of The Hong Kong Institute of Certified Public Accountants, to promote the significance of AI security in the digital age to all sectors of the society.

THOUGHT LEADERSHIP
Ada Chung
The Privacy Commissioner for Personal Data and member of the Institute on Key Recommendations covered by PCPD's model framework for ensuring AI security



APUS

Safeguarding personal data privacy in the AI era with PCPD's Model Framework

Recently, especially since the advent of ChatGPT, artificial intelligence (AI) has become ubiquitous. It is no longer just a buzzword within the tech industry, as we see its application across various regions and industries, including the accounting profession. According to a Thomson Reuters' survey early this year, 73 percent of the surveyed tax and accounting firms believed that generative AI could be applied to their work. Accounting professionals have started integrating AI to automate daily operations such as summarizing and analyzing data and identifying irregular transactions, thereby reducing costs and optimizing efficiency. The trend of integrating AI into organizations' workflow seems to be unstoppable.

AI – Friend or foe?
However “magical” AI may appear to be, the bitter truth is that it is a double-edged sword. Organizations must remain vigilant to the risks posed by this technology, particularly privacy risks, to prevent AI from becoming our foe.

Privacy considerations are crucial because data is the lifeblood of AI. Massive amounts of data are typically involved throughout the life cycle of AI, from development, customization and implementation to termination. For example, when accounting firms customize AI models purchased from AI developers or vendors using sensitive data, such as clients' financial information and personal data, any leakage could be catastrophic. If such data falls into the wrong hands, any subsequent fraud or identity theft will severely tarnish the firms' reputations and undermine the confidence of their customers. Therefore, having robust data security measures in place and ensuring compliance with the Personal Data (Privacy) Ordinance (PDPO) is vital.

Navigating the regulatory regime in Hong Kong
In Hong Kong, the PDPO, which is a principle-based and technology-neutral piece of legislation, applies to the collection, holding, processing and use of personal data, whether through the use of AI or not.

To help organizations establish AI governance and comply with the requirements of the PDPO, as early as 2021, my office, the Office of the Privacy Commissioner for Personal Data (PCPD) published the *Guidance on the Ethical Development and Use of Artificial Intelligence*. Organizations are recommended to adopt the internationally well-recognized data stewardship values (i.e. being respectful, beneficial, and fair to stakeholders) and ethical principles for AI (i.e. accountability; human oversight; transparency and interpretability; data privacy; fairness; beneficial AI; and reliability, robustness and security) when developing and using AI.

More recently in June this year, to support the “Global AI Governance Initiative” promulgated by the Mainland and

to help ensure AI security, the PCPD published the *Artificial Intelligence: Model Personal Data Protection Framework (Model Framework)*. Targeting organizations that procure, implement and use any type of AI systems, including generative AI, and premised on general business processes, the Model Framework covers recommendations and best practices in the areas below:

AI strategy and governance
Active participation by top management is a crucial driving force for the successful implementation of AI strategy and governance. Organizations should first formulate an AI governance strategy that includes a roadmap setting out the directions and purposes for which AI systems may be adopted.

Beyond strategic alignment, when procuring AI systems from third parties, organizations are recommended to consider various governance issues in their supplier management processes, such as key privacy and security obligations or ethical requirements to be conveyed to potential AI suppliers.

Risk assessment and human oversight
Underpinning the Model Framework is a risk-based approach. It is recommended that organizations conduct risk assessments to systematically identify, analyze and evaluate the risks, including privacy risks, involved in the AI life cycle so that corresponding risk mitigation measures, including an appropriate level of human oversight, can be deployed. In one cases that may incur higher risks, organizations should adopt a “human-in-the-loop” approach wherein human actors retain control of the decision-making process.

Customization of AI models and implementation and management of AI systems
When customizing and implementing AI solutions, organizations should minimize the amount of personal data involved. Additionally, organizations should ensure that AI models have undergone rigorous testing and validation before use.

The Model Framework also recommends that organizations establish an AI incident response plan to monitor and address incidents that may inadvertently occur.

Communication and engagement with stakeholders
Regular communication with stakeholders is key to building trust. Organizations should encourage feedback from all parties and strive to make their AI-generated output as transparent as possible.

Be the trusted advisors
Accountants have long been the trusted advisors to individuals and organizations. As technology evolves rapidly, it is more important than ever that accountants keep abreast of the latest trends and measures in AI security in order to maintain the trust placed in them.

October 2024 27



Artificial Intelligence: The Model Personal Data Protection Framework

By Ada Chung Lai Ling, Privacy Commissioner for Personal Data

Since my Office published the *Guidance on the Ethical Development and Use of Artificial Intelligence* (the “2021 AI Guidance”) in 2021, artificial intelligence (AI) has remained in the spotlight. We are now in an era in which the use of ChatGPT has experienced exponential growth and organisations worldwide are racing to leverage the technology, if they have not already experienced it first-

hand. According to a survey published by the Hong Kong Federation Council in October 2023, around 50% of local enterprises are expected to use AI by the end of 2024.

Despite the opportunities that AI offers, we should heed the cautionary words of Stephen Hawking, who once said that “success in creating AI could be the biggest event in the history of our civilisation. But

it could also be the last, unless we learn how to avoid the risk”. Among the risks posed by AI, privacy stands out as one of the most significant. Governments around the world have taken note of this concern and have recognised the need for targeted regulations on AI and robust frameworks that balance innovation with the protection of personal data privacy, among others.

www.hk lawyer.org 35

持份者的參與及國際聯繫

為更清楚了解本地企業如何看待並應對AI帶來的風險，私隱專員公署委託香港生產力促進局進行有關網絡保安準備的調查，並於2024年11月發表「香港企業網絡保安準備指數及AI安全風險」調查報告。

Stakeholder Engagement and International Connections

To better understand how local enterprises perceive and respond to the risks posed by AI, the PCPD commissioned the Hong Kong Productivity Council to conduct a survey on cyber security readiness and released the “Hong Kong Enterprise Cyber Security Readiness Index and AI Security” survey report in November 2024.



在國際層面，私隱專員公署積極與世界各地的私隱或資料保障機構合作，應對新興趨勢及科技急速發展所帶來的挑戰。

在報告年度內，為了推動更緊密AI安全的國際合作，私隱專員公署自2024年10月起擔任環球私隱議會人工智能的道德與數據保障工作分組(AI工作分組)的聯席主席。其他聯席主席為歐洲聯盟、法國及韓國的私隱或資料保障機構。AI工作分組現時有超過40個環球私隱議會成員參與，包括來自澳洲、德國、日本、新西蘭、英國及美國的私隱或資料保障機構。

除了擔任AI工作分組的聯席主席，私隱專員公署亦繼續擔任環球私隱議會國際執法合作工作分組的聯席主席。鑑於網上平台遭大規模擷取個人資料所帶來的私隱問題備受關注，公署作為國際執法合作工作分組聯席主席，於2023年8月與全球11個私隱或資料保障機構共同向社交媒體平台和其他載有公開個人資料的網站發表環球保障私隱期望的聯合聲明(首份聯合聲明)。

繼發表首份聯合聲明後，擷取數據以訓練AI系統的問題引起環球監管機構關注。私隱專員公署聯同全球15個私隱或資料保障機構於2024年10月發表題為「有關數據擷取及保障私隱的聯合聲明」的環球聯合聲明，重申首份聯合聲明所列明的要求，並透過與社交媒體平台及業界持份者交流分享最佳行事常規和經驗，為業界提供進一步指引。

On the international front, the PCPD strived to collaborate with privacy or data protection authorities across the globe to tackle challenges arising from emerging trends and rapid technological advancements.

During the reporting year, with an aim to fostering closer international collaborations on AI security, the PCPD has taken up the position of co-chair in the Ethics and Data Protection in Artificial Intelligence Working Group (AIWG) of the Global Privacy Assembly (GPA) since October 2024. Other incumbent co-chairs are privacy or data protection authorities in the European Union, France and Korea. The AIWG currently consists of more than 40 GPA members, including privacy or data protection authorities in Australia, Germany, Japan, New Zealand, the United Kingdom and the United States of America.

Besides its tenure as co-chair of the AIWG, the PCPD continues to serve as co-chair of the International Enforcement Cooperation Working Group (IEWG) of the GPA. In response to the privacy concerns posed by mass data scraping from online platforms, the PCPD, in its capacity as co-chair of the IEWG, took concerted action with 11 privacy or data protection authorities worldwide to issue a joint statement in August 2023 (Initial Statement), about global expectations on privacy protection to social media platforms and other websites that host publicly accessible personal data.

Subsequent to the issuance of the Initial Statement, concerns about data scraping for AI training have grown among global regulators. The PCPD and 15 privacy or data protection authorities worldwide issued a global joint statement in October 2024 titled "Concluding Joint Statement on Data Scraping and the Protection of Privacy" to reinforce the requirements set out in the Initial Statement, and to share best practices and experiences through engagements with social media platforms and industry stakeholders, thereby providing the industry with further guidance.

加強數據安全

針對近年個人資料外洩事故有上升趨勢，私隱專員公署從多方面提升公眾和機構對數據安全的認識，並加強協助機構應對數據安全的工作。

關注私隱週

私隱專員公署繼續參與由亞太區保障私隱機構成員共同支持的年度保障私隱盛事「關注私隱週」，在2024年5月以「數據安全保私隱」為主題，展開一連串推廣及教育活動，藉此加強機構及市民對保障數據安全的意識。當中的活動包括安排流動展覽車「保障私隱號」走入社區播放教育短片及派發教育刊物，並透過互動遊戲，讓參觀人士加深認識保障個人資料私隱及數據安全的重要性；舉辦數據安全研討會，分享近年資料外洩個案及相關的數據安全措施；以及推出數據安全吉祥物「數據保寶」，在各大運輸網絡、社交媒體、網上平台、報章等渠道宣傳數據安全的訊息。

Fostering Data Security

In response to the rising trend in personal data breach incidents in recent years, the PCPD stepped up its efforts in different aspects to assist organisations in addressing data security issues.

Privacy Awareness Week

The PCPD continued to engage in the annual privacy protection event, "Privacy Awareness Week", jointly supported by members of the Asia Pacific Privacy Authorities. A series of promotional and educational activities was launched in May 2024 under the theme "Safeguard Data Security • Safeguard Privacy" to raise awareness of data security among organisations and members of the public. These activities included launching the "Privacy Protection Truck", a mobile exhibition truck, which reached out to the community to enhance understanding of the importance of protecting personal data privacy and data security through educational videos, collaterals, and interactive games. Data security seminars were also organised to share recent data breach cases and relevant data security measures. The data security mascot, "Data Guardian", was introduced and tasked with promoting data security through different channels, including major public transportation networks, social media, online platforms, newspapers, and more.





「數據安全」套餐

為協助機構防止資料外洩事故，私隱專員公署除了繼續設有「數據安全三大法寶」(即供企業自我評估的「數據安全快測」、「數據安全」專題網頁及「數據安全」熱線)外，亦特別為學校、非牟利機構及中小企推出「數據安全」套餐，提供培訓名額予完成「數據安全快測」的機構免費參加公署的研習班及專題講座，共吸引近200間機構參加。

“Data Security” Package

In addition to the “Data Security Trio” (i.e. the “Data Security Scanner” self-assessment toolkit, the “Data Security” thematic webpage and the “Data Security” Hotline), the PCPD also introduced the “Data Security” Package for schools, non-profit-making organisations (NGOs) and small and medium-sized enterprises (SMEs) to assist organisations in preventing data breaches. The “Data Security” Package offers participating organisations free training quotas for the PCPD’s professional workshops and topical seminars upon completion of an assessment by the “Data Security Scanner”, drawing nearly 200 organisations.

加強培訓及與業界合作

在報告年度內，私隱專員公署舉辦超過190場機構內部培訓講座，並為公眾、教育機構、非牟利機構及中小型企業等舉辦數據安全及處理資料外洩事故研討會，致力推動數據安全管理。此外，公署亦與多個機構合辦相關教育及推廣活動，例如與香港金融管理局及香港銀行公會合辦研討會，推動銀行業的數據安全；參與由香港警務處網絡安全及科技罪案調查科及Cyberbay合辦的狩網運動2024，擔任活動的策略夥伴並為參加機構提供個人資料管理的培訓；以及成為香港互聯網註冊管理有限公司與國際信息系統審計協會中國香港分會合辦的共建員工防火牆嘉許計劃的計劃夥伴等。

Strengthening Training and Cooperation with Industries

During the reporting year, the PCPD conducted over 190 in-house training seminars for various organisations, and organised topical seminars on data security and the handling of data breach incidents for the public, educational institutions, NGOs and SMEs, with a view to promoting data security management. Additionally, the PCPD collaborated with various organisations on data security-related educational and promotional activities, such as co-organising a seminar with the Hong Kong Monetary Authority and the Hong Kong Association of Banks to promote data security in the banking sector; acting as the strategic partner in the BugHunting Campaign 2024 jointly organised by the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force and Cyberbay, and providing training on personal data management for the participating organisations; as well as participating as the scheme partner in the Cyber Security Staff Awareness Recognition Scheme co-organised by the Hong Kong Internet Registration Corporation Limited (HKIRC) and ISACA China Hong Kong Chapter.





私隱專員公署亦與香港互聯網註冊管理有限公司合作推出一系列數據安全教育短片，以輕鬆的手法為機構提供相關指引及貼士，並在中英文報章、網媒及專業期刊撰文，進一步推廣相關訊息，以提升機構和公眾對數據安全的認識。

The PCPD also joined HKIRC in launching a series of educational videos on data security to provide relevant guidance and tips to organisations in a lively manner, and published articles in Chinese and English newspapers, online media and professional journals to further enhance the awareness of data security among organisations and the public.

打擊「起底」

《2021 年個人資料(私隱)(修訂)條例》(《修訂條例》)下打擊「起底」行為的條文於2021年10月8日生效，將「起底」行為刑事化，並賦權私隱專員就有關罪行進行刑事調查及檢控。私隱專員亦可就「起底」訊息發出停止披露通知，以停止「起底」訊息的披露。

於報告年度內，私隱專員公署主動經網上巡查發現的「起底」個案為65宗，較2022-23年度(即「起底」條文生效後首一年的同期)的841宗大跌92%；而公署在報告年度內接獲305宗與「起底」相關的投訴，亦較2022-23年度的676宗下跌55%。

全方位處理「起底」個案

自《修訂條例》生效後，私隱專員公署全方位處理「起底」案件，從刑事調查到搜集證據，以至提出檢控，均由公署直接執行，從而更有效加快針對「起底」案件的執法和檢控行動。

在接獲「起底」投訴後，私隱專員公署會因應案情，根據《修訂條例》就涉嫌觸犯「起底」罪行的個案展開刑事調查，指派刑事調查人員跟進相關調查工作、搜集證據並進行分析，以決定是否就個案展開拘捕行動。

Combatting Doxxing

The provisions criminalising doxxing acts under the Personal Data (Privacy) (Amendment) Ordinance (Amendment Ordinance) came into effect on 8 October 2021. The amendments empower the Privacy Commissioner to carry out criminal investigations and institute prosecutions for doxxing-related offences. The Privacy Commissioner is also empowered to issue cessation notices to request the cessation of disclosure of doxxing messages.

During the reporting year, the number of doxxing cases uncovered by the PCPD's proactive online patrols was 65, representing a significant drop of 92% compared with 841 cases in the 2022-23 reporting year (i.e. the same period in the first year after the commencement of the anti-doxxing provisions). 305 doxxing-related complaints were received by the PCPD during the reporting year, which represented a drop of 55% compared with 676 complaints received during the 2022-23 reporting year.

Handling Doxxing Cases with a Holistic Approach

Since the provisions criminalising doxxing acts under the Amendment Ordinance came into effect, the PCPD has been handling doxxing cases with a holistic approach, from conducting criminal investigations and collecting evidence to commencing prosecutions directly, which effectively expedites enforcement and prosecution actions against doxxing cases.

After receiving a doxxing complaint, depending on the facts of the case, the PCPD may commence criminal investigation into the alleged doxxing-related offences pursuant to the Amendment Ordinance by assigning criminal investigators to follow up on the relevant investigation, collect evidence, and conduct analysis, so as to determine whether to mount an arrest operation.

「起底」個案概述

在報告年度內，私隱專員公署合共處理370宗「起底」個案(其中65宗為經公署主動網上巡查發現的個案、305宗是接獲與「起底」相關的投訴)。公署於同期就88宗個案展開刑事調查，共拘捕了21人。

此外，私隱專員公署轉介了42宗涉及《私隱條例》第64(3C)條下的罪行，及／或涉及其他不屬於《私隱條例》範圍內的罪行，以供警方作進一步調查及考慮作出檢控。

Overview of Doxxing Cases

During the reporting year, the PCPD handled a total of 370 doxxing cases (including 65 doxxing cases uncovered by the PCPD's proactive online patrols and 305 doxxing-related complaints received), commenced 88 criminal investigations and arrested 21 persons.

Furthermore, the PCPD referred 42 doxxing cases involving an offence under section 64(3C) of the PDPO and/or other offences outside the purview of the PDPO to the Police for further investigation and consideration of prosecution.

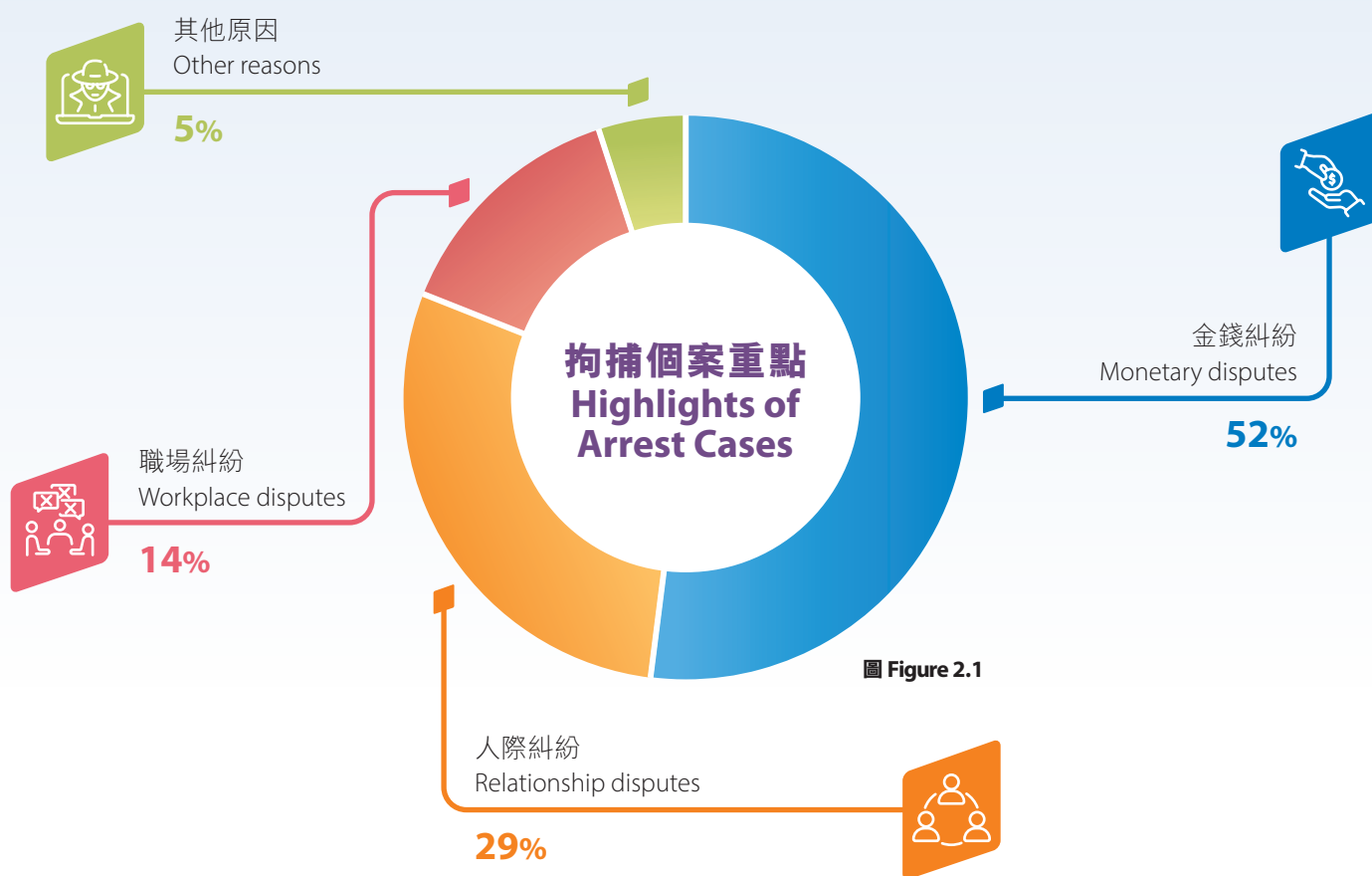


拘捕個案重點

在私隱專員公署拘捕的21人中，將事主「起底」的主要原因包括金錢糾紛(52%)、人際糾紛(29%)及職場糾紛(14%)(圖2.1)。

Highlights of Arrest Cases

Among the 21 persons arrested by the PCPD, the main motives for doxxing were as follows: monetary disputes (52%), relationship disputes (29%) and workplace disputes (14%) (Figure 2.1).



與金錢糾紛有關的案件主要涉及合約爭議，涉及人際糾紛的案件主要關於感情瓜葛及鄰里之間的爭端，而與職場糾紛有關的案件則主要源於同事之間的爭端。

Cases relating to monetary disputes stemmed primarily from contractual disputes, while cases originating from relationship disputes involved mainly emotional entanglements and conflicts between neighbours, and cases relating to workplace disputes generally arose from conflicts between colleagues at work.

至於「起底」的方式，被捕人士中有12人(57%)透過互聯網作出「起底」(包括九人透過社交媒體平台、一人透過即時通訊軟件、一人透過機構網站，以及一人透過以事主的名義申請網上服務)，其餘九人(43%)則涉及透過實物媒介作出「起底」(包括五人張貼單張、二人展示橫額、一人以筆塗鴉，以及一人身穿印有「起底」訊息的衣物)。

As regards the means of doxxing, 12 (57%) of the arrested persons conducted doxxing activities through the Internet (nine through social media platforms, one via instant messaging application, one through the website of an organisation and one through applying for online services in the name of the victim). The remaining nine (43%) arrested persons conducted doxxing activities through physical media (five through posting leaflets, two through displaying banners, one through graffiti and one through wearing clothing with doxxing contents).

移除「起底」訊息

除了通過刑事調查和檢控行動將「起底」者繩之於法外，及時移除「起底」訊息同樣重要，以避免對事主造成進一步傷害。就此，《修訂條例》賦予私隱專員法定權力，可發出停止披露通知，要求移除「起底」訊息。

Removal of Doxxing Messages

Apart from bringing the doxxers to justice through criminal investigations and prosecutions, the timely removal of doxxing messages is of equal importance to preventing further harm to victims. In this regard, the Amendment Ordinance confers statutory powers on the Privacy Commissioner to issue cessation notices to demand for the removal of doxxing messages.

在報告年度內，私隱專員公署向23個網上平台發出了161份停止披露通知，要求他們移除3544則「起底」訊息，亦成功透過發出停止披露通知移除了41個用作「起底」的頻道。儘管停止披露通知的送達對象大部分為海外的網上平台營運商，整體而言應公署要求移除「起底」訊息的遵從率達98.3%。

During the reporting year, the PCPD issued 161 cessation notices to 23 online platforms, requesting the removal of 3,544 doxxing messages. 41 channels used for doxxing were also successfully removed through the issuance of cessation notices. Although most of the cessation notices were served on overseas online platform operators, the overall compliance rate for removing doxxing messages reached 98.3%.

「起底」案件的檢控及判刑

在報告年度內，共有 14 人被裁定「起底」罪名成立，當中一人就兩宗不同的「起底」事件被分別作出檢控，其後被法院合併定罪。刑罰包括監禁、社會服務令、感化令及守行為。監禁刑期介乎 30 日（即時監禁）至三個月（緩刑 24 個月），而判處的社會服務令則介乎 80 至 180 小時。

值得注意的四宗被判監禁個案如下：

Prosecution and Sentencing of Doxxing Cases

During the reporting year, there were a total of 14 persons convicted for doxxing, including one person who was charged for two separate doxxing incidents which were subsequently convicted by the court on joinder. The penalties varied and included imprisonment, community service orders, probation order and bind over order. The imprisonment sentences ranged from 30 days (immediate imprisonment) to three months (suspended for 24 months). The community service orders imposed ranged from 80 to 180 hours.

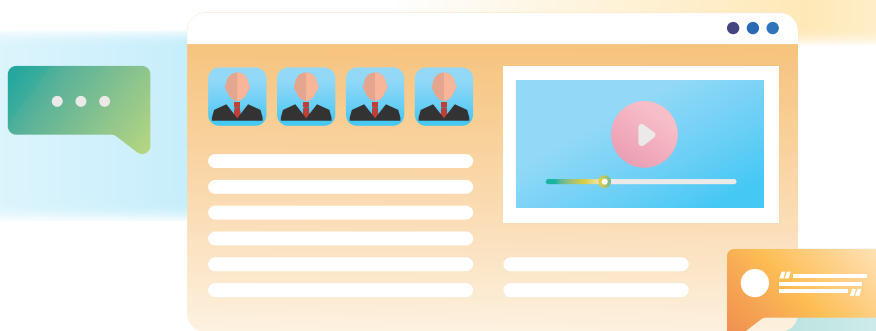
Below are four noteworthy cases involving custodial sentences:

男子將四名人士（包括立法會議員及執法人員）「起底」

被告於 2022 年 3 月至 2023 年 7 月期間，在不同的網上平台披露合共四名人士（包括兩名立法會議員及一名執法人員）的個人資料。於 2024 年 6 月，被告認罪下被法庭裁定他四項「未獲資料當事人同意下披露其個人資料」的罪名成立。法院判處被告監禁三個月，緩刑兩年。

Male Doxxed Four Victims (including Members of the Legislative Council and a Law Enforcement Officer)

Between March 2022 and July 2023, the defendant posted the personal data of a total of four victims (including two members of the Legislative Council and a law enforcement officer) on different social media platforms. The defendant was convicted of four charges of “disclosing personal data without consent” in June 2024 upon a guilty plea. The Court sentenced the defendant to three months’ imprisonment, suspended for two years.



男子「起底」前友人

被告與事主於2022年3月認識，兩人其後關係轉差，事主封鎖了被告的即時通訊軟件帳戶，與被告斷絕聯絡。於2022年7月，被告在一個網上討論區發布了多條包含事主個人資料的訊息，並對事主作出負面的評論。於2024年8月，被告在認罪下被裁定一項「未獲資料當事人同意下披露其個人資料而該披露造成指明傷害」的罪名成立。法院判處被告監禁四星期，緩刑兩年。

Male Doxxed a Former Friend

The defendant got acquainted with the victim in March 2022 but their relationship subsequently turned sour. The victim then blocked the defendant's instant messaging application account and ceased contact with the defendant. In July 2022, the defendant posted a number of messages containing the personal data of the victim on an online forum, alongside some negative comments against the victim. The defendant was convicted of one charge of "disclosing personal data without data subject's consent causing specified harm" in August 2024 upon entering a guilty plea. The Court sentenced the defendant to four weeks' imprisonment, suspended for two years.

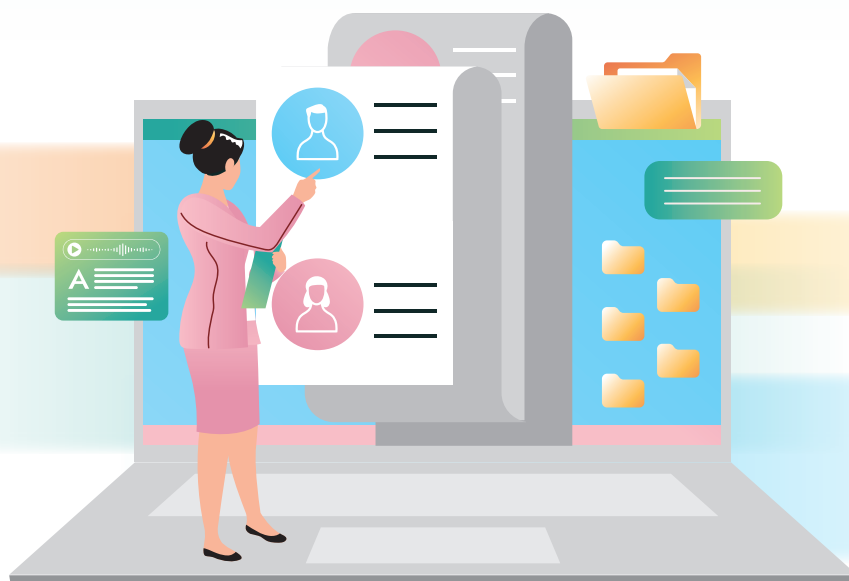


女子將一對母子「起底」

男事主當時為小學生，而女事主是他的母親。被告居於兩名事主附近，並與二人相識。女事主及後與被告關係轉差，女事主指稱被告不時責罵她和男事主。2022年11月至2023年5月期間，被告在一個社交媒體平台的兩個公開群組及兩個個人帳戶內先後發布了20條包含兩名事主的個人資料訊息，並對二人作出負面的評論。於2024年9月，被告認罪下被裁定四項「未獲資料當事人同意下披露其個人資料而該披露造成指明傷害」的罪名成立。法院判處被告即時監禁30日。

Female Doxxed a Mother and Her Child

The male victim was a primary school student at the material time, and the female victim is his mother. The defendant lived in close proximity to the two victims and was acquainted with them. The relationship of the female victim and the defendant turned sour, after which the female victim alleged that the defendant would scold her and the male victim from time to time. Subsequently between November 2022 and May 2023, the defendant posted a total of 20 messages containing the personal data of the victims in two open discussion groups and in two personal accounts of a social media platform, alongside some negative comments against them. The defendant was convicted of four charges of “disclosing personal data without data subject’s consent causing specified harm” in September 2024 upon entering a guilty plea. The Court sentenced the defendant to 30 days’ immediate imprisonment.



女子因感情及金錢糾紛「起底」前男友

事主與被告於2019年開始交往，並定期給予被告生活費。其後，兩人於2023年10月分手。數日後，被告在事主工作地點附近的街道上展示一塊載有事主個人資料的告示牌，並對事主作出負面的評論，包括聲稱事主欠債並要求還款。不久後，被告再分別於事主所居住的大廈外牆及單位門外張貼類似內容的單張，以及在一個社交媒體平台的公開群組發布類似訊息。於2025年1月，被告在認罪下被裁定三項「未獲資料當事人同意下披露其個人資料」的罪名成立。法院判處被告監禁六星期，緩刑兩年。

Female Doxxed Ex-boyfriend over Relationship Entanglement and Monetary Dispute

The victim and the defendant developed an intimate relationship since 2019, in which the victim paid maintenance fee to the defendant on a regular basis. The two subsequently broke up in October 2023. A few days later, the defendant displayed a signboard containing the personal data of the victim on a street near the victim's workplace, alongside some negative comments against the victim, including a claim to demand repayment of debt from the victim. Shortly afterwards, the defendant posted flyers with similar content outside the victim's residential building and his flat. The defendant also posted a message with similar content in an open discussion group on a social media platform. The defendant was convicted of three charges of "disclosing personal data without consent" in January 2025 upon entering a guilty plea. The Court sentenced the defendant to six weeks' imprisonment, suspended for two years.



進行調查

發表調查報告

私隱專員於報告年度發表了多份調查報告，包括關於(i)一個加密貨幣項目在香港的運作及(ii)八間機構透過一個網上招聘平台刊登匿名招聘廣告的調查結果。

私隱專員就一個加密貨幣項目在香港的運作進行調查，並於2024年5月發表調查結果。調查源於私隱專員關注該項目在香港的運作涉及嚴重的個人資料私隱風險，而參與該項目的人士需要讓有關機構透過虹膜掃描收集其面容及虹膜影像以「驗證」人類身分及製作虹膜編碼，藉此獲取註冊身分，並可定期獲得免費虛擬貨幣。調查發現該項目在香港的運作違反《私隱條例》下有關個人資料的收集(保障資料第1(1)、1(2)及1(3)原則)、保留(保障資料第2(2)原則)、透明度(保障資料第5原則)和查閱及改正資料(保障資料第6原則)的規定。

私隱專員已向相關機構送達執行通知，指示其糾正其違規事項，以及防止類似的違規行為再度發生。

Conducting Investigations

Releasing Investigation Reports

During the reporting year, the Privacy Commissioner published a number of investigation reports, including the investigation findings concerning (i) the operation of a cryptocurrency project in Hong Kong and (ii) eight organisations which placed “blind” recruitment advertisements (Blind Ads) through an online recruitment platform.

The Privacy Commissioner conducted an investigation regarding the operation of a cryptocurrency project in Hong Kong and published the investigation findings in May 2024. The matter arose from the Privacy Commissioner’s concern that the operation of the project in Hong Kong involved serious risks to personal data privacy. Participants of the project needed to allow the relevant organisation to collect their face and iris images through iris scanning to verify their humanness and generate an iris code, thereby obtaining a registered identity and after which the participants would be able to receive tokens in the form of cryptocurrency, at regular intervals for free. The investigation found that the operation of the project in Hong Kong had contravened the requirements of Data Protection Principles (DPPs) under the PDPO relating to collection (DPP 1(1), 1(2) and 1(3)), retention (DPP 2(2)), transparency (DPP 5), and data access and correction rights (DPP 6).

The Privacy Commissioner served an Enforcement Notice on the relevant organisation, directing it to remedy the contraventions and prevent similar recurrence in the future.

此外，私隱專員就八間機構透過一個網上招聘平台刊登匿名招聘廣告的個案於2024年12月發表調查結果。調查源於私隱專員關注有機構透過網上招聘平台刊登匿名招聘廣告以收集求職者個人資料的情況。私隱專員調查後發現，八間招聘機構在該網上招聘平台上刊登上述匿名招聘廣告，要求求職者向不知名的招聘機構提供個人資料，以及該網上招聘平台刊登該些招聘廣告，兩者同樣涉及不公平地收集求職者的個人資料，因而違反《私隱條例》下有關個人資料的收集(保障資料第1(2)原則)的規定。

私隱專員已向相關的資料使用者送達執行通知，指示他們糾正其違規事項，以及防止類似的違規行為再度發生，亦向餘下的資料使用者發出勸喻信。

Furthermore, the Privacy Commissioner published the investigation findings in December 2024 regarding eight organisations placing Blind Ads on an online recruitment platform. The investigation arose from the Privacy Commissioner's concern about some organisations' act of placing Blind Ads on online recruitment platforms to collect personal data from job applicants. Upon investigation, the Privacy Commissioner found that all eight organisations that placed the aforesaid Blind Ads on the online recruitment platform and requested job applicants to submit their personal data to unknown recruiting companies, and the online recruitment platform that published the same on its platform were involved in the unfair collection of the job applicants' personal data, which constituted a contravention of DPP 1(2) of the PDPO in relation to the collection of personal data.

The Privacy Commissioner served Enforcement Notices on the data users concerned, directing them to remedy their respective contraventions and prevent future recurrence. Advisory letters were also issued to the remaining data users.



公布八份有關資料外洩事故的調查結果

在報告年度內，私隱專員公布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。2024年8及10月，私隱專員分別就與勒索軟件攻擊有關的資料外洩事故的調查發表調查結果，當中包括學術團體、藝術團體及體育會。私隱專員裁定，上述個案的資料使用者均違反了《私隱條例》保障資料第4(1)原則有關個人資料保安的規定。

在2024年12月及2025年1月，私隱專員分別就一個政府部門通報的一宗個人資料外洩事故，以及一間非牟利機構遭受勒索軟件攻擊一事發表調查結果。私隱專員調查後發現，該政府部門及該機構均違反了《私隱條例》保障資料第2(2)及第4(1)原則有關個人資料保留及保安的規定。

Publishing Eight Investigation Findings on Data Breach Incidents

During the reporting year, the Privacy Commissioner published eight investigation findings on data breach incidents, six of which involved contraventions of the PDPO. In August and October 2024, the Privacy Commissioner published investigation findings respectively on data breach incidents relating to ransomware attacks targeting an academic group, an art organisation, and a sports association. The Privacy Commissioner found that the data users in the above cases contravened DPP 4(1) of the PDPO concerning the security of personal data.

In December 2024 and January 2025, the Privacy Commissioner published investigation findings on a data breach incident reported by a government department and a ransomware attack on the information systems of an NGO respectively. Upon investigation, the Privacy Commissioner found that the data users concerned contravened DPP 2(2) and 4(1) of the PDPO concerning the retention and security of personal data.



在2025年3月，私隱專員再就一間品牌管理及分銷公司的伺服器遭勒索軟件攻擊發表調查結果，並裁定該公司違反了《私隱條例》保障資料第4(1)原則有關個人資料保安的規定。

In March 2025, the Privacy Commissioner further published the investigation findings on a ransomware attack on the servers at a brand management and distribution company. It was found that the company contravened DPP 4(1) of the PDPO concerning the security of personal data.

私隱專員就上述調查向相關的資料使用者送達執行通知，指示他們糾正相關資料外洩事故並防止類似事故再度發生。

The Privacy Commissioner served Enforcement Notices on the data users concerned in the above investigations, directing them to remedy the breach and to prevent recurrence of similar incidents in the future.



提防個人資料詐騙

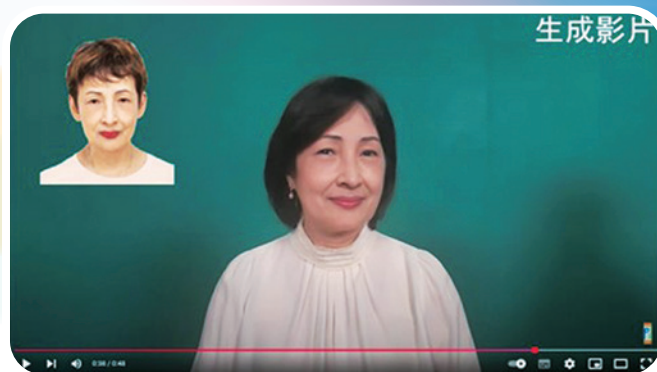
提高市民的防騙意識

面對層出不窮的詐騙手法，提高市民的防騙意識尤其關鍵。在報告年度內，私隱專員公署的個人資料防騙熱線接獲341宗與懷疑誘騙個人資料相關的查詢，較去年的318宗增加7%。公署亦設立了「防騙貼士」專題網站，為市民提供一站式的防騙資訊。公署同時透過發布新聞稿，呼籲市民及機構對騙徒日趨精密的詐騙手法保持警覺。私隱專員亦拍攝短片親身示範透過AI深度偽造技術實時換臉，提醒市民在AI時代有相、有片也未必有真相。

Preventing Personal Data Fraud

Enhancing Public Awareness of Fraud Prevention

With the ever-evolving deceptive tactics, it is crucial to raise public awareness of fraud prevention. During the reporting year, the PCPD's Personal Data Fraud Prevention Hotline received 341 enquiries relating to suspected personal data frauds, representing a 7% increase from the 318 cases in the previous reporting year. The PCPD also launched a thematic website entitled "Anti-Fraud Tips", with a view to providing a one-stop information portal for members of the public. On the other hand, media statements were also issued by the PCPD to urge the public and organisations to remain vigilant against increasingly sophisticated deceptive tactics used by fraudsters. To remind members of the public to beware of fake online contents in the AI era, the Privacy Commissioner also demonstrated instant face swapping using AI deepfake technology in short videos.



此外，私隱專員公署繼續以「個人資料咪亂俾 踢走騙徒靠晒你」為主題，推出一系列防騙宣傳活動，包括拍攝宣傳短片、派發宣傳海報、舉辦專題講座，以及於電視、網上平台、住宅大廈的大堂電視、醫院及各大運輸網絡宣傳防騙訊息。自2025年2月起，公署更與大專院校合作舉辦防騙講座，以免學生跌入騙徒陷阱。

In addition, the PCPD continued to launch a series of anti-fraud publicity activities under the theme "Don't Hand Over Your Personal Data – Beware of Fraudsters", which included producing promotional videos, distributing promotional posters, organising thematic seminars and promoting anti-fraud messages across televisions, online platforms, lobby televisions in residential buildings, hospitals, and major public transportation networks. Since February 2025, the PCPD has further collaborated with universities to organise anti-fraud talks to prevent students from falling prey to scams.



私隱專員公署亦積極參與各界舉辦的防騙活動，並於席間發表演講，以加強市民的防騙意識。

The PCPD also actively participated and delivered speeches in fraud prevention activities for different sectors to enhance public awareness of fraud prevention.



加強長者的警覺性

詐騙手法五花八門，長者亦成為騙徒的詐騙目標。為提高長者對不同詐騙手法的警覺性，私隱專員及公署關愛義工隊走進社區，於中秋前夕上門探訪長者，又為長者舉辦大型的聖誕防騙聚會，向一眾長者分享防騙貼士。

Enhancing Vigilance among Elders

With a myriad of fraudulent tricks, the elderly become prey for scammers. To raise awareness of various fraud tactics among the elderly, the Privacy Commissioner and the PCPD's Volunteer Team reached out to the community to pay home visits to the elderly on the eve of the Mid-Autumn Festival, and organised a Christmas fraud prevention gathering to share fraud prevention tips with elders.



此外，私隱專員公署亦與多間機構攜手合作，包括香港房屋協會、醫院管理局及社會福利署等，在本港多個出租屋邨、醫院、診所、長者地區中心、長者鄰舍中心、長者活動中心等張貼防騙宣傳海報或播放防騙短片；更透過醫院管理局的流動應用程式「HA Go」的橫額廣告吸引用戶瀏覽公署的防騙短片，藉此向長者宣傳防騙訊息。

Additionally, the PCPD also collaborated with various organisations, including the Hong Kong Housing Society, the Hospital Authority, and the Social Welfare Department, to display fraud prevention posters or broadcast anti-fraud videos in rental estates, hospitals, clinics, District Elderly Community Centres, Neighbourhood Elderly Centres, Social Centres for the Elderly and etc. across the city. Furthermore, the PCPD also made use of banner advertisements on “HA Go”, the Hospital Authority’s mobile application, to engage users’ interest in watching the PCPD’s anti-fraud videos, thereby promoting fraud prevention messages to the elderly.

推動數據跨境流動

致力促進粵港澳大灣區個人信息跨境流動

現時，全球數字經濟發展迅速，數據無疑在推動經濟增長方面發揮着不可或缺的作用。數據跨境流動在推進商務、貿易、經濟及科技等範疇的發展扮演舉足輕重的角色。內地於2024年11月發布的《全球數據跨境流動合作倡議》說明國家鼓勵及着重推動數據跨境流動的發展。

私隱專員公署一直致力促進粵港澳大灣區（大灣區）個人信息跨境流動，協助推動大灣區數字經濟的高質量發展，進一步令香港融入國家發展大局。

《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同》便利措施擴展至全港各行各業

國家互聯網信息辦公室（國家網信辦）與香港特別行政區政府創新科技及工業局（創科及工業局）早於2023年6月29日簽署《促進粵港澳大灣區數據跨境流動的合作備忘錄》，共同推動大灣區數據跨境流動的工作。同年12月13日，國家網信辦、創科及工業局及私隱專員公署共同制定《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同》（《大灣區標準合同》），旨在提供兩地合規途徑，促進大灣區個人信息跨境流動。

Promoting Cross-boundary Data Flows

Endeavouring to Facilitate Cross-boundary Flows of Personal Information Within the Greater Bay Area

With the global digital economy developing rapidly at present, data undoubtedly becomes indispensable in driving economic growth. Cross-border data flows play a significant role in promoting the development of commerce, trade, economy and technology, among others. The “Global Cross-border Data Flow Cooperation Initiative”, promulgated by the Mainland in November 2024, demonstrates that the Country encourages and emphasises the promotion of the development of cross-border data flows.

The PCPD has been endeavouring to facilitate cross-boundary flows of personal information within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA), which helps promote the high quality development of digital economy in the GBA and contributes to Hong Kong’s further integration into the overall development of the Country.

Extending Facilitation Measures of Standard Contract for Cross-boundary Flow of Personal Information Within the GBA (Mainland, Hong Kong) to All Sectors in Hong Kong

The Cyberspace Administration of China (CAC) and the Innovation, Technology and Industry Bureau (ITIB) of the Government of the Hong Kong Special Administrative Region signed the Memorandum of Understanding on Facilitating Cross-boundary Data Flow Within the Guangdong-Hong Kong-Macao Greater Bay Area on 29 June 2023 to jointly promote cross-boundary data flows in the GBA. On 13 December 2023, the CAC, the ITIB, and the PCPD formulated the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) (GBA SC), thereby providing a mechanism to facilitate cross-boundary flows of personal information within the GBA that is compliant with the relevant requirements in both the Mainland and Hong Kong.

《行政長官2024年施政報告》宣布，將原本只在銀行、信貸資料及醫療業界試行的《大灣區標準合同》便利措施擴展至全港各行各業。香港特別行政區政府數字政策辦公室（數字辦）隨後公布，相關安排於2024年11月1日起全面生效。

有關措施不但能便民利企，更可以進一步促進大灣區個人信息跨境流動，以配合政府建立「數字灣區」的政策。

鼓勵企業採用《大灣區標準合同》

私隱專員公署全力支持實施《大灣區標準合同》便利措施，並積極開展相關的宣傳教育工作，推廣《大灣區標準合同》應用於不同行業中。

私隱專員公署於2024年4月舉辦「粵港澳大灣區個人信息跨境流動」研討會，吸引超過130名來自銀行、法律、保險等行業及政府或公營機構的人士參加。研討會上，私隱專員向參加者闡釋合約方在《大灣區標準合同》下的義務和責任，並概述根據《私隱條例》從香港跨境轉移個人資料的要求，及國家網信辦公布的《促進和規範數據跨境流動規定》的特定豁免條文。

In the Chief Executive's Policy Address 2024, it was announced that the facilitation measures of the GBA SC, originally piloted in the banking, credit referencing, and healthcare industries, would be extended to all sectors in Hong Kong. Subsequently, as announced by the Digital Policy Office (DPO) of the Government of the Hong Kong Special Administrative Region, the relevant arrangements came into effect on 1 November 2024.

Not only do the above measures benefit individuals and organisations, but they also facilitate cross-boundary flows of personal information within the GBA, as part of the Government's initiative in building a "Digital Bay Area".

Encouraging Enterprises to Adopt the GBA SC

The PCPD fully supports the implementation of the facilitation measures of the GBA SC, and enthusiastically engages in relevant publicity and education endeavours to promote the adoption of the GBA SC across industries and sectors.

The PCPD organised a seminar on "Cross-boundary Flow of Personal Information Within the Greater Bay Area" in April 2024, which attracted more than 130 participants from various sectors, including banking, legal, insurance and government or public bodies. At the seminar, the Privacy Commissioner explained the obligations and responsibilities of contracting parties under the GBA SC, and outlined the requirements under the PDPO pertaining to cross-border personal data transfers from Hong Kong as well as the relaxation provisions under the Regulations on Facilitating and Regulating Cross-Border Data Flow issued by the CAC.

此外，私隱專員於2024年12月出席由數字辦舉辦的《大灣區標準合同》便利措施簡介會。私隱專員在簡介會上向各行各業的人士介紹《大灣區標準合同》的內容以及《私隱條例》的相關規定，並鼓勵企業採用《大灣區標準合同》進行大灣區內的個人信息跨境轉移。

In addition, the Privacy Commissioner attended the briefing session for facilitation measures on the GBA SC organised by the DPO in December 2024, where the Privacy Commissioner introduced the terms of the GBA SC and the relevant requirements under the PDPO to attendees from various sectors, and encouraged enterprises to adopt the GBA SC for cross-boundary transfers of personal information within the GBA.



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%。

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 telephone¹ 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 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。

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

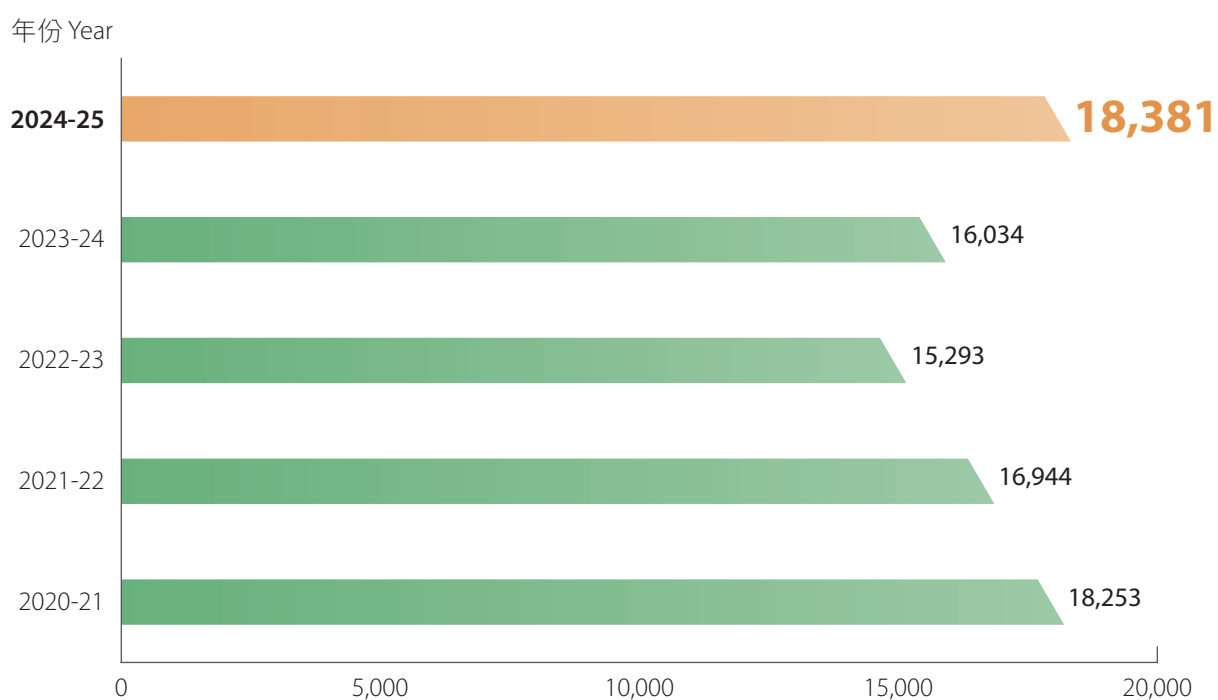


圖 Figure 3.1



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

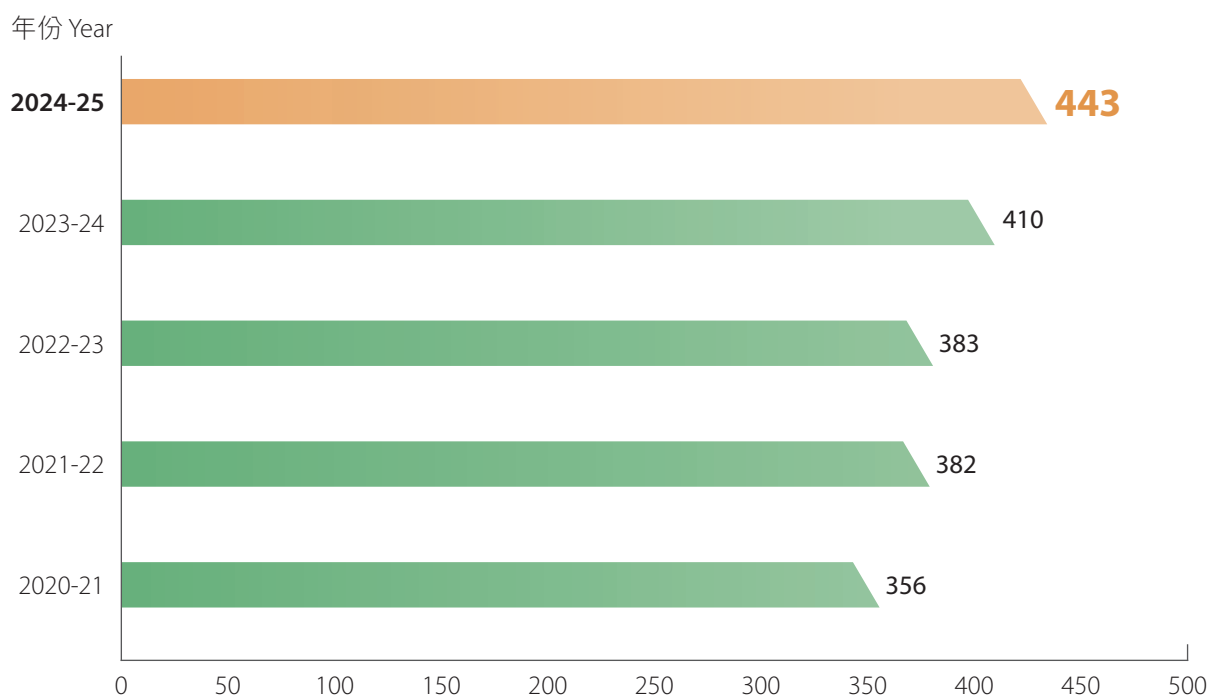


圖 Figure 3.2

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

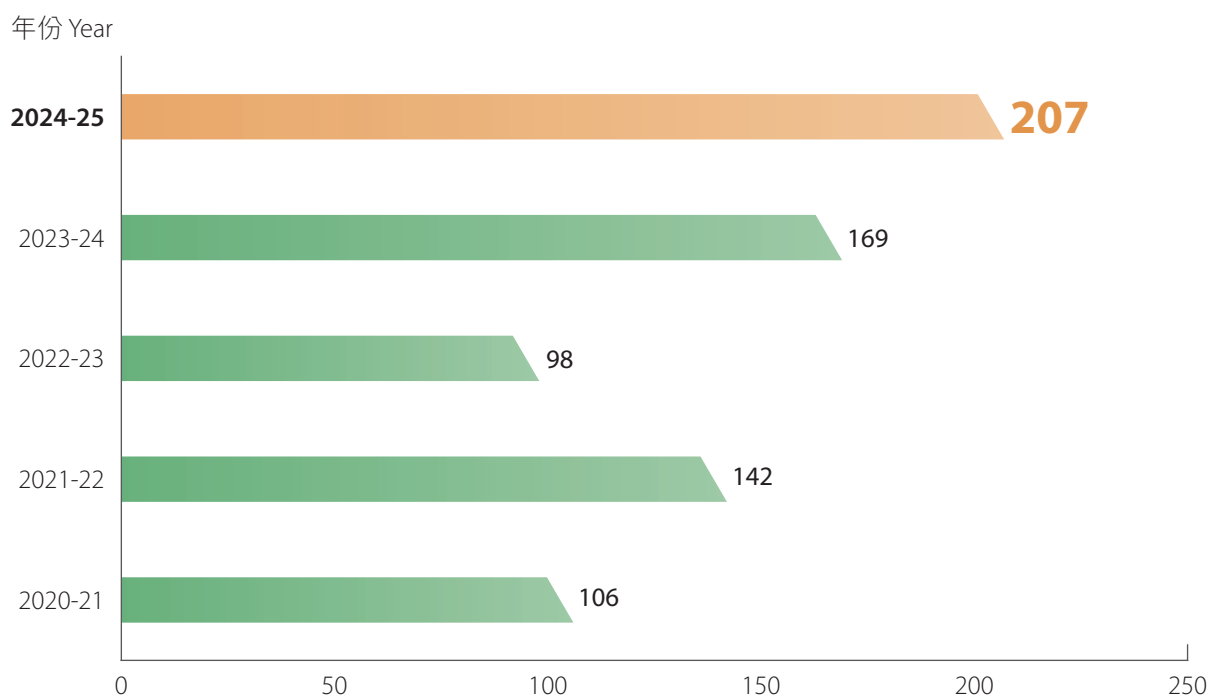


圖 Figure 3.3

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：

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) 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； | (1) Lack of written policies on the retention of personal data collected in the RTD operations; |
| (2) 未有清楚向承辦商提出刪除相關資料的要求； | (2) Failure to make unequivocal request to the contractor for deletion of the relevant data; |
| (3) 沒有自行主動刪除涉事的個人資料；及 | (3) Failure to take the initiative to delete the personal data involved; and |
| (4) 沒有適當跟進承辦商刪除資料。 | (4) Failure to properly follow up with the contractor on the deletion of data. |

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。

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.

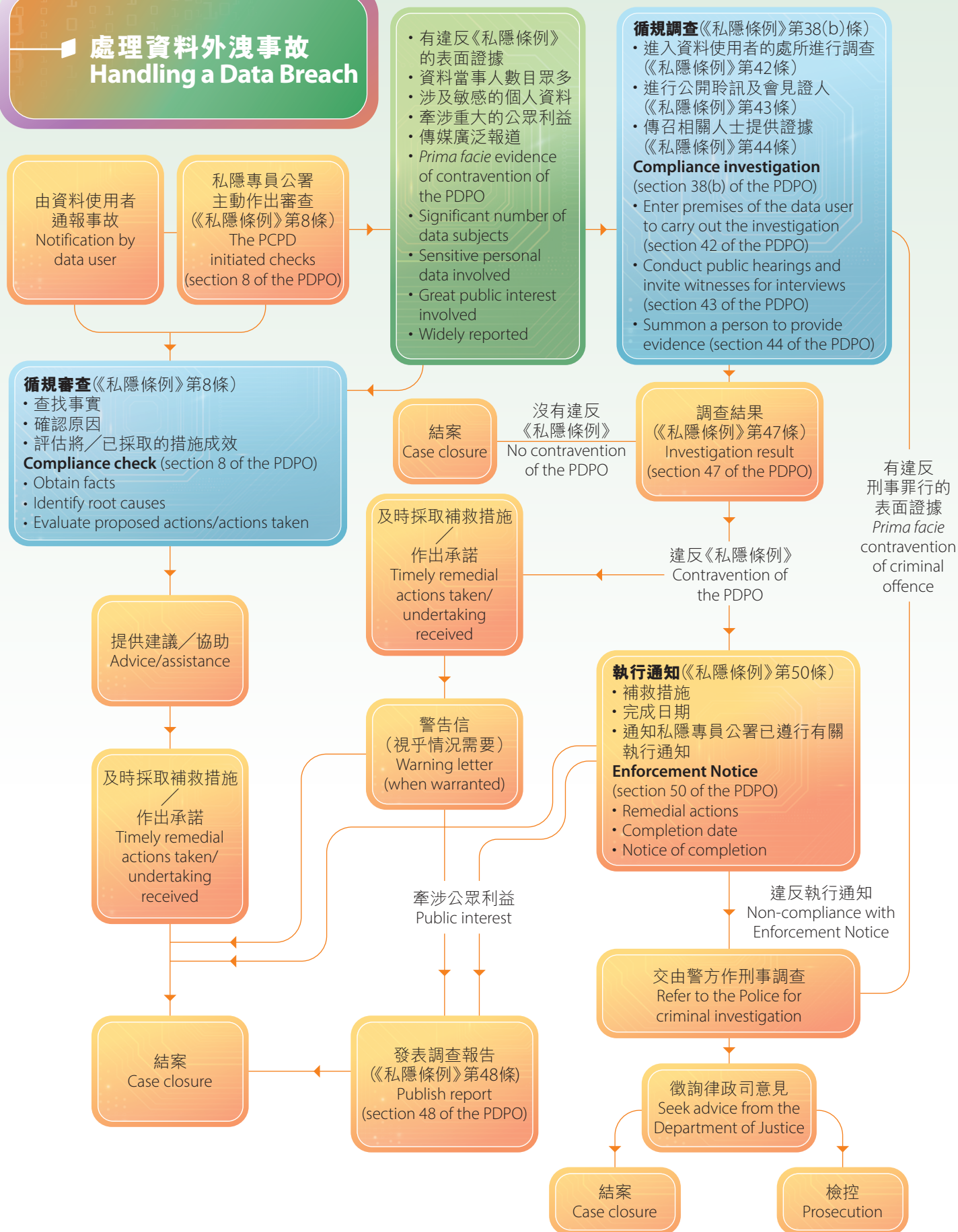
資訊保安措施

- 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



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。

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。

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.

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。

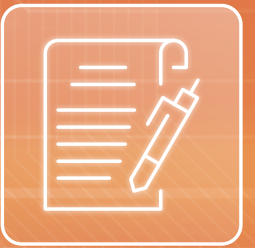
Compliance Promotion

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.



投訴及上訴

Complaints and Appeals

投訴處理

投訴的整體趨勢

在本報告年度，私隱專員公署接獲 3,450 宗投訴（當中包括經公署主動網上巡查發現的「起底」個案），較 2023-24 年度的 3,600 宗下跌約 4.2%。其中，涉及「起底」的投訴個案為 305 宗，而經公署主動網上巡查發現的個案有 65 宗。

隨着私隱專員公署持續針對「起底」罪行果斷執法，「起底」情況已經顯著改善。與「起底」相關的投訴及經公署主動網上巡查發現的「起底」個案總數，由上一報告年度的 631 宗顯著下跌 41% 至本報告年度的 370 宗。儘管近年涉及「起底」的個案有持續下跌的趨勢，惟打擊「起底」仍然是公署的重要工作目標。

Complaint Handling

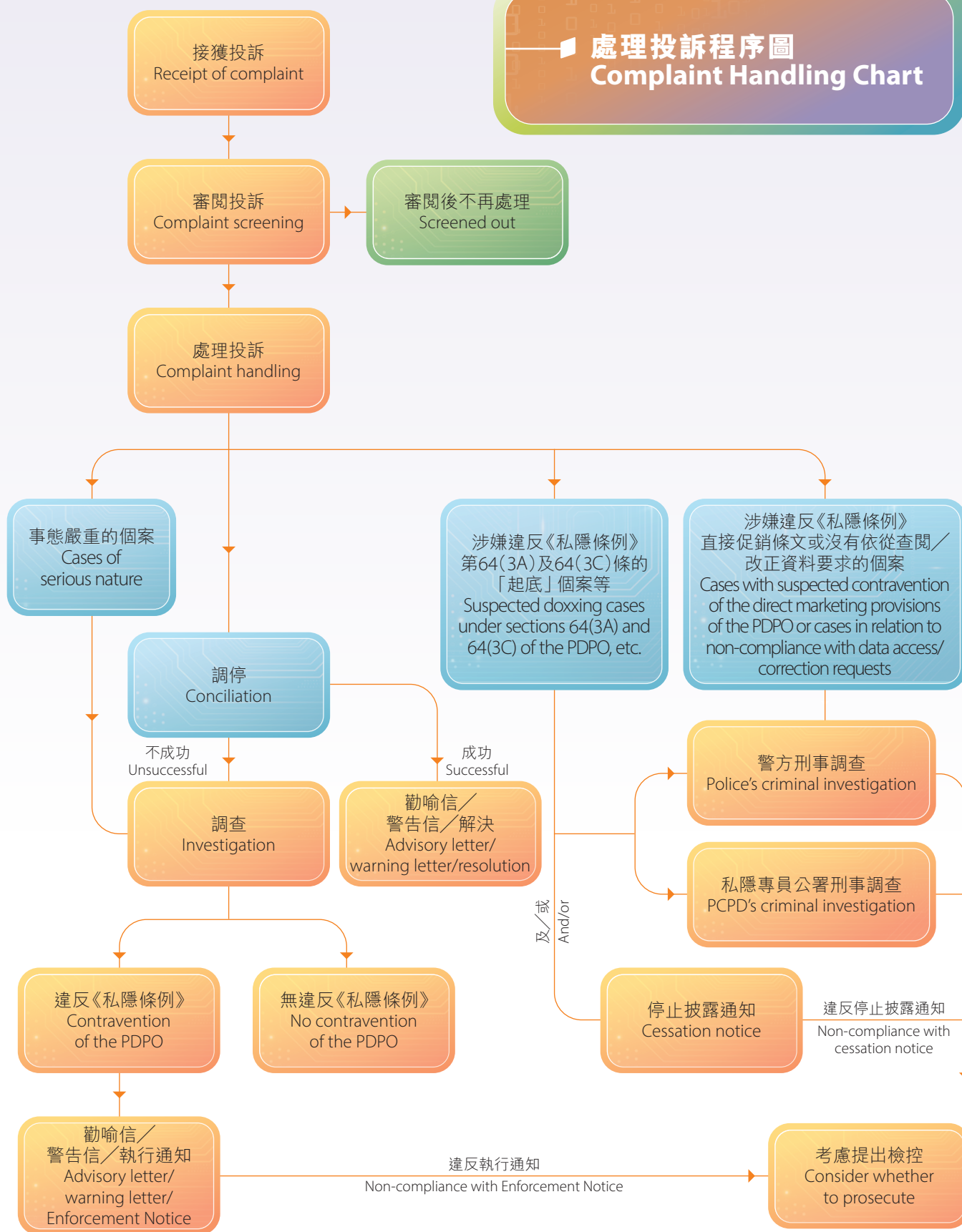
Overall Trend of Complaints

In this reporting year, the PCPD received 3,450 complaints (which includes the number of doxxing cases uncovered through proactive online patrols), indicating a 4.2% decrease from the 3,600 cases in 2023-24. This total comprised 305 doxxing-related complaints and 65 doxxing cases uncovered by proactive online patrols.

With the continuous and unwavering law enforcement efforts of the PCPD, the problem of doxxing has largely been ameliorated. The total number of doxxing-related complaints and cases detected through proactive online patrols dropped significantly by 41%, from 631 to 370 year-on-year. While doxxing cases continue to decline in recent years, combatting doxxing offences remains a key priority for the PCPD.



處理投訴程序圖 Complaint Handling Chart



詳情請參閱私隱專員公署的處理投訴政策：https://www.pcpd.org.hk/tc_chi/complaints/policy/complaint_policy.html

For details, please refer to the PCPD's Complaint Handling Policy: https://www.pcpd.org.hk/english/complaints/policy/complaint_policy.html

接獲的投訴及經主動網上巡查發現的「起底」個案

私隱專員公署在2024-25年度共收到3,450宗投訴及經主動網上巡查發現的「起底」個案。撇除當中305宗與「起底」相關的投訴個案及65宗經主動網上巡查發現的「起底」個案，公署在本報告年度共接獲3,080宗非「起底」相關的投訴，較去年增加3.7%(圖4.1)。

Complaints Received and Doxxing Cases Uncovered by Proactive Online Patrols

The number of complaints received and doxxing cases uncovered by proactive online patrols of the PCPD totalled 3,450 in the year 2024-25. With the 305 doxxing-related complaints and 65 doxxing cases uncovered by proactive online patrols factored out, the PCPD received 3,080 non-doxxing-related complaints in the reporting year, representing a 3.7% increase from the previous reporting year (Figure 4.1).

接獲的投訴個案及作出主動巡查個案數目 Number of Complaints Received and Doxxing Cases Uncovered by Proactive Online Patrols

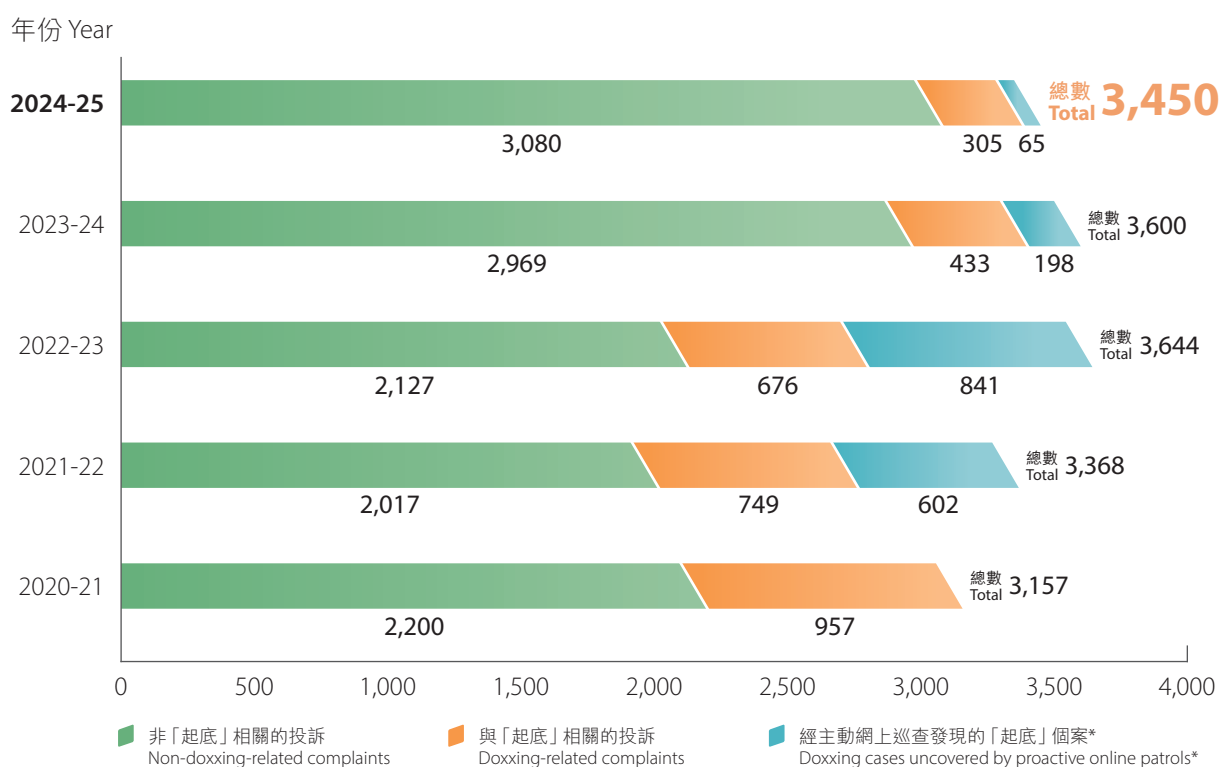


圖 Figure 4.1

* 自2021年《修訂條例》於2021年10月8日正式生效後，私隱專員公署定期作出主動網上巡查，就發現的「起底」訊息，私隱專員會根據《修訂條例》賦予的權力發出停止披露通知。

* Since the 2021 Amendment Ordinance came into force on 8 October 2021, the PCPD has been conducting regular proactive online patrols and the Privacy Commissioner would issue cessation notices in relation to doxxing messages found, as empowered under the Amendment Ordinance.

被投訴者類別

3,080 宗與「起底」無關的投訴的被投訴者可分為以下類別(圖4.2)：

- 私營機構(1,520 宗)，主要涉及銀行、金融機構、物業管理公司、零售機構及醫療機構；
- 個人(1,221 宗)，當中大部分個案與私人事務引起的糾紛及鄰居安裝閉路電視有關；及
- 政府部門及公共機構(339 宗)，主要涉及醫護機構、執法機關及教育機構。

Types of Parties being Complained Against

The types of parties being complained against among the 3,080 non-doxxing-related complaints can be categorised as follows (Figure 4.2):

- Private organisations (1,520 cases), with the majority involving banks, financial institutions, property management companies, retail business organisations, and healthcare institutions;
- Individuals (1,221 cases), with disputes mainly arising from domestic affairs and the installation of CCTV by neighbours; and
- Government departments and public organisations (339 cases), with the majority involving healthcare institutions, law enforcement agencies, and educational institutions.

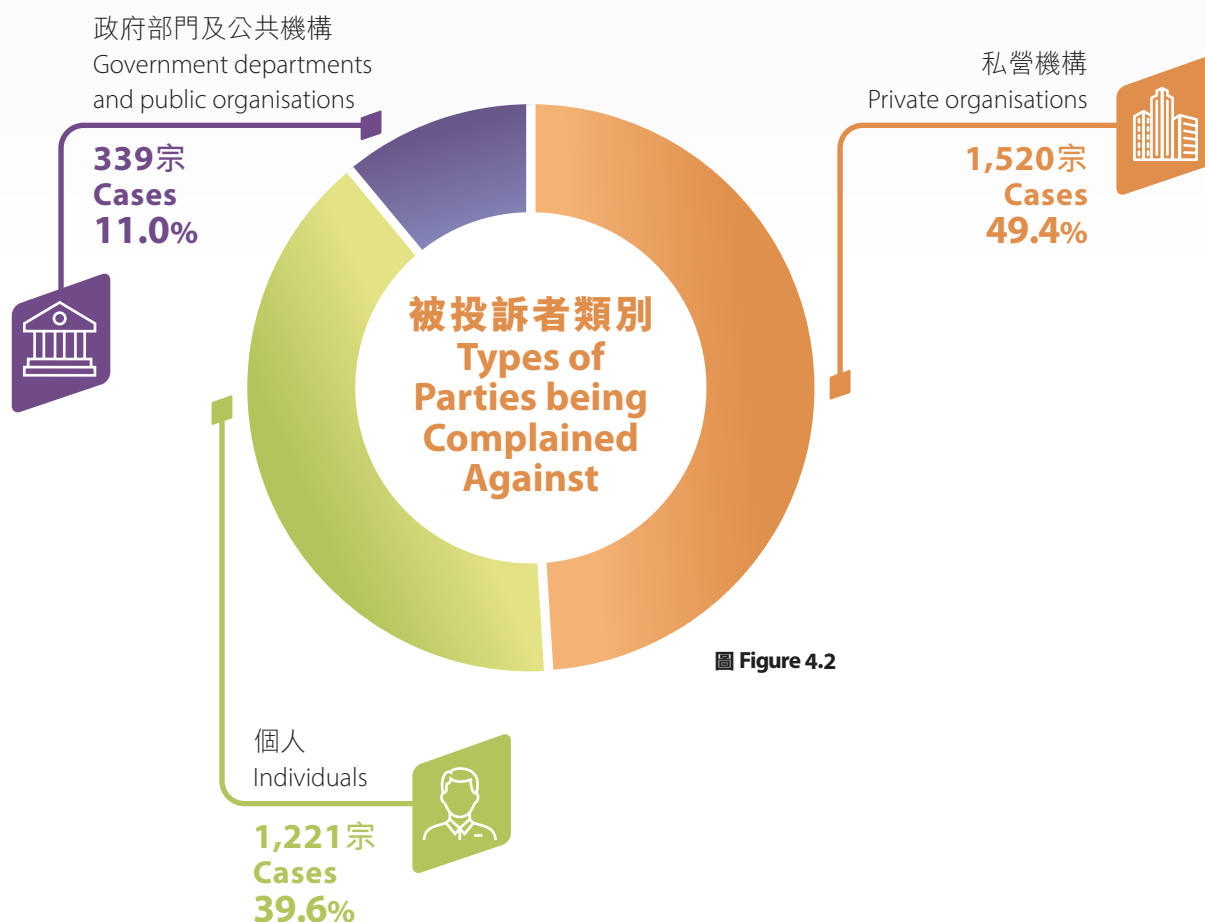


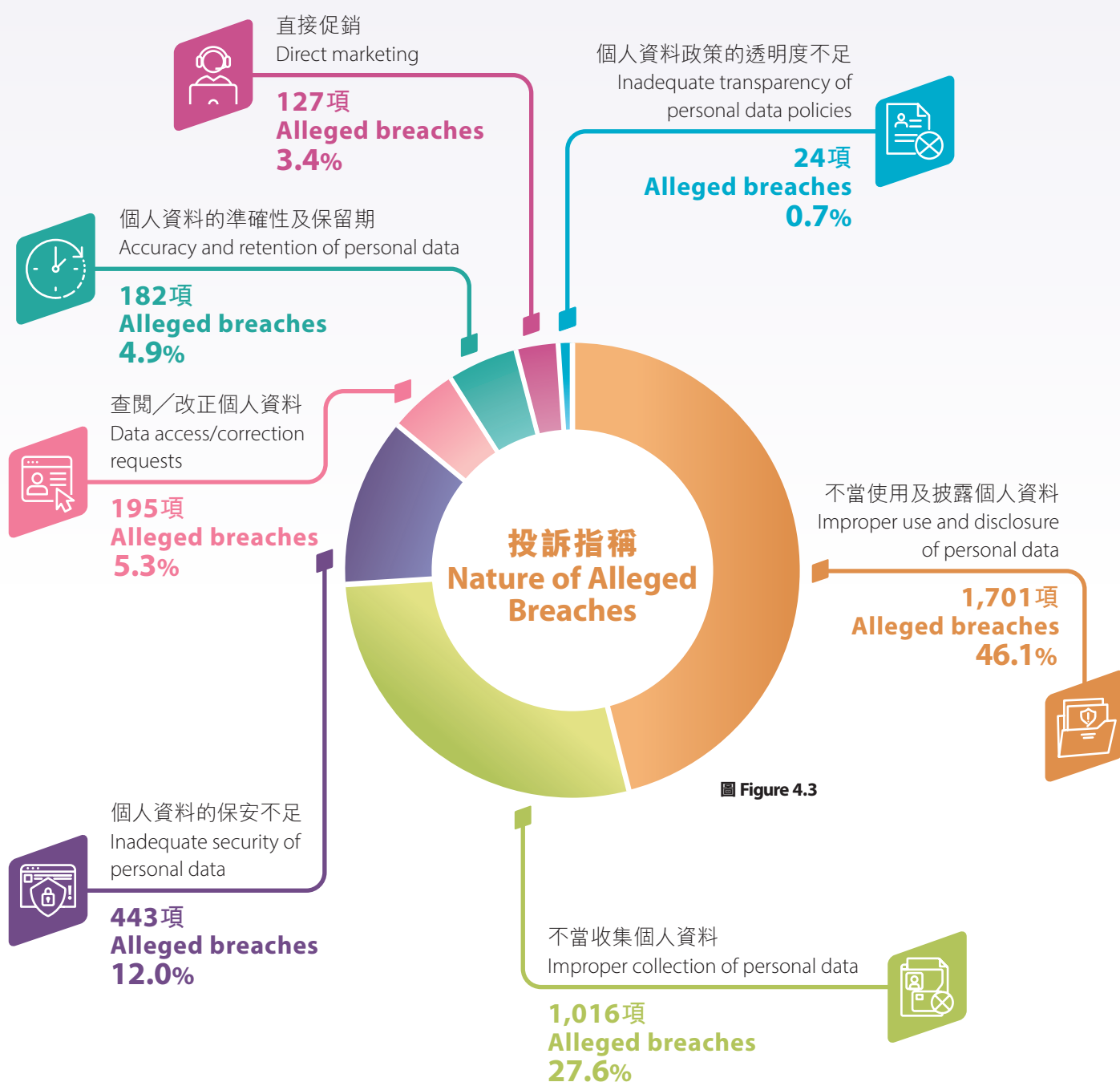
圖 Figure 4.2

投訴指稱

除「起底」相關個案外，3,080宗投訴共涉及3,688項涉嫌違規行為（單一投訴或會牽涉多於一項指稱），涉嫌的違規行為的性質如下（圖4.3）：

Nature of Alleged Breaches

Excluding doxxing-related cases, the 3,080 complaints involved a total of 3,688 alleged breaches (as one complaint might have involved more than one allegation). The nature of the alleged breaches is shown below (Figure 4.3):



投訴所涉範疇

撇除「起底」個案，私隱專員公署在報告年度內接獲的投訴所涉及的主要範疇分布如圖4.4所示。

雖然與資訊科技相關的投訴由去年的1,304宗減少21%至2024-25年度的1,030宗，惟此類別的投訴仍然遠超其他範疇的投訴，佔整體投訴個案約三成。有關情況是源於社交媒體和智能電話應用程式的使用在日常生活日漸增加。在這數碼時代，資料使用者透過互聯網或電子方式收集及使用更多個人資料的情況已成不可避免的趨勢。

除了與資訊科技相關的投訴外，其他範疇的投訴分布與上年度相若，其中涉及香港身份證號碼／副本及其他身份代號的投訴比上一報告年度減少約12%。有關減幅反映資料使用者在《私隱條例》下有關收集香港身份證號碼／副本及其他身份代號方面的保障個人資料私隱意識顯著提升，顯示私隱專員公署在公眾教育、循規及執法方面的努力取得成效。

Subject Matters of Complaints

Excluding doxxing cases, the distribution of major subject matters of complaints received by the PCPD in the reporting year is as shown in figure 4.4.

While the number of complaints relating to information technology decreased by 21% from 1,304 in the previous reporting year to 1,030 in the year 2024-25, this category still outnumbered all other subject matters, accounting for approximately 30% of all complaints. This is attributable to the increasing use of social media and smartphone applications in daily life. In this digital era, it is an inevitable trend for data users to collect and use more personal data through the Internet or electronic means.

Aside from the complaints relating to information technology, the distribution of other major subject matters of complaints received by the PCPD in the reporting year was similar to that of last year. Notably, the number of complaints relating to Hong Kong Identity Card (HKID Card) numbers/copies and other personal identifiers decreased by 12% compared with the last reporting year. The decline reflects a significant increase in data users' awareness of protecting personal data privacy in the collection of HKID Card numbers/copies and other identifiers under the PDPO, indicating the effectiveness of the PCPD's efforts in public education, compliance and enforcement initiatives.

投訴所涉範疇 Subject Matters of Complaints

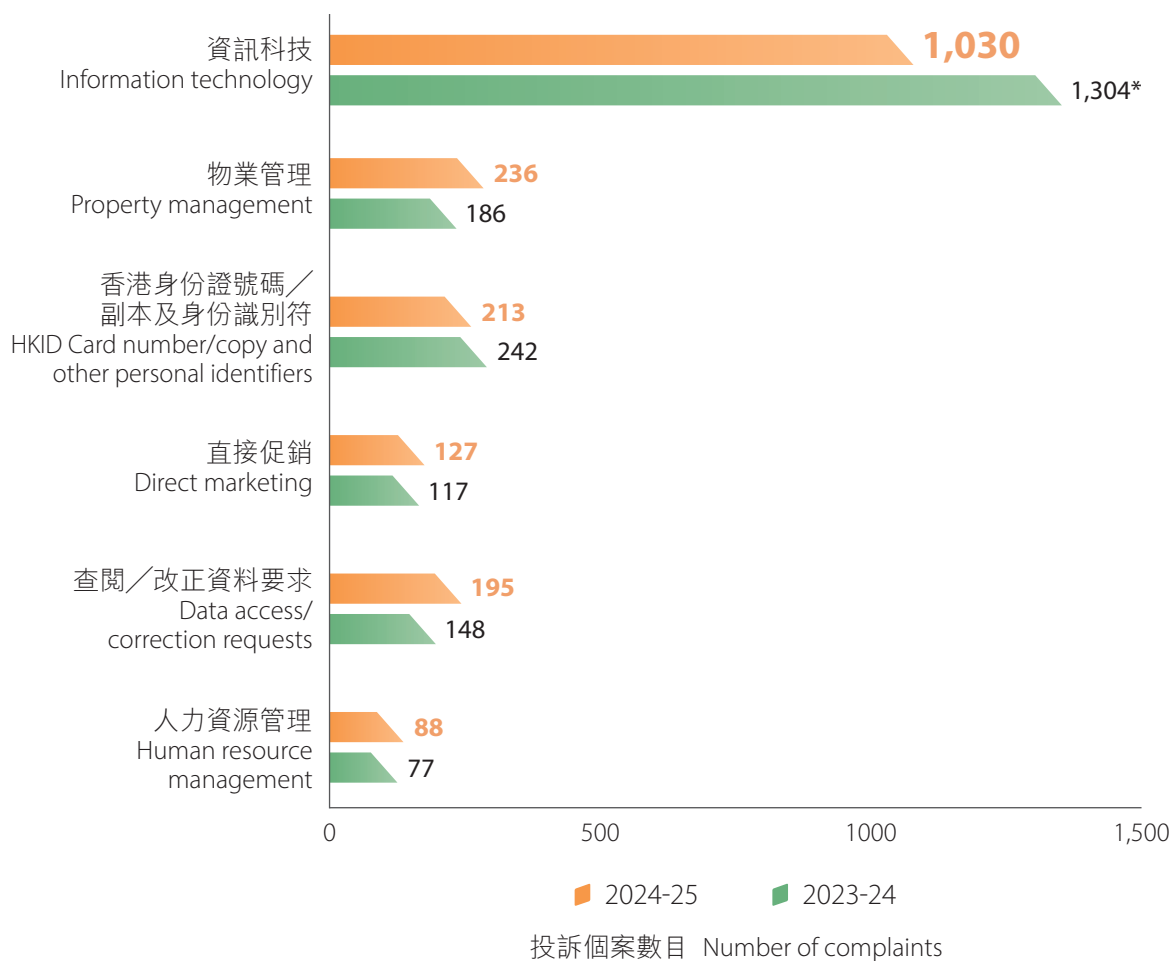


圖 Figure 4.4

* 超過500宗與資訊科技有關的投訴源自於同一位投訴人。

* There are more than 500 complaints related to information technology lodged by the same complainant.

年度投訴摘要

在 2024-25 報告年度，私隱專員公署共處理了 4,278 宗投訴，包括新接獲的 3,450 宗投訴（當中包括 305 宗與「起底」相關的投訴及 65 宗經主動網上巡查發現的「起底」個案），以及承接上一報告年度的 828 宗投訴。截至 2025 年 3 月 31 日，其中 3,238 宗投訴（75.7%）已在本報告年度完成，餘下 1,040 宗（24.3%）則仍在處理中。

若撇除與「起底」相關的投訴及經網上巡查發現的「起底」個案，私隱專員公署在本報告年度完成處理 2,822 宗非「起底」相關的投訴，其中 1,830 宗經公署初步評估後結案，餘下 992 宗則獲受理作進一步處理。

在這 992 宗投訴當中，私隱專員公署以調停方式成功解決 881 宗（88.8%）。另有 21 宗涉及刑事成份的投訴（主要與直接促銷有關），公署在收集涉嫌違反《私隱條例》相關規定的初步證據後，將案件轉交警方作進一步調查及考慮檢控。公署就餘下的 90 宗投訴進行調查，並發現其中 33 宗違反《私隱條例》的規定。公署已向被投訴者發出執行通知、警告信或勸喻信，指示或要求其採取補救行動或適當和切實可行的措施，以防止違規行為再次發生。

Summary of Complaints Handled

In the 2024-25 reporting year, the PCPD handled a total of 4,278 complaints, which consisted of 3,450 new cases (including 305 doxxing-related complaints and 65 doxxing cases uncovered by proactive online patrols) and 828 complaints carried forward from the previous reporting year. Among them, the handling of 3,238 complaints (75.7%) were concluded during the reporting year, while the remaining 1,040 complaints (24.3%) were still in progress as at 31 March 2025.

Excluding the doxxing-related complaints and doxxing cases uncovered by proactive online patrols, the PCPD completed the handling of 2,822 non-doxxing related complaints in this reporting year, of which 1,830 complaints were concluded after preliminary assessments, while the other 992 complaints were accepted for further handling.

Among these 992 complaints, the PCPD successfully resolved 881 complaints (88.8%) through conciliation. The other 21 complaints, which involved possible criminal elements (mostly relating to direct marketing), were referred to the Police for further investigation and consideration for prosecution following the PCPD's collection of *prima facie* evidence of suspected contraventions of the PDPO. The PCPD carried out investigations into the remaining 90 complaints and found 33 cases to be in contravention of the requirements of the PDPO. The PCPD issued Enforcement Notices, warning letters, or advisory letters to direct or request the parties being complained against to take remedial actions or implement appropriate and practicable measures to prevent recurrence of the contraventions.

進行調查

私隱專員於報告年度內發表了多份調查報告，當中包括(i)有關一個加密貨幣項目在香港的運作及(ii)八間機構透過一個網上招聘平台刊登匿名招聘廣告的調查結果。

關於一個加密貨幣項目在香港的運作的調查結果

私隱專員就一個加密貨幣項目(該項目)在香港的運作發表調查結果。調查源於私隱專員關注該項目在香港的運作涉及嚴重的個人資料私隱風險，因此主動啟動對該項目的調查，以了解該項目在香港的運作是否涉及違反《私隱條例》的規定。

調查發現，參與該項目的人士需要讓有關機構透過虹膜掃描收集其面容及虹膜影像以「驗證」人類身分及製作虹膜編碼，藉此獲取註冊身分，並可定期免費獲得虛擬貨幣。

私隱專員裁定該項目在香港的運作違反《私隱條例》附表1有關個人資料的收集、保留、透明度、查閱及改正資料的保障資料原則，當中包括：

Conducting Investigations

During the reporting period, the Privacy Commissioner published a number of investigation reports, including the investigation findings concerning (i) the operation of a cryptocurrency project in Hong Kong and (ii) eight organisations which placed “blind” recruitment advertisements (Blind Ads).

Investigation Findings on the Operation of a Cryptocurrency Project in Hong Kong

The Privacy Commissioner published investigation findings regarding the operation of a cryptocurrency project (the Project) in Hong Kong. Originating from the Privacy Commissioner’s concern that the operation of the Project in Hong Kong involved serious risks to personal data privacy, proactive investigation was initiated by the Privacy Commissioner into the Project to determine whether the operation of the Project in Hong Kong has contravened the requirements of the PDPO.

The investigation findings showed that participants of the Project were asked to authorise the relevant organisation’s collection of images of their faces and irises through iris scanning, with a view to verifying their humanness and generating iris codes, as part of obtaining a registered identity that allowed them to receive tokens in the form of cryptocurrency at regular intervals for free.

The Privacy Commissioner found that the operation of the Project in Hong Kong had contravened the Data Protection Principles (DPPs) in Schedule 1 to the PDPO relating to the collection, retention, transparency, data access and correction rights, which included:

- 保障資料第1(1)原則：私隱專員認為該項目收集面容及虹膜影像並非必需，而且超乎適度；
- DPP 1(1): The Privacy Commissioner considered that the face and iris images collected by the Project were unnecessary and excessive;
- 保障資料第1(2)原則：該項目不公平地收集個人資料，特別是相關《私隱聲明》和《生物辨識資料同意書》的內容不但欠缺中文版本，而且營運點的職員也不會向參與者解說或確認他們明白上述文件的內容，更不會告知參與者向其披露生物辨識資料的風險，又或解答參與者的問題；
- DPP 1(2): The Project collected personal data unfairly, in particular the relevant “Privacy Notice” and “Biometric Data Consent Form” were not available in Chinese, nor did the iris scanning device operators at the operating locations offer any explanation or confirm with the participants to ensure that they understood the said documents. They also did not communicate the possible risks pertaining to the disclosure of biometric data, nor did they answer participants’ questions;
- 保障資料第1(3)原則：在收集個人資料時或之前，參與者未獲清楚告知法例上訂明需要告知的資訊，包括收集個人資料的目的、他們是有責任或可自願提供其個人資料、資料可轉移予哪些類別的人士，以及參與者查閱和更正個人資料的權利和方式；
- DPP 1(3): On or before the collection of personal data, participants were not clearly informed of the information as specified under the PDPO, including the purpose(s) of collection, whether it was obligatory or voluntary for them to provide their personal data, the classes of possible transferees, and the right and means to request access to and correction of their personal data;
- 保障資料第2(2)原則：該項目會保留個人資料長達10年，以用作訓練核實身分程序的人工智能模型，私隱專員認為時間過長，實屬過度保留個人資料；
- DPP 2(2): The Project would retain personal data for a maximum of 10 years for the purpose of training AI models for the user verification process. The Privacy Commissioner considered that the retention period was too long which amounted to prolonged retention of personal data;

保障資料第5原則：處理個人資料的政策及行事常規透明度不足。在相關時間，該項目的《私隱聲明》並沒有提供中文版，對以中文為母語的參與者而言，私隱專員認為參與者無法清楚明白相關政策、行事常規、條款或細則，因此透明度不足；及

保障資料第6原則：參與者未能行使查閱和改正個人資料的權利。

DPP 5: Insufficient transparency of the personal data policy and practices. The Privacy Notice at the material time was not available in Chinese. The Privacy Commissioner was of the view that participants using Chinese as native language would not be able to clearly understand the relevant policies and practices, terms and conditions of the Project, resulting in a lack of transparency; and

DPP 6: Participants did not have the means to exercise their rights of data access and correction.

基於以上缺失，私隱專員遂向有關機構發出執行通知，要求該項目停止在香港的所有運作，包括以虹膜掃描裝置收集市民的虹膜及面容影像。

In view of the above deficiencies, the Privacy Commissioner served an Enforcement Notice on the relevant organisation, directing it to cease all operations under the Project in Hong Kong. These included scanning and collecting iris and face images of members of the public using iris scanning devices.

關於八間機構透過一個網上招聘平台刊登匿名招聘廣告的調查結果

私隱專員就八間機構透過一個網上招聘平台(該平台)刊登匿名招聘廣告發表調查結果。調查源於私隱專員關注有機構透過該平台刊登匿名招聘廣告以收集求職者個人資料的情況可能涉及違反《私隱條例》的相關規定。私隱專員就此啟動對該平台及八間涉及在該平台刊登匿名招聘廣告的機構的調查。

Investigation Findings on Eight Organisations Placing Blind Ads on an Online Recruitment Platform

The Privacy Commissioner published investigation findings regarding eight organisations placing Blind Ads on an online recruitment platform (the Platform). The investigation arose from the Privacy Commissioner's concern that the act of placing Blind Ads on the Platform by organisations to collect personal data from job applicants might constitute a contravention of the relevant requirements under the PDPO. As such, investigations were initiated on the Platform and eight organisations that had placed Blind Ads on the Platform.

一般而言，匿名招聘廣告即廣告中沒有披露招聘機構（僱主或其委託的招聘代理）的名稱或提供足夠資料以辨識相關機構的身分，以及沒有向求職者提供方式聯絡機構以獲取進一步資料或聯絡方式未有提供足夠的資料以辨識機構的身分，卻直接要求求職者遞交個人資料，例如香港身份證號碼、聯絡資料或履歷等。

調查發現，在該平台登記開立帳戶的機構可透過其帳戶刊登廣告進行招聘。招聘機構可以用「私人廣告商」（即「Private Advertiser」）的名義刊登招聘廣告而不披露機構的名稱。八間招聘機構在調查中透過該平台以「私人廣告商」名義刊登匿名招聘廣告，收集求職者的個人資料。

私隱專員裁定八間招聘機構在該平台上刊登上述匿名招聘廣告，要求求職者向不知名的招聘機構提供個人資料，以及該平台透過其平台刊登該些廣告，兩者同樣涉及不公平地收集求職者的個人資料，因而違反《私隱條例》的保障資料第1(2)原則的規定。

私隱專員遂向該平台及三間招聘機構發出執行通知，指示相關機構糾正其違反事項，以及防止同類違反的行為再發生，亦向餘下五間機構發出勸喻信。

In general, a Blind Ad is one that does not identify the recruiting organisation (either the employer or a recruitment agency acting on its behalf) nor contain sufficient information to identify the organisation, and does not provide a means for job applicants to make further enquiries or such means does not contain sufficient information to identify the organisation. Yet, it directly invites job applicants to submit their personal data, such as their HKID Card numbers, contact details or resumes.

The investigation revealed that organisations with a registered account on the Platform could place recruitment advertisements on it. A recruiting organisation can publish recruitment advertisements in the name of a "Private Advertiser" without disclosing its name. The eight recruiting organisations under investigation published Blind Ads in the names of "Private Advertisers" to collect the job applicants' personal data.

The Privacy Commissioner found that all eight organisations that placed the aforesaid Blind Ads on the Platform and requested job applicants to submit their personal data to unknown recruiting companies, and the Platform that published the said Blind Ads were involved in the unfair collection of the personal data of job applicants, which constituted contraventions of DPP 1(2) of the PDPO.

The Privacy Commissioner therefore served Enforcement Notices on the Platform and three recruiting organisations, directing them to take measures to remedy the contraventions and prevent future recurrence of similar contraventions. Advisory letters were issued to the remaining five organisations.

向行政上訴委員會提出的上訴

行政上訴委員會(委員會)是根據《行政上訴委員會條例》(香港法例第442章)而設立的法定組織，負責處理對私隱專員在《私隱條例》下的決定而提出的上訴，並作出裁決。

行政上訴案件統計資料

於報告年度內，委員會合共頒布16宗裁決(包括於過往年度提出的上訴)，當中14宗被駁回及兩宗被裁定得直(即發還私隱專員公署作進一步處理)。在同一報告年度內，有五宗上訴由上訴人自行撤回(圖4.5)。

Appeals Lodged with the Administrative Appeals Board

The Administrative Appeals Board (AAB), established under the Administrative Appeals Board Ordinance (Chapter 442 of the Laws of Hong Kong), is the statutory body which hears and determines appeals against the Privacy Commissioner's decisions under the PDPO.

Statistics of AAB cases

During the reporting year, the AAB handed down a total of 16 decisions (which included appeals lodged in previous years), in which 14 appeals were dismissed and two appeals were allowed (i.e. remitted to the PCPD for further investigation). In the same reporting year, five appeals were lodged and subsequently withdrawn by the appellants (Figure 4.5).

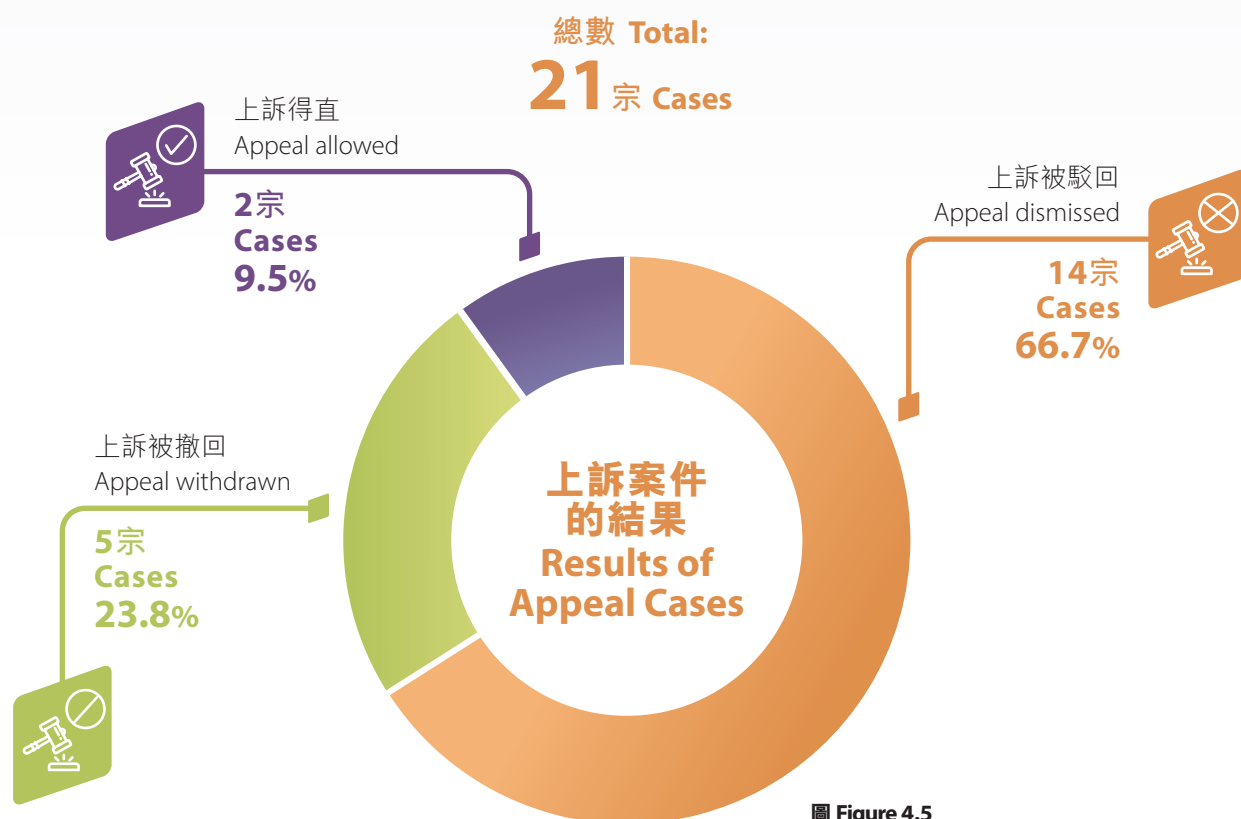


圖 Figure 4.5

接獲的行政上訴案件的性質及涉及《私隱條例》的規定

私隱專員公署於報告年度內共接獲43宗上訴個案。其中：

- 23宗個案為不服私隱專員根據《私隱條例》第39(1)及／或(2)條及公署發出的《處理投訴政策》拒絕進行或決定終止由投訴引發的調查之決定而作出的上訴；
- 九宗涉及私隱專員在作出調查後不送達執行通知的決定；
- 一宗涉及私隱專員在作出調查後送達執行通知的決定；
- 四宗涉及私隱專員不接納相關個案為《私隱條例》第37條下的「投訴」的決定；及
- 餘下的六宗個案涉及不就《私隱條例》第64條所訂罪行進行指明調查的決定。

Nature of AAB Cases Received and Provisions of the PDPO Involved

A total of 43 appeals were received during the reporting year. Among which:

- 23 of these were related to appeals against the Privacy Commissioner's decisions to refuse to carry out or terminate investigations initiated by complaints under sections 39(1) and/or (2) of the PDPO and in accordance with the Complaint Handling Policy issued by the PCPD;
- Nine appeals were against the Privacy Commissioner's decisions not to serve Enforcement Notices after investigations;
- One appeal was against the Privacy Commissioner's decision to serve an Enforcement Notice after investigation;
- Four appeals were against the Privacy Commissioner's decisions not to accept the relevant case as a "complaint" under section 37 of the PDPO; and
- The remaining six appeals were against the Privacy Commissioner's decisions not to carry out specified investigations into alleged offences under section 64 of the PDPO.

上述 43 宗上訴個案中，具體涉及以下指稱（圖4.6）：

The particulars of the 43 appeal cases involved the following allegations (Figure 4.6):

- | | |
|---------------------------|---|
| ■ 違反保障資料原則：20宗 | ■ Contraventions of DPPs: 20 cases |
| ■ 不遵從查閱資料要求：八宗 | ■ Non-compliance with data access requests: eight cases |
| ■ 個案未構成在未獲同意下披露個人資料的罪行：六宗 | ■ Not constituting offences for disclosing personal data without consent: six cases |
| ■ 不接納個案為投訴：四宗 | ■ Not accepted as a complaint: four cases |
| ■ 為依從查閱資料要求而徵收的費用：兩宗 | ■ Imposition of fees for complying with data access requests: two cases |
| ■ 在未獲同意下披露個人資料的罪行：兩宗 | ■ Offences for disclosing personal data without consent: two cases |
| ■ 不遵從改正資料要求：一宗 | ■ Non-compliance with data correction requests: one case |

總數 Total:
43宗 Cases

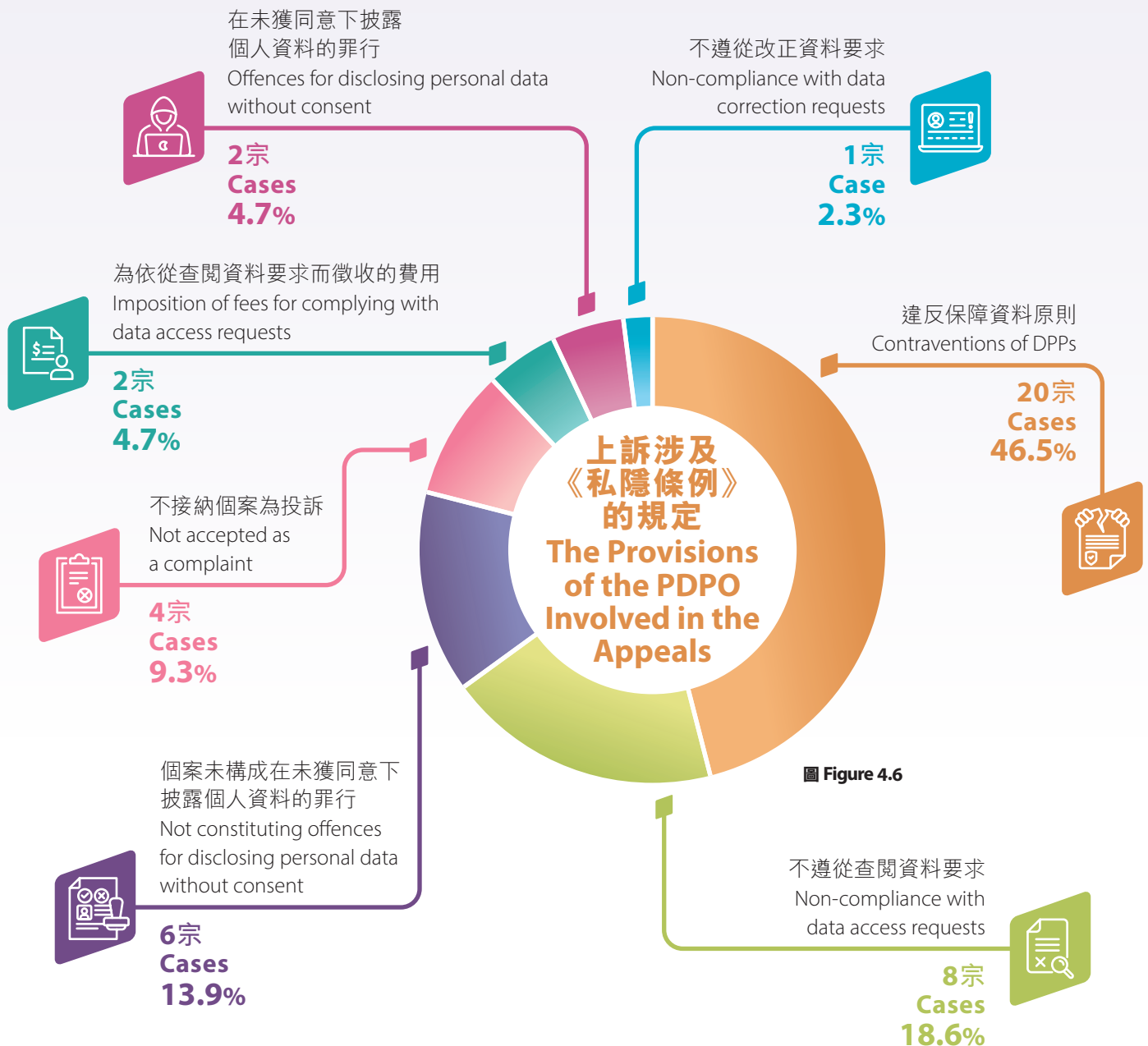


圖 Figure 4.6

而43宗接獲的上訴個案當中，牽涉的保障資料原則的分類如下(單一個案或會牽涉多於一項保障資料原則)(圖4.7)：

Of the 43 appeal cases received, the distribution of DPPs concerned is as follows (one appeal might involve more than one DPP) (Figure 4.7):

■ 第1原則(收集資料原則)：九宗

■ DPP 1 (Data Collection Principle): nine cases

■ 第2原則(資料準確及保留原則)：七宗

■ DPP 2 (Data Accuracy and Retention Principle): seven cases

■ 第3原則(使用資料原則)：13宗

■ DPP 3 (Data Use Principle): 13 cases

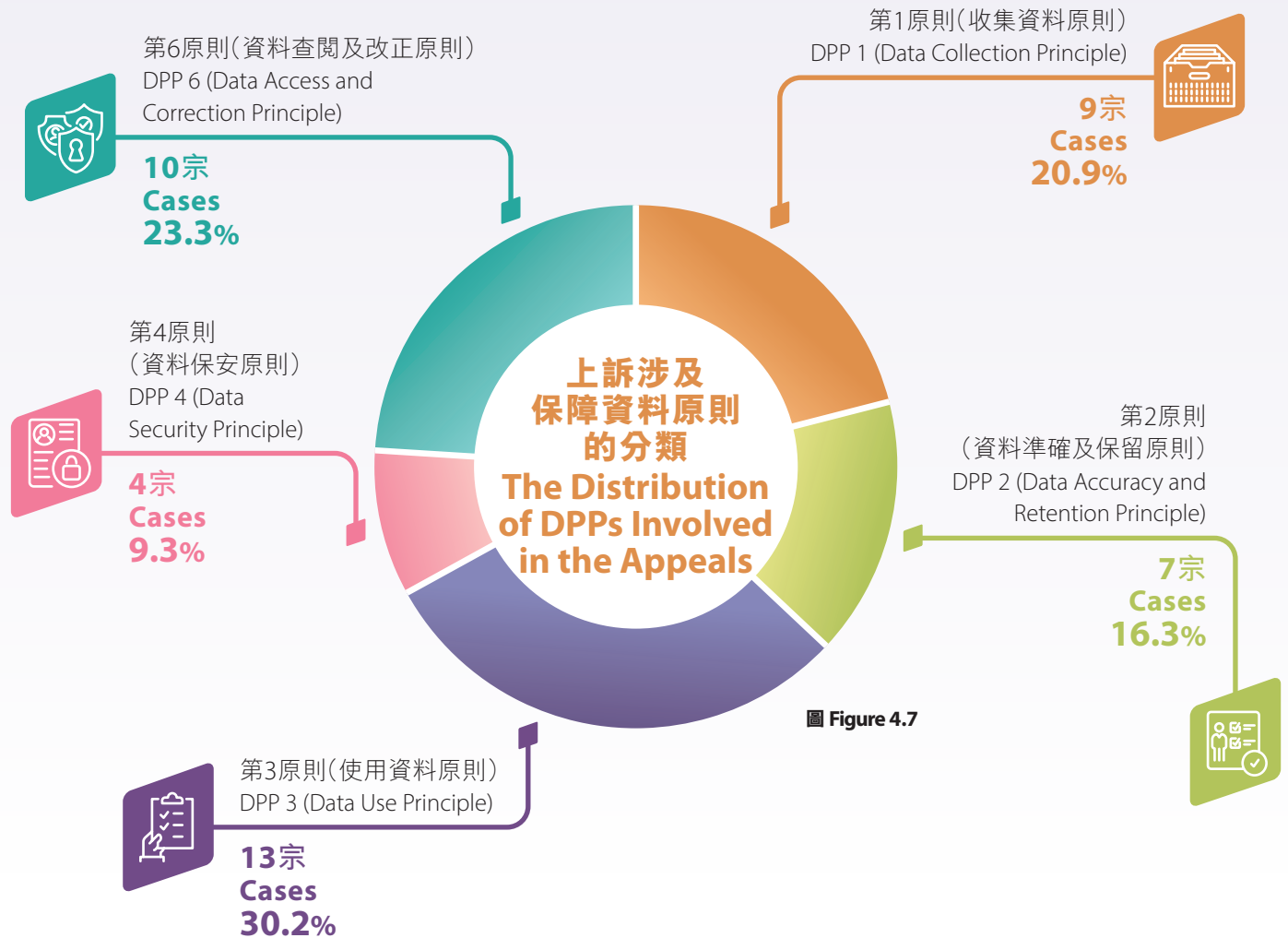
■ 第4原則(資料保安原則)：四宗

■ DPP 4 (Data Security Principle): four cases

■ 第6原則(資料查閱及改正原則)：10宗

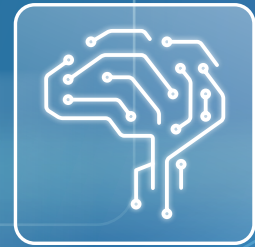
■ DPP 6 (Data Access and Correction Principle): 10 cases

總數 Total:
43宗 Cases*



* 單一個案或會牽涉多於一項保障資料原則。

* One appeal might involve more than one DPP.



宣傳與教育

Promotion and Education



與不同界別聯繫

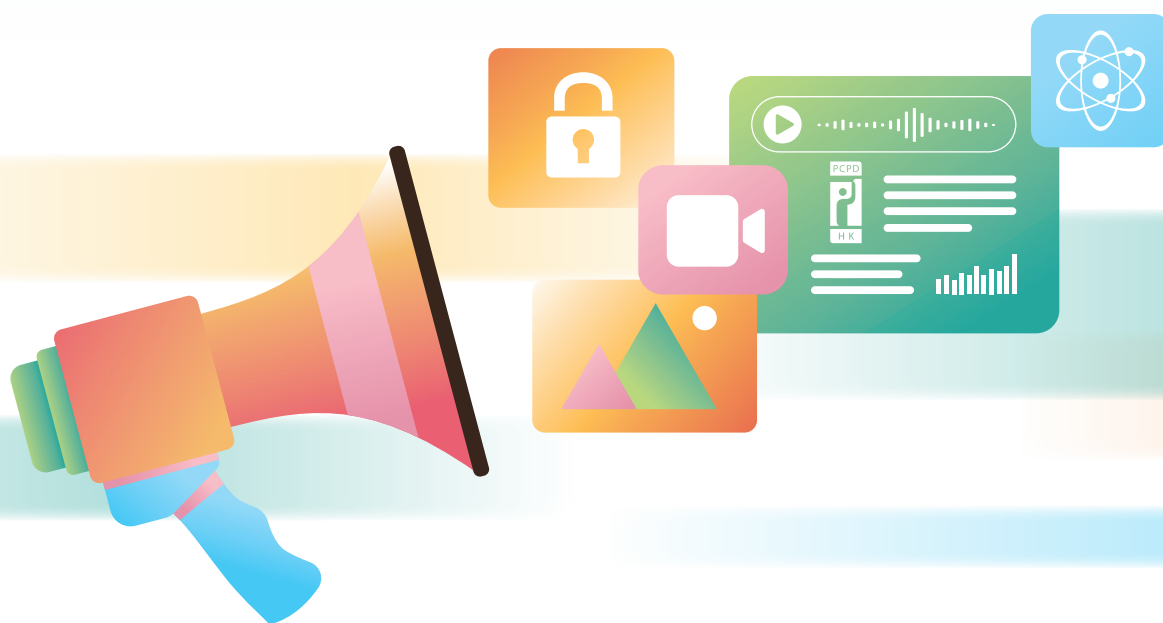
私隱專員公署於報告年度內繼續積極拓展全面的宣傳與教育活動，藉此加強社會各界對保障個人資料私隱的意識。憑藉多管齊下的推廣、教育及媒體活動，公署成功聯繫不同界別，促使他們進一步認識及理解保護和尊重個人資料私隱的重要性。

私隱專員公署持續不懈推動社會各界遵守《私隱條例》，制定多項適合不同持份者的宣傳活動、講座、會議和培訓課程。面對多樣化的私隱挑戰，公署亦積極透過發布指引、新聞稿和文章、接受訪問和回應傳媒查詢，以及在社交媒體平台宣傳等多種渠道回應社會關注，堅定履行其使命。

Engagement with Different Sectors

The PCPD has continued to actively expand its comprehensive promotional and educational activities during the reporting year, with a view to enhancing awareness of personal data privacy protection across various sectors of the community. Thanks to a multi-faceted approach that encapsulates promotion, education, and media outreach, the PCPD has successfully engaged different sectors, enabling them to deepen their understanding of the importance of protecting and respecting personal data privacy.

The PCPD remained a dedicated advocate for compliance with the PDPO across all sectors, with a slew of promotional activities, seminars, conferences, and training sessions tailored for different stakeholders. In the face of evolving privacy challenges, the PCPD also actively responded to societal concerns through multiple channels, including issuing guidelines, media statements and articles, attending interviews and responding to media enquiries, and promoting through social media platforms, to steadfastly fulfil its mission.



於報告年度內，私隱專員公署舉辦的各項活動共錄得 57,900 人次參加，充份展現公署在瞬息萬變的數碼新時代中，積極推動保障個人資料私隱所取得的顯著成效。

During the reporting year, the PCPD's activities recorded 57,900 attendances, clearly demonstrating the significant achievements made in promoting the protection of personal data privacy in the ever-changing digital era.



出版新書“Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)” (香港個人資料(私隱)法例的符規實務指南(第三版))

為響應2024國家網絡安全宣傳周，私隱專員公署聯同香港城市大學出版社出版英文新書“Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”(香港個人資料(私隱)法例的符規實務指南(第三版))，並於2024年9月舉行新書發布會。

The Publication of “Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”

In support of 2024 China Cybersecurity Week, the PCPD collaborated with the City University of Hong Kong Press to publish the third edition of “Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance”. A book launch was held in September 2024.



新書除了全面介紹及解釋《私隱條例》的規定及保障資料原則，亦涵蓋私隱專員公署就遵從《私隱條例》條文進行的監管和執法工作。新版本新增了三個章節，剖析打擊「起底」的新條文、從香港跨境轉移個人資料，以及內地的個人信息保護相關規定。

The new book provides a comprehensive overview and explanations of the requirements and data protection principles under the PDPO, and encompasses an account of the supervision and enforcement work carried out by the PCPD pursuant to provisions of the PDPO. Three new chapters are added in this new edition, namely, the anti-doxxing regime, cross-border transfers of personal data from Hong Kong, and the Mainland's personal information protection regime.

針對不同行業的保障私隱活動

於報告年度內，私隱專員公署共舉辦或參與30項涵蓋會計、教育、金融、人力資源、資訊科技、保險、法律、醫護、物業管理及社會服務等多個行業的保障個人資料私隱的宣傳及教育活動，吸引超過11,000名相關行業的人士參加。公署透過與不同夥伴機構合作，有效地向相關從業者分享保障個人資料的重要訊息，協助業界建立保障和尊重個人資料私隱的文化。有關夥伴機構

Industry-specific Privacy Campaigns

During the reporting year, the PCPD organised or participated in 30 industry-specific promotional and educational events in relation to personal data privacy protection, covering sectors such as accounting, education, finance, human resources, information technology, insurance, legal, medical and healthcare, property management, and social services. These events attracted over 11,000 participants from the relevant industries. Through collaborations with various partner organisations, the PCPD effectively spread the message of personal data protection to practitioners of respective industries, with a view to fostering a culture of protecting



包括：香港城市大學、數字政策辦公室、教育局、Google Developer Group Cloud Hong Kong、香港應用科技研究院、香港網絡安全事故協調中心、香港電腦學會、香港互聯網註冊管理有限公司、香港投資基金公會、香港金融管理局、香港警務處、香港生產力促進局、醫院管理局、全球元治理公會、保險業監管局、勞工處、私人財富管理公會、香港校董學會、香港銀行公會、香港社會服務聯會、香港保險業聯會、香港銀行學會、香港會計師公會、香港科技大學、香港華人會計師公會及香港大學。

and respecting personal data privacy in these sectors. These partner organisations included City University of Hong Kong, Digital Policy Office, Education Bureau, Google Developer Group Cloud Hong Kong, Hong Kong Applied Science and Technology Research Institute, Hong Kong Computer Emergency Response Team Coordination Centre, Hong Kong Computer Society, Hong Kong Internet Registration Corporation Limited (HKIRC), Hong Kong Investment Funds Association, Hong Kong Monetary Authority, Hong Kong Police Force, Hong Kong Productivity Council, Hospital Authority, Institute of Global Metagovernors, Insurance Authority, Labour Department, Private Wealth Management Association, The Hong Kong Academy of School Managers, The Hong Kong Association of Banks, The Hong Kong Council of Social Service, The Hong Kong Federation of Insurers, The Hong Kong Institute of Bankers, The Hong Kong Institute of Certified Public Accountants, The Hong Kong University of Science and Technology, The Society of Chinese Accountants and Auditors and The University of Hong Kong.



專題演講及講座

針對大眾關注的個人資料私隱議題，私隱專員公署於報告年度內舉辦多場專題研討會，涵蓋人工智能(AI)安全、數據管治、數據安全、資料外洩事故處理、粵港澳大灣區個人信息跨境流動、提防個人資料詐騙、資料保障與處理查閱資料要求等範疇。此外，公署亦積極參與其他機構舉辦的研討會及講座，向不同界別的人士分享有關個人資料私隱的最新資訊及意見，例如資訊素養、「起底」罪行的相關規定、數據流動及網絡安全等。

Speaking Engagements and Seminars on Topical Issues

In response to public concerns over widely discussed topics relating to personal data privacy, the PCPD organised various topical seminars during the reporting year, including artificial intelligence (AI) security, data governance, data security, data breach handling, cross-boundary flows of personal information within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA), fraud prevention, data protection and handling of data access requests, etc. Additionally, the PCPD also actively participated in seminars and talks organised by other organisations to share with stakeholders up-to-date information and advice on different personal data privacy issues, such as information literacy, the anti-doxxing regime under the PDPO, data flow, and cybersecurity, etc.

問答環節



專業研習班

私隱專員公署舉辦不同範疇的專業研習班，內容涵蓋資料保障法律實務、與《私隱條例》有關的法院及行政上訴委員會案例、個人資料私隱管理系統、查閱資料要求、與直接促銷活動及人力資源管理有關的保障資料私隱措施，以及和物業管理、保險、銀行或金融服務行業有關的保障私隱議題。研習班獲超過30個專業機構及行業協會支持。在報告年度內，公署合共舉辦了27場專業研習班，吸引超過760名專業人士及相關行業的從業員參加。

Professional Workshops

The PCPD organised professional workshops on different aspects, covering topics on data protection law, court cases and Administrative Appeals Board's decisions relating to the PDPO, personal data privacy management programme, data access requests, data protection measures relating to direct marketing activities and human resource management, as well as privacy protection issues specific to property management, insurance, banking and financial services industries. These workshops were supported by more than 30 professional organisations and industry associations. During the reporting year, the PCPD organised a total of 27 professional workshops, attracting over 760 professionals and practitioners in relevant fields.

簡介講座及機構內部培訓

在報告年度內，私隱專員公署積極推動公眾及機構認識《私隱條例》，包括舉辦14場免費講座，向公眾解釋《私隱條例》的相關規定；以及舉辦191場為公私營機構度身訂造的內部培訓講座，講解《私隱條例》的要求，並提升機構的數據安全意識。

Introductory Seminars and In-house Training Programmes

During the reporting year, the PCPD stepped up its efforts to promote understanding of the PDPO among the public and organisations by organising 14 free introductory seminars for the general public to explain the PDPO's provisions, while providing 191 tailor-made in-house training sessions for public and private organisations to elucidate the requirements of the PDPO and promote data security awareness.

與持份者會面

為加深了解各界持份者對保障個人資料私隱的看法，私隱專員公署積極與不同界別的人士和機構聯繫，了解他們關注的私隱議題。公署與不同政府部門、商會、專業團體、組織、機構的代表、保障資料主任聯會會員、長者及青少年等保持溝通，就最新的私隱議題分享見解及互相交流。

Meetings with Stakeholders

To gain a better understanding of the perspectives of various stakeholders on personal data privacy protection, the PCPD strived to engage with individuals and bodies from different sectors to understand their concerns over privacy issues. The PCPD communicated with representatives from government departments, chambers of commerce, professional bodies, associations, organisations, members of the Data Protection Officers' Club, as well as elderly and youth groups, to share insights and exchange views on the latest privacy issues.



保障資料主任聯會

私隱專員公署於2000年成立保障資料主任聯會(聯會)，為公私營機構的保障資料人員提供具成效的培訓和經驗交流平台，讓他們獲取有關私隱領域的最新資訊，促進個人資料私隱符規。截至2025年3月底，聯會會員人數超過450名。

Data Protection Officers' Club

The PCPD established the Data Protection Officers' Club (DPOC) in 2000, providing an effective training and experience sharing platform for data protection practitioners in both public and private sectors to access the latest information in the privacy landscape and drive data privacy compliance. As at the end of March 2025, there are over 450 DPOC members.



保障資料主任聯會
**DATA
PROTECTION
OFFICERS'
CLUB**

在報告年度內，私隱專員公署為聯會會員舉辦了多場專題講座，當中包括企業使用AI的經驗分享會，邀請行業代表向會員分享如何以私隱友善的方式開發、採購及使用AI的實踐經驗。另外，公署亦舉辦了以粵港澳大灣區個人信息跨境流動為題的講座，協助會員了解《私隱條例》下有關從香港跨境轉移個人資料的法規要求。

During the reporting year, the PCPD organised multiple topical seminars for DPOC members, including a sharing session on the use of AI by enterprises, where an industry representative was invited to share his practical experiences in developing, procuring and using AI in a privacy-friendly manner. Additionally, the PCPD also held a seminar on the cross-boundary flow of personal information within the GBA, with the aim of helping members understand the regulatory requirements under the PDPO concerning the cross-boundary transfers of personal data from Hong Kong.

媒體拓展及宣傳

新聞稿及傳媒查詢

在報告年度內，私隱專員公署共發布了62篇新聞稿，並回覆了225宗傳媒查詢。傳媒關注議題包括多宗個人資料外洩事故、數據安全、使用生成式AI為個人資料私隱帶來的挑戰、公署的執法行動、「起底」個案和數間公司結束營業而影響客戶的個人資料私隱，以及預防個人資料詐騙等。

Media Outreach and Publicity

Media Statements and Enquiries

During the reporting year, the PCPD issued 62 media statements and responded to 225 media enquiries. Topics of media concern included multiple personal data breach incidents, data security, challenges to personal data privacy brought by the use of generative AI, the PCPD's enforcement actions, cases of doxxing and business closure that affected customers' personal data privacy, and prevention of personal data fraud, etc.



記者會、訪問、在報章及行業或專業刊物的文章

私隱專員公署分別於2024年4至6月、9至12月及2025年1月及3月舉行了九場記者會，讓傳媒及公眾人士了解公署的工作。記者會涵蓋公署2024年工作報告、發表七個調查結果、「香港企業網絡保安準備指數及AI安全風險」調查報告和推出學校、非牟利機構及中小企「數據安全」套餐、發布《人工智能（AI）：個人資料保障模範框架》（《模範框架》）和《僱員使用生成式AI的指引清單》，以及《私隱條例》下打擊「起底」行為的條文生效三年以來的成效。

Media Briefings, Interviews and Articles in Newspapers and Industry or Professional Journals

The PCPD organised nine media briefings from April to June, and September to December 2024, as well as in January and March 2025 respectively, allowing the media and members of the public to better understand the PCPD's work. The media briefings covered the PCPD's work report for the year 2024, the release of seven investigation findings, the "Hong Kong Enterprise Cyber Security Readiness Index and AI Security" survey report, and the launch of the "Data Security" Package for schools, non-profit-making organisations, and small and medium-sized enterprises, the publication of the "Artificial Intelligence: Model Personal Data Protection Framework" (Model Framework) and the "Checklist on Guidelines for the Use of Generative AI by Employees", as well as a summary of the three-year enforcement work since the commencement of the provisions criminalising doxxing acts under the PDPO.





另外，私隱專員及其團隊就多個有關私隱的議題接受了49次電視、電台及報章訪問，內容涵蓋《模範框架》、多宗資料外洩事故的調查結果、《數碼時代的私隱保障：實測十個網上旅遊平台收集個人資料的情況》報告等多個主題。

私隱專員亦在報章及行業或專業刊物上發表文章，以回應時下備受關注的私隱議題並提供建議，包括《模範框架》、數據安全、粵港澳大灣區個人信息跨境流動。

In addition, the Privacy Commissioner and her team conducted 49 television, radio and newspaper interviews on various privacy-related topics, including the Model Framework, the investigation findings of various data breach incidents, and the report on “Privacy Protection in the Digital Age: A Study of the Collection of Personal Data by 10 Online Travel Platforms”, etc.

The Privacy Commissioner also published articles in newspapers and industry or professional journals to address and advise on topical privacy issues, such as the Model Framework, data security, and cross-boundary flows of personal information within the GBA.

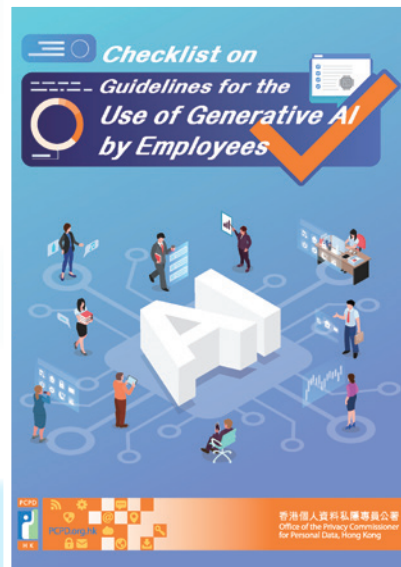
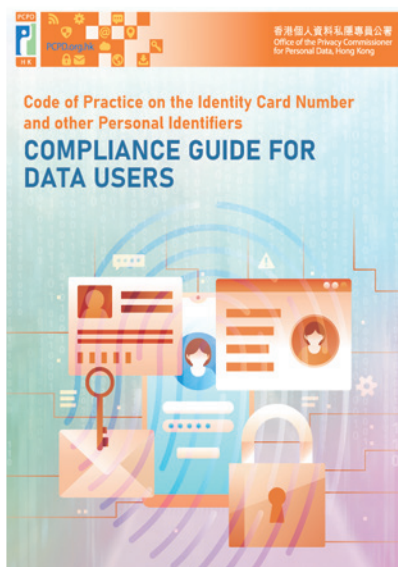
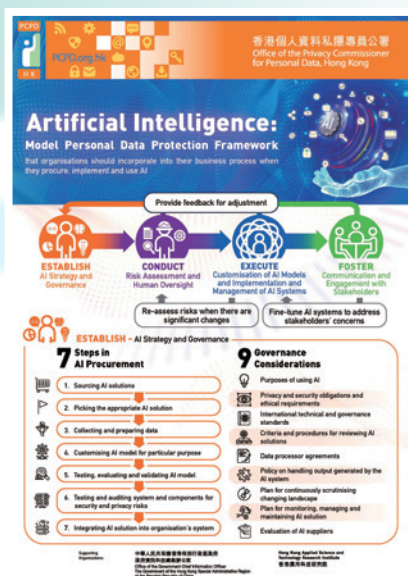


宣傳及教育刊物

在報告年度內，除了出版新書“Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”（香港個人資料(私隱)法例的符規實務指南(第三版)）外，私隱專員公署亦就不同熱門議題編製多份刊物，為持份者提供實用指引及合規建議，當中包括《人工智能(AI)：個人資料保障模範框架》及其單張、新版《身份證號碼及其他身份代號實務守則：資料使用者指引》及《身份證號碼與你的私隱》資料單張、《數碼時代的私隱保障：實測十個網上旅遊平台收集個人資料的情況》報告、《求職者就披露刑事紀錄須知》資料單張、《雲端運算指引》，以及《僱員使用生成式AI的指引清單》。

Publicity and Educational Materials

During the reporting year, alongside the publication of the new book “Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”, the PCPD also published a number of publications on various hot topics, providing stakeholders with practical guidelines and compliance advice. The publications included the “Artificial Intelligence: Model Personal Data Protection Framework” and its leaflet, new versions of the “Code of Practice on the Identity Card Number and other Personal Identifiers: Compliance Guide for Data Users” and an information leaflet titled “Your Identity Card Number and Your Privacy”, a report on “Privacy Protection in the Digital Age: A Study of the Collection of Personal Data by 10 Online Travel Platforms”, an information leaflet on “Note for Job Applicants on Disclosure of Criminal Records”, as well as the guidance on “Cloud Computing” and “Checklist on Guidelines for the Use of Generative AI by Employees”.

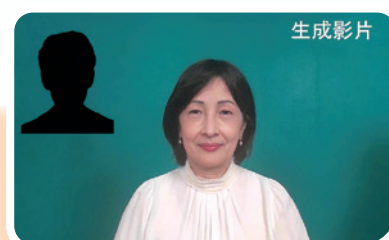


製作「貼地」的宣傳及教育短片

為了加深機構及公眾對《私隱條例》的理解及掌握保障個人資料私隱的最新資訊，私隱專員公署於報告年度內就不同主題製作了多段宣傳及教育短片。其中一條短片展示了私隱專員在社交媒體平台親身示範透過深度偽造技術實時換臉，提醒市民在AI時代有相、有片也未必有真相。公署亦為新書“Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”製作兩段短片，簡介近年私隱法的發展。

Creating Down-to-earth Promotional and Educational Videos

To promote a better understanding of the PDPO and access to the latest information on personal data privacy protection among organisations and members of the public, the PCPD produced a series of promotional and educational videos on various topics during the reporting year. One of the videos features the Privacy Commissioner in a real-time demonstration of face-swapping using deepfake technology on social media platforms, reminding the public that appearances and videos can be deceptive in the age of AI. Furthermore, two videos were produced to introduce the latest developments in privacy law, in conjunction with the publication of “Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance (Third Edition)”.



此外，為協助機構提高員工對網絡安全及保障個人資料的意識，私隱專員公署與香港互聯網註冊管理有限公司合作推出一連三集的宣傳短片，以輕鬆的手法為機構提供相關指引及貼士。公署亦將專題講座及記者會的錄影片段上載至公署網站，讓公眾及機構可隨時重溫有關內容。

In addition, to assist organisations in raising their employees' awareness of cybersecurity and personal data protection, the PCPD collaborated with the HKIRC to launch a promotional video trilogy to provide relevant guidance and tips in a lively manner to organisations. Recordings of thematic seminars and media briefings are available on the PCPD's website, allowing the public and organisations to access and review the content at any time.

網站及社交媒體平台

私隱專員公署透過網站傳遞有關公署的工作、保障個人資料私隱及其最新發展的資訊，效果顯著。在報告年度內，公署的網站錄得超過4,135,300瀏覽人次，較上一個報告年度大幅增加了60%。

為了更貼近公眾，私隱專員公署定期更新其社交媒體平台，以淺白的文字和插圖講解個人資料私隱保障的資訊。在報告年度內，公署在社交媒體平台上共發表671篇帖文，涵蓋不同的個人資料私隱議題，又以數據安全吉祥物「數據保寶」推出一系列數據安全懶人包，提供在密碼管理、使用社交媒體及智能電話時保障個人資料私隱的實用貼士。

Website and Social Media Platforms

The PCPD effectively disseminates information about its work, personal data privacy protection, and the latest developments through its website. During the reporting year, the dedicated website garnered over 4,135,300 visits, representing a substantial 60% increase compared to the previous reporting year.

To level up public engagement, the PCPD regularly updates its social media platforms, using straightforward language and illustrations to elucidate personal data privacy protection. Throughout the reporting year, the PCPD published 671 posts on social media platforms, covering a wide range of personal data privacy topics. The PCPD also introduced a series of data security “info-packs” featuring the data security mascot “Data Guardian”, offering practical tips on personal data privacy protection in areas of password management, social media usage and smartphone security.



青少年教育

保障私隱學生大使・學校夥伴嘉許計劃2024

為向青少年推廣尊重及保障個人資料私隱的重要訊息，私隱專員公署舉辦「保障私隱學生大使・學校夥伴嘉許計劃」(嘉許計劃)，共有 67 間中學成為「學校夥伴」，與公署攜手宣揚反「起底」的訊息，包括舉辦相關的教育講座、播放教育影片及派發宣傳刊物等，合共吸引超過 17,000 名學生參與。

Youth Education

Student Ambassador for Privacy Protection Programme – Partnering Schools Recognition Scheme 2024

To promote the importance of respecting and protecting personal data privacy among the youth, the PCPD organised the “Student Ambassador for Privacy Protection Programme – Partnering Schools Recognition Scheme 2024” (Student Ambassador Programme). A total of 67 secondary schools became “Partnering Schools”, joining hands with the PCPD in disseminating anti-doxxing messages by organising educational talks, broadcasting educational videos and distributing promotional materials, with a total of more than 17,000 students participated in the activities.



嘉許計劃亦包括「AI新世代保障私隱領袖培訓計劃」(領袖培訓計劃)，讓參加學生透過AI專題講座及互動體驗工作坊等活動，學習個人資料私隱管理系統的重要性，以及認識符合《私隱條例》規定的AI應用標準。活動獲得教育局、科技和教育界的機構支持。計劃的嘉許典禮於2024年11月圓滿舉行，並邀得政制及內地事務局局長曾國衛先生, GBS, IDSM, JP擔任主禮嘉賓。

The Student Ambassador Programme also featured the “Future Leaders of AI and Privacy Protection Training Programme” (Future Leaders Programme), which enabled participating students to learn the importance of personal data privacy management programmes and AI application standards that comply with the PDPO through activities such as a topical seminar and an AI practical workshop. The Future Leaders Programme was organised under the auspices of the Education Bureau and organisations from technological and educational sectors. The Student Ambassador Programme culminated in a recognition ceremony in November 2024, officiated by the Secretary for Constitutional and Mainland Affairs, Mr Erick TSANG Kwok-wai, GBS, IDSM, JP.



反「起底」學校教育巡迴講座

為提高中學生在使用社交媒體時保護個人資料的意識，以及培養他們向網絡欺凌及「起底」說「不」的正確態度，私隱專員公署持續舉辦反「起底」學校教育巡迴講座，透過到校講座的形式向中學生推廣相關資訊。在報告年度內，公署人員曾到訪 32 間中學，向約 9,300 名學生宣揚反「起底」訊息。

School Touring of Anti-doxxing Education Talks

With a view to enhancing secondary school students' awareness of personal data protection when using social media and nurturing their correct attitude to say "No" to cyberbullying and "doxxing", the PCPD continued to organise the School Touring of Anti-doxxing Education Talks to promote the messages among students. During the reporting year, representatives from the PCPD visited 32 schools to promote the anti-doxxing message to around 9,300 students.



內地及國際聯繫

Mainland and International Connections



與內地聯繫

積極與內地機構聯繫及加強協作

香港與國家的發展環環相扣。為推動香港進一步融入國家發展大局，及協助香港充分發揮「一國兩制」下「背靠祖國、聯通世界」的獨特優勢，私隱專員公署一直積極促進及參與與內地機構的協作及交流。

例如，為配合政府推動數字經濟的發展方向，私隱專員公署一直致力與粵港澳大灣區（大灣區）的相關機構加強交流。數據跨境流動是推動「數字灣區」發展的重要動力，而數據流通亦有助香港發展成為數據中心。因此，積極促進與內地機構緊密聯繫及合作是公署的重點工作之一。

Connections with the Mainland

Active Liaison and Stronger Collaboration with Mainland Organisations

The development dynamics of Hong Kong and the Country are closely intertwined. To facilitate Hong Kong's further integration into the overall development of the Country, and to assist Hong Kong in fully capitalising on its distinctive advantages of being able to enjoy the strong support of the Motherland while being closely connected to the world under the "One Country, Two Systems" principle, the PCPD has been actively facilitating and participating in collaboration and exchanges with Mainland organisations.

For example, to dovetail with the Government's policy initiative in advancing the development of digital economy, the PCPD has been actively engaging in communications with relevant organisations in the Guangdong-Hong Kong-Macao Greater Bay Area (GBA). Cross-boundary data flow is an important driving force for the "Digital Bay Area", and the flows of data is conducive to the development of Hong Kong as a data centre. One of the important tasks of the PCPD, thus, is to actively facilitate close liaison and cooperation with Mainland organisations.



2024年國家網絡安全宣傳周

「2024年國家網絡安全宣傳周」(宣傳周)於2024年9月在廣東省南沙舉行。期間，內地、香港及澳門特別行政區同時舉辦各項活動。私隱專員帶領私隱專員公署代表積極參與宣傳周的各項活動。

當中，私隱專員公署時任署理高級律師黃寶漫女士於2024年9月10日出席在廣東省南沙舉行的「粵港澳大灣區數據跨境流動合作閉門會」，並在會上發表演講，闡述《粵港澳大灣區(內地、香港)個人信息跨境流動標準合同》的便利措施。是次會議為大灣區政府部門領導、法律專業人士、業界人士及學者提供平台，讓與會者就促進大灣區數據跨境流動的議題進行深入討論及廣泛交流。

2024世界互聯網大會

私隱專員公署署理助理個人資料私隱專員(法律)賴皓茵女士於2024年11月21日出席在浙江省烏鎮舉行的2024世界互聯網大會「深化數據跨境流動合作，推動全球數字經濟發展」分論壇，與內地的監管機構代表、專家及學者就數據跨境流動國際合作、合規等範疇進行深度交流，以了解更多有關內地建立和推動數字經濟的最新發展。

2024 China Cybersecurity Week

The “2024 China Cybersecurity Week” (Cybersecurity Week) was held in Nansha, Guangdong Province in September 2024. Various activities were held concurrently in the Mainland and the Special Administrative Regions of Hong Kong and Macao during the Cybersecurity Week. The Privacy Commissioner led the representatives of the PCPD to actively participate in various activities of the Cybersecurity Week.

Among the activities, the then Acting Senior Legal Counsel of the PCPD, Ms Clemence WONG, attended the “Closed Meeting on Cooperation in the Cross-boundary Data Flow Within the GBA” held in Nansha, Guangdong Province, on 10 September 2024 and gave a speech to elucidate the facilitation measures relating to the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong). The meeting acted as a platform for government leaders, legal professionals, practitioners and scholars in the GBA to engage in extensive discussions and exchange insights on promoting cross-boundary data flows within the GBA.

2024 World Internet Conference

Acting Assistant Privacy Commissioner for Personal Data (Legal) of the PCPD, Ms Fiona LAI, attended a sub-forum on “Deepening Collaboration on Cross-border Data Flows and Promoting the Development of Global Digital Economy” at the 2024 World Internet Conference held in Wuzhen, Zhejiang Province, on 21 November 2024, where she exchanged views with representatives of the Mainland regulatory authorities, experts and scholars on issues relating to international collaboration and regulatory compliance in cross-border data flows, with a view to further understanding the Mainland’s latest advancement in establishing and promoting digital economy.

全球及地區性私隱保障網絡

在現今高度互聯互通及數碼化的世界，人工智能(AI)等科技的發展日新月異，對私隱保障構成前所未見的複雜挑戰。數據無分國界，唯有各地通力合作才能解決這些問題。

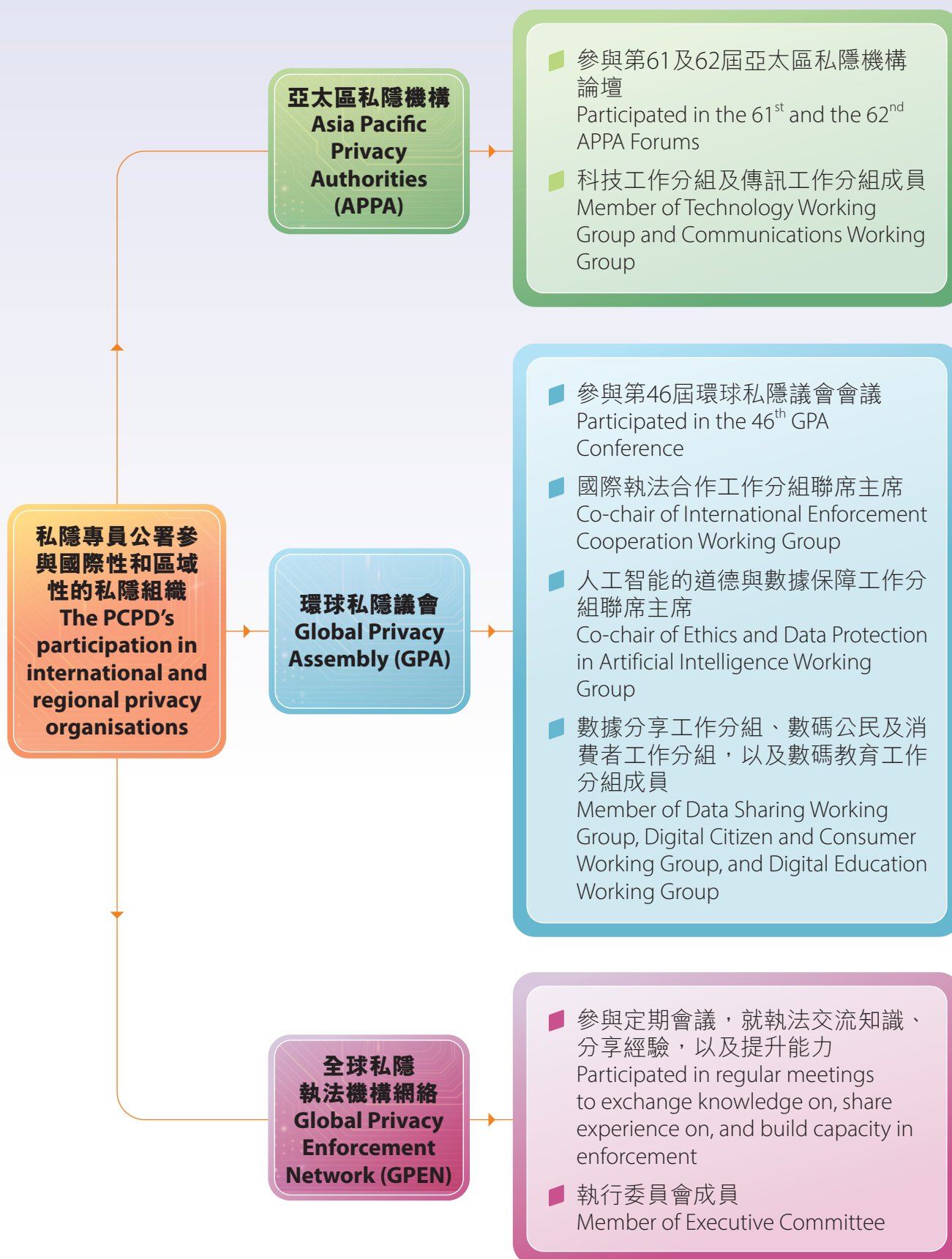
本報告年度內，私隱專員公署一直積極參與多個國際性及區域性的私隱保障平台，並定期與世界各地的私隱或資料保障機構交換見解和經驗。透過與國際社群交流所得的專業知識及與其他監管機構的緊密合作，公署致力在不斷轉變的數碼世界中保障個人資料私隱。

Global and Regional Privacy Protection Networks

In today's highly connected and digitalised world, the rapid advancement of technologies, such as artificial intelligence (AI), has brought about increasingly complex privacy protection challenges than ever before. With data knowing no borders, addressing these issues requires coordinated global efforts.

During the reporting year, the PCPD remained actively engaged in numerous privacy platforms at both international and regional levels, and regularly exchanged insights and experiences with fellow privacy or data protection authorities worldwide. By leveraging expertise from the international community and fostering closer collaboration with other regulators, the PCPD is committed to safeguarding personal data privacy in the ever-changing digital landscape.





亞太區私隱機構

亞太區私隱機構於1992年成立，是亞太區內20個私隱或資料保障機構加強合作、討論最佳行事常規，以及分享有關私隱規例和新興科技資訊的主要平台。

Asia Pacific Privacy Authorities

The Asia Pacific Privacy Authorities (APPA), formed in 1992, is the principal forum for 20 privacy or data protection authorities in the Asia Pacific region to strengthen cooperation, discuss best practices and share information on privacy regulations and emerging technologies.



第61屆亞太區私隱機構論壇

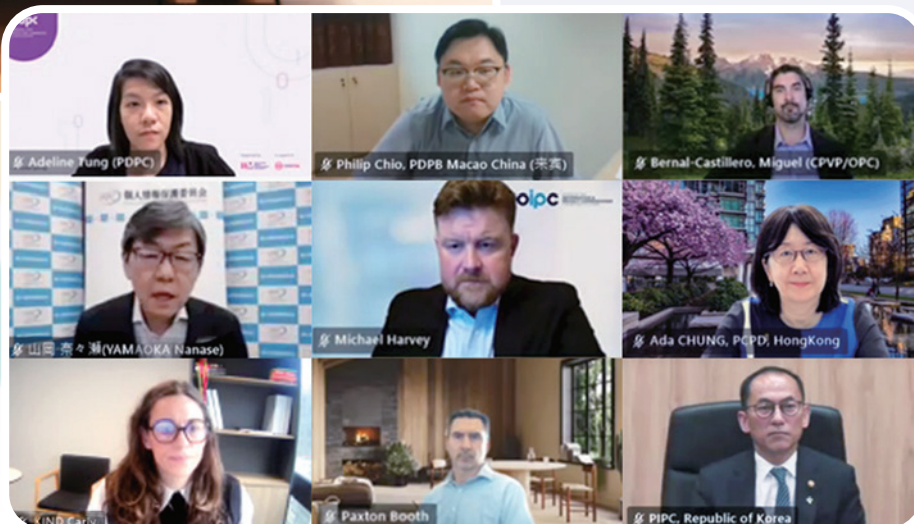
私隱專員與私隱專員公署代表於2024年6月20至21日出席以視像模式舉行的第61屆亞太區私隱機構論壇。論壇的重點討論事項如下：

- AI治理的政策及相關新猷；
- 調查及執法；
- 資料外洩事故通報的處理；
- 私隱強化科技；及
- 兒童私隱。

61st APPA Forum

The Privacy Commissioner and representatives of the PCPD attended the 61st APPA Forum held virtually between 20 and 21 June 2024. Major themes discussed at the forum included:

- AI governance policies and initiatives;
- Investigations and enforcements;
- Handling data breach incident reports;
- Privacy enhancing technologies; and
- Children's privacy.



論壇中，私隱專員介紹了私隱專員公署於2024年6月發布的《人工智能（AI）：個人資料保障模範框架》（《模範框架》）。私隱專員向亞太區私隱機構成員解釋，《模範框架》建基於一般業務流程，旨在提供國際認可及切實可行的建議和最佳行事常規，以協助機構在採購、實施及使用AI，包括生成式AI時，遵從《私隱條例》的相關規定。

At the forum, the Privacy Commissioner gave an overview of the “Artificial Intelligence: Model Personal Data Protection Framework” (Model Framework) issued by the PCPD in June 2024. The Privacy Commissioner explained to APPA members that the Model Framework, premised on general business procedures, aimed at providing internationally recognised and practical recommendations and best practices to assist organisations in procuring, implementing and using AI, including generative AI, in compliance with the relevant requirements of the PDPO.

第62屆亞太區私隱機構論壇

私隱專員連同私隱專員公署代表於2024年11月26至27日在日本東京出席第62屆亞太區私隱機構論壇。論壇的重點討論事項如下：

- AI及新興科技的管治；
- 執法及立法進展；
- 培訓及提高意識的活動；
- 跨境資料轉移；及
- 保障兒童私隱。

在論壇上，私隱專員參與題為「亞太區人工智能及新興科技的治理：觀點與措施」的專題討論，與來自日本、韓國、新加坡及美國的監管機構代表及學者探討AI治理與保障個人資料私隱的相互關係。

私隱專員亦分別與意大利、日本、韓國及新加坡的監管機構的專員或高級人員代表進行雙邊會談，探討不同的資料保障議題以及合作範圍，加強在個人資料私隱方面的國際合作。

62nd APPA Forum

The Privacy Commissioner and representatives of the PCPD attended the 62nd APPA Forum between 26 and 27 November 2024 in Tokyo, Japan. Major themes discussed at the forum included:

- Governance of AI and emerging technologies;
- Enforcement and legislative developments;
- Training and awareness raising activities;
- Cross-border data transfers; and
- Protecting children's privacy.

At the forum, the Privacy Commissioner participated in a panel discussion titled "Governance of AI and Emerging Technologies in the Asia Pacific Region: Perspectives and Initiatives" alongside regulators and academics from Japan, Korea, Singapore, and the United States of America, where the panellists explored the interplay between governance of AI and protection of personal data privacy.

The Privacy Commissioner also held bilateral meetings with Commissioners or senior representatives from regulators in Italy, Japan, Korea and Singapore respectively, during which the parties discussed various data protection issues and explored opportunities for collaboration with a view to reinforcing international cooperation in the field of personal data privacy.



環球私隱議會

環球私隱議會（前身為國際資料保障及私隱專員會議）是一個具領導地位的國際平台，集合全球超過130個私隱或資料保障機構，就私隱議題和最新國際發展進行討論和交流意見。

Global Privacy Assembly

The Global Privacy Assembly (GPA), formerly known as the International Conference of Data Protection and Privacy Commissioners, is the leading international forum where over 130 privacy or data protection authorities from across the globe are convened to discuss and exchange views on privacy issues and the latest international developments.



第46屆環球私隱議會會議

私隱專員及私隱專員公署代表於2024年10月28日至11月1日出席第46屆環球私隱議會。會議於澤西以視像及實體的混合模式舉行，會上討論了AI、網絡安全、兒童教育、跨境資料轉移，以及監管機構合作等私隱議題。

46th GPA Conference

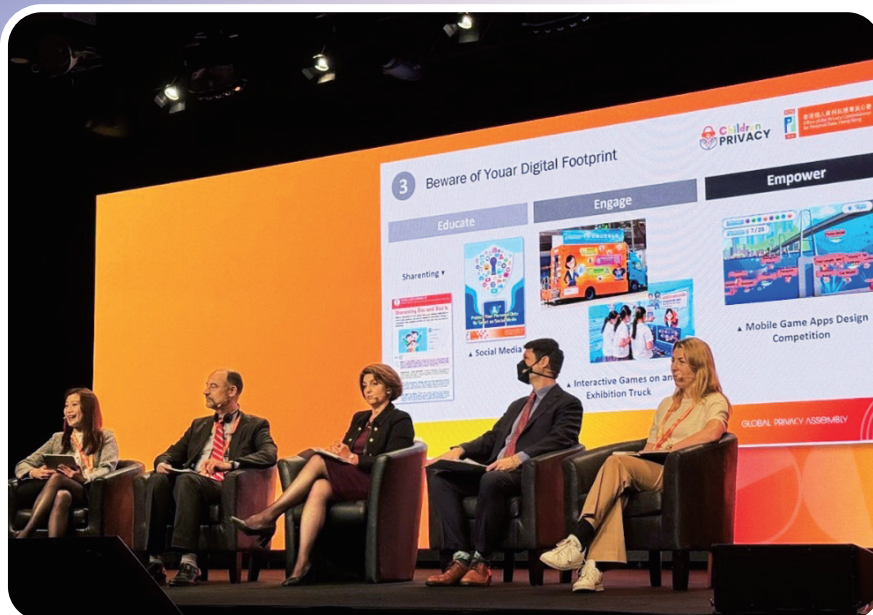
The Privacy Commissioner and representatives of the PCPD attended the 46th GPA Conference from 28 October to 1 November 2024. The hybrid conference, which was held in Jersey, featured discussions on privacy issues relating to AI, cybersecurity, children education, cross-border data transfers, regulatory cooperation and more.

在公開環節上，私隱專員公署時任助理個人資料私隱專員（企業傳訊及合規）黎智敏女士在專題研討會上以「教育從根本開始：私隱教育對社會的影響」為題發言，講述公署以積極主動的態度，透過出版物、舉辦講座及比賽等一系列活動，推廣香港兒童的私隱教育。其中一個值得留意的例子是公署於2024年5月約一連兩星期安排流動展覽車「保障私隱號」穿梭全港不同的地區，以生動有趣的方式，透過互動小遊戲，讓參觀人士加深認識保障個人資料私隱及數據安全的重要性。

在閉門會議中，由私隱專員公署擔任聯席主席的環球私隱議會國際執法合作工作分組向大會提交年度報告。工作分組於年內的重點工作包括舉辦多個閉門會議，以促進各地私隱或資料保障機構就不同執法議題分享資訊和進行協作。

In the open session, the then Assistant Privacy Commissioner for Personal Data (Corporate Communications and Compliance) of the PCPD, Ms Joyce LAI, spoke at a panel titled “Education from the Ground up: The Societal Impact of Privacy Education”, where she discussed the PCPD’s proactive approach in promoting privacy education for children in Hong Kong through an array of initiatives such as publications, seminars, competitions and more. One notable example among them is the “Privacy Protection Truck”, a mobile exhibition which toured around the city for around two weeks in May 2024, featuring interactive games to enhance the visitors’ understanding of protecting personal data privacy and data security in a lively and interesting manner.

In the closed session, the GPA’s International Enforcement Cooperation Working Group, co-chaired by the PCPD, presented its annual report to the GPA. Highlights of its work in 2024 included a multitude of closed sessions designed to facilitate information exchange and collaboration among privacy or data protection authorities on various enforcement issues.



環球私隱議會人工智能的道德與數據保障工作分組聯席主席

為了在與AI有關的全球倡議及合作方面發揮更具戰略性的作用，私隱專員公署自2024年10月起，與歐洲聯盟、法國及韓國的私隱或資料保障機構一同擔任環球私隱議會人工智能的道德與數據保障工作分組的聯席主席。

人工智能的道德與數據保障工作分組是環球私隱議會的一個恆常分組，為各成員提供一個制定策略的平台，以促進在AI領域尊重資料保障和道德原則，並推動這方面的國際協作成果。

Co-chairmanship at the GPA's Ethics and Data Protection in Artificial Intelligence Working Group

With a view to playing a more strategic role in global initiatives and collaboration on AI, the PCPD took the initiative to serve as the co-chair of the GPA's Ethics and Data Protection in Artificial Intelligence Working Group (AIWG), alongside privacy or data protection authorities of the European Union, France and Korea since October 2024.

Established as a permanent working group of the GPA, the AIWG serves as a platform for members to develop strategies in promoting respect for data protection and ethical principles in the context of AI, and to foster concerted efforts in this field on international level.



全球私隱執法機構網絡

全球私隱執法機構網絡於2010年成立，由超過80個成員組成，旨在促進私隱執法機構的跨境合作。於本報告年度，私隱專員公署繼續擔任全球私隱執法機構網絡的執行委員會成員，協助統籌網絡的活動。公署亦參與定期會議，與其他成員交流知識並討論執法議題。

Global Privacy Enforcement Network

Founded in 2010 and currently consisting of over 80 members, the Global Privacy Enforcement Network (GPEN) aims to facilitate cross-border cooperation among privacy enforcement authorities. During the reporting year, the PCPD continued to hold a membership in the Executive Committee of the GPEN, helping to steer the overall activities of the network. The PCPD also took part in regular meetings to exchange knowledge and discuss enforcement issues with other members.



Global Privacy Enforcement Network

「誘導性設計模式」環球聯合報告

2024年初，私隱專員公署與全球25個私隱或資料保障執法機構（包括澳洲、加拿大、日本、澳門、新加坡、英國、美國等）及27個消費者保障機構共同進行全球性保障私隱抽查行動（抽查行動）。抽查行動以「誘導性設計模式」為題，為全球私隱執法機構網絡和國際消費者保障執法網絡發起的共同行動。

Global Joint Report on “Deceptive Design Patterns”

In early 2024, the PCPD joined hands with 25 privacy or data protection enforcement authorities (including those from Australia, Canada, Japan, Macao, Singapore, the United Kingdom, the United States of America, and more) and 27 consumer protection authorities worldwide to conduct a global privacy protection sweep (Sweep), which was coordinated jointly by the GPEN and the International Consumer Protection and Enforcement Network under the theme of “Deceptive Design Patterns”.

參與機構在抽查行動期間檢視了來自多個行業（包括零售、健康和健身、旅行和住宿，以及社交媒體和約會）的1,000多個網站和流動應用程式，以了解這些平台使用誘導性設計模式的慣性及種類。抽查行動結果的報告於2024年7月發表。

During the Sweep, participating authorities examined more than 1,000 websites and mobile applications across various industries (including retail, health and fitness, travel and accommodation, and social media and dating) to gauge the frequency and types of deceptive design patterns used by these platforms. A report summarising the findings of the Sweep was released in July 2024.



網絡安全實踐社群

穩健的數據安全措施對於保障個人資料免遭未獲准許的查閱及濫用至關重要，因此網絡安全對保障個人資料私隱具有關鍵作用。就此，環球私隱議會與全球私隱執法機構網絡攜手設立國際性的「網絡安全實踐社群」。該社群旨在匯集就網絡安全進行監管及執法的私隱或資料保障監管機構的專家。自網絡安全實踐社群設立以來，私隱專員公署代表積極參與定期會議，以了解網絡安全方面的最新趨勢，並與其他業界人士交流知識。

Cybersecurity Community of Practice

Cybersecurity plays a pivotal role in safeguarding personal data privacy, as robust data security measures are crucial to personal data protection against unauthorised access and misuse. In this regard, the international "Cybersecurity Community of Practice" (CoP) was jointly established by the GPA and the GPEN to bring together experts in cybersecurity regulation and enforcement from privacy or data protection authorities. Since the inception of the CoP, representatives of the PCPD have actively participated in regular meetings to keep abreast of the latest trends in cybersecurity and to exchange knowledge with fellow practitioners.

財務報表

Financial Statements



獨立核數師報告 Independent Auditor's Report

致：個人資料私隱專員

(依據《個人資料(私隱)條例》在香港成立的
單一法團)

意見

本核數師(以下簡稱「我們」)已審核列載於第152至177頁**個人資料私隱專員**的財務報表，此財務報表包括於2025年3月31日的財務狀況表與截至該日止年度的全面收益表、資金變動表及現金流量表，以及財務報表附註(包括重要會計政策信息)。

我們認為，該等財務報表已根據香港會計師公會發出的《香港財務報告準則會計準則》真實而公平地反映個人資料私隱專員於2025年3月31日的財務狀況及截至該日止年度的財務表現及現金流量。

意見基準

我們已根據香港會計師公會頒佈的《香港核數準則》進行審核。我們於該等準則下的責任已於本報告的「核數師就審核財務報表須承擔的責任」一節進一步闡述。我們根據香港會計師公會制定的《專業會計師職業道德守則》(「守則」)獨立於個人資料私隱專員，我們亦已根據守則達致我們的其他道德責任。我們認為我們所獲得的審核憑證屬充足及適當以為我們的意見提供基準。

TO: THE PRIVACY COMMISSIONER FOR PERSONAL DATA

(A CORPORATION SOLE IN HONG KONG ESTABLISHED UNDER THE PERSONAL DATA (PRIVACY) ORDINANCE)

Opinion

We have audited the financial statements of **The Privacy Commissioner for Personal Data** (the "PCPD") set out on pages 152 to 177, which comprise the statement of financial position as at 31 March 2025, and the statement of comprehensive income, statement of changes in funds and statement of cash flows for the year then ended, and notes to the financial statements, including material accounting policy information.

In our opinion, the financial statements give a true and fair view of the financial position of the PCPD as at 31 March 2025, and of its financial performance and its cash flows for the year then ended in accordance with HKFRS Accounting Standards ("HKFRSs") issued by the Hong Kong Institute of Certified Public Accountants ("HKICPA").

Basis for Opinion

We conducted our audit in accordance with Hong Kong Standards on Auditing ("HKSAs") issued by the HKICPA. Our responsibilities under those standards are further described in the auditor's responsibilities for the audit of the financial statements section of our report. We are independent of the PCPD in accordance with the HKICPA's Code of Ethics for Professional Accountants ("the Code"), and we have fulfilled our other ethical responsibilities in accordance with the Code. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

財務報表及其核數師報告以外的資料

個人資料私隱專員負責編製其他資料。其他資料包括年報所載的資料，但不包括財務報表及我們就此的核數師報告。

我們有關財務報表的意見並不涵蓋其他資料，我們並不會就此發表任何形式的核證結論。

就我們對財務報表的審核而言，我們的責任是閱讀其他資料，從而考慮其他資料是否與財務報表或我們在審核過程中獲悉的資料存在重大不符，或存在重大錯誤陳述。如我們基於已完成的工作認為其他資料出現重大錯誤陳述，我們須報告此一事實。我們就此並無報告事項。

個人資料私隱專員及管治層就財務報表須承擔的責任

個人資料私隱專員須負責根據香港會計師公會頒佈的《香港財務報告準則會計準則》編製真實而公平的財務報表，及落實其認為編製財務報表所必要的內部控制，以使財務報表不存在由於欺詐或錯誤而導致的重大錯誤陳述。

在編製財務報表時，個人資料私隱專員須負責評估其持續經營的能力，並披露與持續經營有關的事項（如適用）。除非個人資料私隱專員有意清盤，或停止營運，或除此之外並無其他實際可行的辦法，否則個人資料私隱專員須採用以持續經營為基礎的會計法。

管治層須負責監督個人資料私隱專員的財務報告流程。

Information other than the Financial Statements and Auditor's Report thereon

The Privacy Commissioner is responsible for the other information. The other information comprises the information included in the annual report, but does not include the financial statements and our auditor's report thereon.

Our opinion on the financial statements does not cover the other information and we do not express any form of assurance conclusion thereon.

In connection with our audit of the financial statements, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit or otherwise appears to be materially misstated. If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Responsibilities of the Privacy Commissioner and those Charged with Governance for the Financial Statements

The Privacy Commissioner is responsible for the preparation of the financial statements that give a true and fair view in accordance with HKFRSs issued by the HKICPA, and for such internal control as the Privacy Commissioner determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Privacy Commissioner is responsible for assessing the PCPD's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the Privacy Commissioner either intends to liquidate the PCPD or to cease operations, or has no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the PCPD's financial reporting process.

核數師就審核財務報表須承擔的責任

我們的目標，是對整體財務報表是否不存在由於欺詐或錯誤而導致的重大錯誤陳述取得合理保證，並作出包括我們意見的核數師報告。本報告是根據協定的委聘條款僅向個人資料私隱專員作出，除此之外別無其他目的。我們不會就本報告的內容向任何其他人士負上或承擔任何責任。合理保證是高水平的保證，但不能保證按照《香港核數準則》進行的審核在某一重大錯誤陳述存在時總能發現。錯誤陳述可以由欺詐或錯誤引起，如合理預期它們個別或匯總起來可能影響財務報表的使用者所作出的經濟決定，則有關的錯誤陳述可被視作重大。

我們根據《香港核數準則》進行審核的工作之一，是運用專業判斷，在整個審核過程中抱持專業懷疑態度。我們亦：

- 識別和評估由於欺詐或錯誤而導致財務報表存在重大錯誤陳述的風險，設計及執行審核程序以應對該等風險，以及取得充足和適當的審核憑證，作為我們意見的基礎。由於欺詐可能涉及串謀、偽造、蓄意遺漏、虛假陳述，或凌駕於內部控制之上，因此未能發現因欺詐而導致的重大錯誤陳述的風險高於因錯誤而導致的重大錯誤陳述的風險。
- 了解與審核相關的內部控制，以設計適當的審核程序，但目的並非對個人資料私隱專員內部控制的效能發表意見。
- 評價個人資料私隱專員所採用會計政策的恰當性及所作出會計估計和相關披露資料的合理性。

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. This report is made solely to you, as a body, in accordance with the agreed terms of engagement, and for no other purposes. We do not assume responsibility towards or accept liability to any other person for the contents of this report. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with HKSA's will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with HKSA's, we exercise professional judgment and maintain professional skepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the PCPD's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Privacy Commissioner.

對個人資料私隱專員採用持續經營會計基礎的恰當性作出結論。根據所得的審核憑證，決定是否存在與事件或情況有關的重大不確定性，而可能對個人資料私隱專員持續經營的能力構成重大疑慮。如我們認為存在重大不確定性，則有必要在核數師報告中提請使用者對財務報表中的相關披露資料的關注。如有關的披露資料不足，則修訂我們的意見。我們的結論是基於截至核數師報告日期所取得的審核憑證。然而，未來事件或情況可能導致個人資料私隱專員不能繼續持續經營。

評價財務報表(包括披露資料)的整體列報方式、結構及內容，以及財務報表是否公允反映有關交易和事項。

Conclude on the appropriateness of the Privacy Commissioner's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the PCPD's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the PCPD to cease to continue as a going concern.

Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

我們與管治層就不同事項進行溝通，當中包括計劃的審核範圍、時間安排、重大審核發現，包括我們在審核期間識別出內部控制的任何重大缺陷。

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

黃龍德會計師事務所有限公司

執業會計師

曾卓鋒
FCPA (Practising), ACA, MSCA
香港執業資深會計師

執業證書號碼：P06369

香港，2025年7月31日

PATRICK WONG C.P.A. LIMITED

Certified Public Accountants

TSANG CHEUK FUNG ANDY
FCPA (Practising), ACA, MSCA
Certified Public Accountant (Practising), Hong Kong

Practising Certificate Number: P06369

Hong Kong, 31 July 2025

全面收益表 Statement of Comprehensive Income

截至2025年3月31日止年度 YEAR ENDED 31 MARCH 2025

		附註 Notes	2025 \$	2024 \$
收入	Income			
政府補助金	Government subventions	5	103,555,665	99,382,291
政府專案資助金	Government project funds	13	12,663,265	–
銀行利息	Bank interest		1,452,939	1,545,784
講座收費	Seminar fees		1,560,960	1,649,060
會員費	Membership fees		122,800	93,600
「防疫抗疫基金」下創造 職位計劃的財務資助	Financial assistance under Job Creation Scheme of Anti-epidemic Fund		–	1,210,207
雜項收入	Miscellaneous income		7,943	108,661
			119,363,572	103,989,603
支出	Expenditure			
核數師酬金	Auditor's remuneration		57,000	56,000
行政費用	Administrative expenses		2,325,991	2,007,106
顧問服務	Consultancy services		380,000	385,000
物業、機器及設備的折舊	Depreciation of property, plant and equipment			
– 由資本補助金支付	– financed by capital subvention fund	9	236,150	287,071
– 由其他資金來源支付	– financed by other sources of funds	9	8,638,910	9,005,764
僱員薪俸	Staff emoluments	6	94,414,400	81,323,667
辦公室的營運租賃租金	Operating lease rentals in respect of office premises		306,926	292,860
海外訪問／會議支出	Overseas visit/conference		250,425	469,713
宣傳推廣及教育支出	Promotion and education expenses		5,436,192	5,035,289
法律協助計劃	Legal assistance scheme		58,530	36,530
處置物業、機器及設備 的損失	Loss on disposal of property, plant and equipment		26,690	–
其他營運費用	Other operating expenses		6,252,539	6,312,503
租賃負債利息	Interest on lease liabilities	18	734,007	226,192
			119,117,760	105,437,695
年內盈餘／(虧損)及 全面收益／(虧損)總額	Surplus/(deficit) and total comprehensive income/(loss) for the year		245,812	(1,448,092)

第156至177頁的附註屬本財務報表的組成部分。

The notes on pages 156 to 177 are an integral part of these financial statements.

財務狀況表 Statement of Financial Position

於2025年3月31日 AT 31 MARCH 2025

		附註 Notes	2025 \$	2024 \$
非流動資產	Non-current asset			
物業、機器及設備	Property, plant and equipment	9	15,532,128	21,961,536
流動資產	Current assets			
應收款項、按金及預付款項	Accounts receivable, deposits and prepayments		1,453,659	1,505,853
銀行結存及現金	Bank balances and cash	10	79,915,718	44,023,819
			81,369,377	45,529,672
流動負債	Current liabilities			
應付款項及應計費用	Accounts payable and accruals		242,996	180,049
職員約滿酬金撥備	Provision for staff gratuity	11	5,378,866	4,805,529
未放取年假撥備	Provision for unutilised annual leave		1,347,306	1,245,973
預收政府補助金	Government subvention received in advance	12	13,497,959	9,740,217
預收政府專案資助金	Government project funds received in advance	13	30,100,735	—
資本補助金	Capital subvention fund	16	83,137	—
租賃負債	Lease liabilities	14, 18	7,824,824	6,868,997
			58,475,823	22,840,765
流動資產淨值	Net current assets		22,893,554	22,688,907
資產總額減流動負債	Total assets less current liabilities		38,425,682	44,650,443
非流動負債	Non-current liabilities			
政府的約滿酬金補助款	Government subvention for gratuity	15	3,693,527	3,990,784
職員約滿酬金撥備	Provision for staff gratuity	11	2,199,572	1,804,453
資本補助金	Capital subvention fund	16	—	319,287
租賃負債	Lease liabilities	14, 18	6,768,050	13,017,198
			12,661,149	19,131,722
資產淨值	Net assets		25,764,533	25,518,721
資金	Funds			
一般儲備	General reserve	17	25,764,533	25,518,721

本財務報表已於2025年7月31日獲私隱專員批准及授權刊發

Approved and authorised for issue by the Privacy Commissioner on 31 July 2025.

鍾麗玲, SBS

香港個人資料私隱專員

Ada CHUNG Lai-ling, SBS

Privacy Commissioner for Personal Data, Hong Kong

第156至177頁的附註屬本財務報表的組成部分。

The notes on pages 156 to 177 are an integral part of these financial statements.

資金變動表 Statement of Changes In Funds

截至2025年3月31日止年度 YEAR ENDED 31 MARCH 2025

		全面收益表 Statement of comprehensive income \$	一般儲備 General reserve \$	總計 Total \$
於2023年4月1日的結餘	Balance at 1 April 2023	–	30,385,007	30,385,007
年內虧損及 全面虧損總額	Deficit and total comprehensive loss for the year	(1,448,092)	–	(1,448,092)
調撥	Transfer	1,448,092	(1,448,092)	–
政府收回上年盈餘	Previous year's surplus recovered by Government	–	(3,418,194)	(3,418,194)
於2024年3月31日及 2024年4月1日的結餘	Balances at 31 March 2024 and at 1 April 2024	–	25,518,721	25,518,721
年內盈餘及 全面收益總額	Surplus and total comprehensive income for the year	245,812	–	245,812
調撥	Transfer	(245,812)	245,812	–
於2025年3月31日的結餘	Balance at 31 March 2025	–	25,764,533	25,764,533

第156至177頁的附註屬本財務報表的組成部分。

The notes on pages 156 to 177 are an integral part of these financial statements.

現金流量表 Statement of Cash Flows

截至 2025年3月31日止年度 YEAR ENDED 31 MARCH 2025

	附註 Notes	2025 \$	2024 \$
營運活動	Operating activities		
年內盈餘／(虧損)	Surplus/(deficit) for the year	245,812	(1,448,092)
調整：	Adjustments for:		
– 折舊支出	– Depreciation expense	8,875,060	9,292,835
– 處置物業、機器及設備的虧損／(收入)	– Loss/(gain) on disposal of property, plant and equipment	26,690	(8,000)
– 利息收入	– Interest income	(1,452,939)	(1,545,784)
– 租賃負債利息	– Interest on lease liabilities	734,007	226,192
– 政府收回上年盈餘	– Previous year's surplus recovered by Government	–	(3,418,194)
營運資本變動前的營運盈餘	Operating surplus before working capital changes	8,428,630	3,098,957
應收款項、按金及預付款項(增加)／減少	(Increase)/decrease in accounts receivable, deposits and prepayments	(44,613)	1,001,158
應付款項及應計費用增加／(減少)	Increase/(decrease) in accounts payable and accruals	62,947	(395,544)
職員約滿酬金撥備增加	Increase in provision for staff gratuity	968,456	937,962
未放取年假撥備增加／(減少)	Increase/(decrease) in provision for unutilised annual leave	101,333	(163,526)
預收政府補助金增加	Increase in government subvention received in advance	3,757,742	1,564,624
預收政府專案資助金增加	Increase in government project funds received in advance	30,100,735	–
政府的約滿酬金補助款減少	Decrease in government subvention for gratuity	(297,257)	(96,194)
資本補助金減少	Decrease in capital subvention fund	(236,150)	(287,071)
營運活動所得現金淨額	Net cash generated from operating activities	42,841,823	5,660,366
投資活動	Investing activities		
收取利息	Interest received	1,549,746	1,598,902
三個月以上之短期銀行存款減少	Decrease in short-term bank deposits with maturity more than three months	–	9,069,954
購置物業、機器及設備的付款	Payments for property, plant and equipment	(459,884)	(331,715)
處置物業、機器及設備的得益	Proceeds from disposals of property, plant and equipment	–	8,000
投資活動所得現金淨額	Net cash from investing activities	1,089,862	10,345,141
融資活動	Financing activities		
已付租賃負債本金	Capital element of lease rentals paid	18 (7,305,779)	(7,839,401)
已付租賃負債利息	Interest element of lease rentals paid	18 (734,007)	(226,192)
融資活動所用現金淨額	Net cash used in financing activities	(8,039,786)	(8,065,593)
現金及現金等值的增加	Net increase in cash and cash equivalents	35,891,899	7,939,914
年初的現金及現金等值	Cash and cash equivalents at the beginning of year	44,023,819	36,083,905
年底的現金及現金等值	Cash and cash equivalents at the end of year	79,915,718	44,023,819
現金及現金等值結存分析	Analysis of balances of cash and cash equivalents		
銀行結存及現金	Bank balances and cash	10 79,915,718	44,023,819
年底的現金及現金等值	Cash and cash equivalents at the end of the year	79,915,718	44,023,819

第156至177頁的附註屬本財務報表的組成部分。

The notes on pages 156 to 177 are an integral part of these financial statements.

財務報表附註 Notes to The Financial Statements

2025年3月31日 31 MARCH 2025

1. 一般資料

個人資料私隱專員是根據1995年8月3日制定的《個人資料(私隱)條例》而於香港設立的單一法團，目的是要在個人資料方面保障個人的私隱，並就附帶及相關事宜訂定條文。註冊辦事處地址為香港灣仔皇后大道東248號大新金融中心12樓。

2. 遵從《香港財務報告準則會計準則》的聲明

個人資料私隱專員的財務報表是按照香港會計師公會頒佈的所有適用的《香港財務報告準則會計準則》(包含所有適用的個別《香港財務報告準則會計準則》、《香港會計準則》和詮釋)以及香港公認會計原則的規定編製。重要會計政策信息概要載列於附註3。

3. 重要會計政策信息

(a) 財務報表的編製基準

編製本財務報表時是以歷史成本作為計量基礎。

(b) 物業、機器及設備

物業、機器及設備於財務狀況表按成本扣除累積折舊和其後的減值虧損(如有)列帳。

折舊是以直線法在以下估計可使用年期内沖銷其成本(已扣除剩餘價值)而予以確認：

擁有資產

汽車	3年
電腦及軟件	3年
辦公室設備	5年
家具及固定裝置	5年
租賃物業裝修工程	3年

1. General Information

The Privacy Commissioner for Personal Data (the "PCPD") is a corporation sole established in Hong Kong under the Personal Data (Privacy) Ordinance 1995 enacted on 3 August 1995 for the purpose of protecting the privacy of individuals in relation to personal data and to provide for matters incidental thereto or connected therewith. The address of its registered office is 12/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong.

2. Statement of Compliance with HKFRS Accounting Standards

The PCPD's financial statements have been prepared in accordance with all applicable HKFRS Accounting Standards ("HKFRSs"), which includes all applicable individual HKFRSs, Hong Kong Accounting Standards ("HKASs") and Interpretations issued by the Hong Kong Institute of Certified Public Accountants ("HKICPA") and accounting principles generally accepted in Hong Kong. A summary of material accounting policy information is set out in note 3.

3. Material Accounting Policy Information

(a) Basis of Preparation of the Financial Statements

The measurement basis used in preparing the financial statements is historical cost.

(b) Property, Plant and Equipment

Property, plant and equipment are stated in the statement of financial position at cost less accumulated depreciation and subsequent impairment losses, if any.

Depreciation is recognised so as to write off the cost of assets less their residual values over their estimated useful lives, using the straight-line method, as follows:

Owned Assets

Motor vehicle	3 years
Computers and software	3 years
Office equipment	5 years
Furniture and fixtures	5 years
Leasehold improvements	3 years

3. 重要會計政策信息(續)

(b) 物業、機器及設備(續)

使用權資產

租賃土地及樓宇 按租賃期

估計可使用年期、剩餘價值及折舊方法會於各報告期末檢討，而任何估計變動的影響以預期基準列帳。

物業、機器及設備項目於出售或當預期持續使用該資產不再帶來未來經濟利益時終止確認。出售或廢棄物業、機器及設備項目產生之任何收益或虧損按出售所得款項與資產帳面值間之差額計算，並於全面收益表內確認。

(c) 確認及終止確認金融工具

金融資產及金融負債於個人資料私隱專員成為工具合約條文的訂約方時，於財務狀況表確認。

當從資產收取現金流量的合約權利屆滿；個人資料私隱專員實質上轉移資產擁有權的所有風險及回報；或個人資料私隱專員沒有實質上轉移或保留資產擁有權的所有風險及回報但亦無保留資產的控制權時，金融資產會被終止確認。在終止確認金融資產時，資產帳面值與已收代價之差額於損益確認。

當有關合約的特定責任獲解除、取消或屆滿時，金融負債會被終止確認。終止確認的金融負債帳面值與已付代價之差額於損益確認。

3. Material Accounting Policy Information (Continued)

(b) Property, Plant and Equipment (Continued)

Right-of-use Asset

Leasehold land and building Over the lease term

The estimated useful lives, residual values and depreciation method are reviewed at the end of each reporting period, with the effect of any changes in estimate accounted for on a prospective basis.

An item of property, plant and equipment is derecognised upon disposal or when no future economic benefits are expected to arise from the continued use of the asset. Any gain or loss arising on the disposal or retirement of an item of property, plant and equipment is determined as the difference between the sales proceeds and the carrying amount of the asset and is recognised in the statement of comprehensive income.

(c) Recognition and Derecognition of Financial Instruments

Financial assets and financial liabilities are recognised in the statement of financial position when the PCPD becomes a party to the contractual provisions of the instruments.

Financial assets are derecognised when the contractual rights to receive cash flows from the assets expire; the PCPD transfers substantially all the risks and rewards of ownership of the assets; or the PCPD neither transfers nor retains substantially all the risks and rewards of ownership of the assets but has not retained control on the assets. On derecognition of a financial asset, the difference between the assets' carrying amount and the sum of the consideration received is recognised in profit or loss.

Financial liabilities are derecognised when the obligation specified in the relevant contract is discharged, cancelled or expired. The difference between the carrying amount of the financial liability derecognised and the consideration paid is recognised in profit or loss.

3. 重要會計政策信息(續)

(d) 金融資產

金融資產按交易日基準確認及終止確認(其中金融資產的買賣所根據的合約條款規定須於有關市場設定的時限內交付金融資產)，並初步按公平值加直接應佔交易成本計量，惟按公平值計入損益的投資則除外。收購按公平值計入損益的投資之直接應佔交易成本即時於損益確認。

按攤銷成本計量的金融資產

撥歸此類的金融資產(包括貿易及其他應收款項)須同時符合下列兩項條件：

- 持有資產的業務模式是以收取合約現金流量為目標；及
- 資產的合約條款於特定日期產生僅為支付本金及未償還本金利息的現金流量。

按攤銷成本計量的金融資產其後以實際利率方式按攤銷成本減預期信貸虧損的虧損撥備計算。

3. Material Accounting Policy Information (Continued)

(d) Financial Assets

Financial assets are recognised and derecognised on a trade date basis where the purchase or sale of an asset is under a contract whose terms require delivery of the asset within the timeframe established by the market concerned, and are initially measured at fair value, plus directly attributable transaction costs except in the case of investments at fair value through profit or loss. Transaction costs directly attributable to the acquisition of investments at fair value through profit or loss are recognised immediately in profit or loss.

Financial Assets at Amortised Cost

Financial assets (including trade and other receivables) are classified under this category if they satisfy both of the following conditions:

- the assets are held within a business model whose objective is to hold assets in order to collect contractual cash flows; and
- the contractual terms of the assets give rise on specified dates to cash flows that are solely payments of principal and interest on the principal amount outstanding.

Financial assets at amortised cost are subsequently measured at amortised cost using the effective interest method less loss allowances for expected credit losses.

3. 重要會計政策信息(續)

(e) 預期信貸虧損的虧損撥備

個人資料私隱專員就按攤銷成本計量的金融資產的預期信貸虧損確認虧損撥備。預期信貸虧損為加權平均信貸虧損，以發生違約風險的金額作為加權數值。

在各報告期末，如金融工具的信貸風險自初始確認以來大幅增加，個人資料私隱專員會就貿易應收款項按金融工具的預計有效期內，所有可能違約事件產生的預期信貸虧損（「全期預期信貸虧損」），計算該金融工具的虧損撥備。

如在報告期末，金融工具（貿易應收款項除外）的信貸風險自初始確認以來並無大幅增加，則個人資料私隱專員會按全期預期信貸虧損的部分，即報告期後12個月內，因可能發生的違約事件而預期產生的虧損，計算該金融工具的虧損撥備。

預期信貸虧損金額或為調整報告期末虧損撥備至所需金額所作撥回金額是於損益確認為減值收益或虧損。

3. Material Accounting Policy Information (Continued)

(e) Loss Allowances for Expected Credit Losses

The PCPD recognises loss allowances for expected credit losses on financial assets at amortised cost. Expected credit losses are the weighted average of credit losses with the respective risks of a default occurring as the weights.

At the end of each reporting period, the PCPD measures the loss allowance for a financial instrument at an amount equal to the expected credit losses that result from all possible default events over the expected life of that financial instrument ("lifetime expected credit losses") for trade receivables, or if the credit risk on that financial instrument has increased significantly since initial recognition.

If, at the end of the reporting period, the credit risk on a financial instrument (other than trade receivables) has not increased significantly since initial recognition, the PCPD measures the loss allowance for that financial instrument at an amount equal to the portion of lifetime expected credit losses that represents the expected credit losses that result from default events on that financial instrument that are possible within 12 months after the reporting period.

The amount of expected credit losses or reversal to adjust the loss allowance at the end of the reporting period to the required amount is recognised in profit or loss as an impairment gain or loss.

3. 重要會計政策信息(續)

(f) 合約資產及合約負債

合約資產於個人資料私隱專員根據合約所載付款條款，於無條件享有該代價前確認收入時確認。合約資產根據附註3(e)所載政策評估預計信貸虧損，並於收取代價權利成為無條件時重新分類至應收款項。合約負債於客戶支付代價或在對代價具有無條件的權利(在此情況下，相應應收款項已確認)時，而在個人資料私隱專員確認相關收入前予以確認。

(g) 租賃

(i) 租賃的定義

倘合約為換取代價而給予在一段時間內控制可識別資產使用的權利，則該合約屬於或包含租賃。

就於首次應用日期或之後訂立或修改或因業務合併而簽訂的合約而言，個人資料私隱專員根據《香港財務報告準則》第16號的定義於開始、修訂日期或收購日期(視何者合適而定)評估該合約是否屬於或包含租賃。除非合約的條款及條件其後出現變動，否則有關合約將不予重新評估。

(ii) 個人資料私隱專員作為承租人 **短期租賃及低價值資產租賃**

個人資料私隱專員將短期租賃確認豁免應用於租期自開始日期起計為期12個月或以下並且不包括購買選擇權的租賃。個人資料私隱專員亦對低價值資產租賃應用確認豁免。短期租賃及低價值資產租賃的租賃付款按直線法於租賃期內確認為開支。

3. Material Accounting Policy Information (Continued)

(f) Contract Assets and Contract Liabilities

A contract asset is recognised when the PCPD recognises revenue before being unconditionally entitled to the consideration under the payment terms set out in the contract. Contract assets are assessed for expected credit losses in accordance with the policy set out in note 3(e) and are reclassified to receivables when the right to the consideration has become unconditional. A contract liability is recognised when the customer pays consideration, or has an unconditional right to consideration (in such case, a corresponding receivable is recognised), before the PCPD recognises the related revenue.

(g) Leases

(i) Definition of a Lease

A contract is, or contains, a lease if the contract conveys the right to control the use of an identified asset for a period of time in exchange for consideration.

For contracts entered into or modified on or after the date of initial application, the PCPD assesses whether a contract is or contains a lease based on the definition under HKFRS 16 at inception or modification date as appropriate. Such contract will not be reassessed unless the terms and conditions of the contract are subsequently changed.

(ii) The PCPD as a Lessee

Short-term Leases and Leases of Low-value Assets

The PCPD applies the short-term lease recognition exemption to leases that have a lease term of 12 months or less from the commencement date and do not contain a purchase option. It also applies the recognition exemption for lease of low-value assets. Lease payments on short-term leases and leases of low-value assets are recognised as expense on a straight-line basis over the lease term.

3. 重要會計政策信息(續)

(g) 租賃(續)

(ii) 個人資料私隱專員作為承租人(續)

使用權資產

使用權資產的成本包括：

- (a) 初始計量租賃負債的金額；
- (b) 於開始日期或之前支付的任何租賃付款減去任何已收的租賃優惠；及
- (c) 個人資料私隱專員產生的任何初始直接成本。

使用權資產按成本減任何累計折舊及減值虧損計量，並就租賃負債的任何重新計量作出調整。

如個人資料私隱專員合理確定會於租賃期限屆滿時取得相關租賃資產擁有權的使用權資產，該資產自開始日期至可使用年期結束計算折舊，否則使用權資產於估計可使用年期與租賃期限兩者的較短者以直線法折舊。

3. Material Accounting Policy Information (Continued)

(g) Leases (Continued)

(ii) The PCPD as a Lessee (Continued)

Right-of-use Assets

The cost of right-of-use asset includes:

- (a) the amount of the initial measurement of the lease liability;
- (b) any lease payments made at or before the commencement date, less any lease incentives received; and
- (c) any initial direct costs incurred by the PCPD.

Right-of-use assets are measured at cost, less any accumulated depreciation and impairment losses, and adjusted for any remeasurement of lease liabilities.

Right-of-use assets in which the PCPD is reasonably certain to obtain ownership of the underlying leased assets at the end of the lease term is depreciated from commencement date to the end of the useful life. Otherwise, right-of-use assets are depreciated on a straight-line basis over the shorter of its estimated useful life and the lease term.

3. 重要會計政策信息(續)

(g) 租賃(續)

(ii) 個人資料私隱專員作為承租人(續)

租賃負債

於租賃開始日期，個人資料私隱專員按該日未支付的租賃付款現值確認及計量租賃負債。計算租賃付款現值時，倘租賃內含的利率難以釐定，則個人資料私隱專員會使用租賃開始日期的遞增借貸利率計算。

租賃付款包括固定付款(包括實質固定付款)減任何應收租賃優惠。

開始日期後，租賃負債是透過利息增長及租賃付款調整。

當出現以下情況，個人資料私隱專員會重新計量租賃負債(並對相關使用權資產作出相應調整)：

- (a) 租賃期已更改或對行使購買選擇權的評估有變，在該情況下，相關租賃負債於重新評估日期透過使用經修訂折現率折現經修訂租賃付款而重新計量。
- (b) 租賃付款因檢討市場租金後市場租金有變而出現變動，在該情況下，相關租賃負債透過使用初始折現率折現經修訂租賃付款而重新計量。

個人資料私隱專員於財務狀況表內將租賃負債呈列為單獨項目。

3. Material Accounting Policy Information (Continued)

(g) Leases (Continued)

(ii) The PCPD as a Lessee (Continued)

Lease Liabilities

At the commencement date of a lease, the PCPD recognises and measures the lease liability at the present value of lease payments that are unpaid at that date. In calculating the present value of lease payments, the PCPD uses the incremental borrowing rate at the lease commencement date if the interest rate implicit in the lease is not readily determinable.

The lease payments include fixed payments (including in-substance fixed payments) less any lease incentives receivable.

After the commencement date, lease liabilities are adjusted by interest accretion and lease payments.

The PCPD remeasures lease liabilities (and makes a corresponding adjustment to the related right-of-use assets) whenever:

- (a) the lease term has changed or there is a change in the assessment of exercise of a purchase option, in which case the related lease liability is remeasured by discounting the revised lease payments using a revised discount rate at the date of reassessment.
- (b) the lease payments change due to changes in market rental rates following a market rent review, in which cases the related lease liability is remeasured by discounting the revised lease payments using the initial discount rate.

The PCPD presents lease liabilities as a separate line item on the statement of financial position.

3. 重要會計政策信息(續)

(h) 現金及現金等值

現金包括銀行及手頭現金。現金等值是短期及高流動性的投資，這些投資可以隨時轉換為已知數額的現金，價值變動的風險不大。

(i) 應付款項

應付款項於初期按公平值確認，其後按攤銷成本列帳，但若短期應付款的折現影響並不重大，則按成本列帳。

(j) 撥備及或然負債

如果個人資料私隱專員須就已發生的事件承擔法律或推定責任，因而預期很可能會導致經濟利益流出，在有關金額能夠可靠地估計時，個人資料私隱專員便會對該時間或金額不確定的負債計提撥備。如果貨幣時間價值重大，則按預計履行責任所需費用的現值計提撥備。

如果經濟利益流出的可能性較低，或是無法對有關金額作出可靠的估計，便會將該責任披露為或然負債，但經濟利益流出的可能性極低則除外。如果個人資料私隱專員的責任須視乎某項或多項未來事件是否發生才能確定是否存在，除非經濟利益流出的可能性極低，該責任亦會被披露為或然負債。

3. Material Accounting Policy Information (Continued)

(h) Cash and Cash Equivalents

Cash comprises cash on hand and at bank. Cash equivalents are short-term, highly liquid investments that are readily convertible to known amounts of cash and which are subject to an insignificant risk of changes in value.

(i) Accounts and Other Payables

Accounts and other payables are initially measured at fair value and, after initial recognition, at amortised cost, except for short-term payables with no stated interest rate and the effect of discounting being immaterial, that are measured at their original invoice amount.

(j) Provisions and Contingent Liabilities

Provisions are recognised for liabilities of uncertain timing or amount when the PCPD has a legal or constructive obligation arising as a result of a past event, it is probable that an outflow of economic benefits will be required to settle the obligation and a reliable estimate can be made. Where the time value of money is material, provisions are stated at the present value of the expenditure expected to settle the obligation.

Where it is not probable that an outflow of economic benefits will be required, or the amount cannot be estimated reliably, the obligation is disclosed as a contingent liability, unless the probability of outflow of economic benefits is remote. Possible obligations, whose existence will only be confirmed by the occurrence or non-occurrence of one or more future events are also disclosed as contingent liabilities unless the probability of outflow of economic benefits is remote.

3. 重要會計政策信息(續)

(k) 收入確認

(i) 政府補助及資助金

如有合理保證可取得政府補助，而且個人資料私隱專員可以符合所有附帶條件，則會按補助金額的公平值確認政府補助。

與指定計劃方案有關的政府補助金包括在資本補助金內，並且延遲至須與擬補償的成本產生時，才在全面收益表內確認。

與購置物業、機器及設備有關的政府補助金包括在資本補助金內，並按有關資產的預計年限，以直線法記入全面收益表內。

用於彌補個人資料私隱專員已產生支出的政府補助金及專案資助金，會在支出產生的期間在全面收益表確認為收入。

「防疫抗疫基金」下創造職位計劃的財務資助按應計制在全面收益表內確認，以配對擬補償的僱員成本。

(ii) 銀行利息收入

銀行利息收入以實際利率方式計算。

(iii) 講座收費及會員費收入

講座收費及會員費收入按應計制確認。

3. Material Accounting Policy Information (Continued)

(k) Income Recognition

(i) Government Subventions and Funding

Government subventions are recognised at their fair value where there is a reasonable assurance that the grant will be received and the PCPD will comply with all attached conditions.

Government subventions relating to specific projects are included in the capital subvention fund and are deferred and recognised in the statement of comprehensive income over the period necessary to match them with the costs that they are intended to compensate.

Government subventions relating to the purchase of property, plant and equipment are included in the capital subvention fund and are credited to the statement of comprehensive income on a straight-line basis over the expected lives of the related assets.

Government subventions and project funds that compensate the PCPD for expenses incurred are recognised as income in the statement of comprehensive income in the same periods in which the expenses are incurred.

Financial assistance under Job Creation Scheme of Anti-epidemic Fund is recognised in the statement of comprehensive income on an accrual basis to match them with the staff costs that they are intended to compensate.

(ii) Bank Interest Income

Bank interest income is recognised using the effective interest method.

(iii) Seminar and Membership Fees Income

Seminar and membership fees income are recognised on an accrual basis.

3. 重要會計政策信息(續)

(I) 僱員薪俸

(i) 僱員可享有的假期及約滿酬金

僱員可享用的年假及約滿酬金在該等假期及合約期累計予僱員時確認。個人資料私隱專員已為僱員在計至年結日止所提供的服務而在年假及約滿酬金方面預計引致的責任作出撥備。

僱員可享用的病假及分娩假或侍產假不作確認，直至僱員放取該等假期時才予以確認。

(ii) 退休福利成本

個人資料私隱專員已經加入《強制性公積金條例》下成立的強制性公積金計劃(「強積金計劃」)。僱主的供款額為僱員有關入息的5%至強制性供款上限。該計劃的資產與個人資料私隱專員的資產分開持有，並由信託人以基金託管。

向強積金計劃支付的供款於到期日列作支出。

(m) 資產減值

在報告期末，個人資料私隱專員會檢討具有限可使用年期的資產的帳面值，以判斷該資產是否出現減值虧損。當顯示可能出現減值虧損時，該資產的可收回值會被評估以計算其虧損幅度。如該資產的可收回值並不可能被評估，個人資料私隱專員會評估該資產所屬的現金產生單位可收回值。當確定了一個合理及一致的分類基礎時，企業資產會被分類為獨立現金產生單位或現金產生單位的最小組別。

3. Material Accounting Policy Information (Continued)

(I) Staff Emoluments

(i) Employee Leave and Gratuity Entitlements

Employee entitlements to annual leave and gratuities are recognised when they accrue to employees. A provision is made for the estimated liability for annual leave and gratuities as a result of services rendered by employees up to the year-end date.

Employee entitlements to sick leave and maternity or paternity leave are not recognised until the time of leave.

(ii) Retirement Benefit Costs

The PCPD has joined the Mandatory Provident Fund Scheme (the MPF Scheme) established under the Mandatory Provident Fund Schemes Ordinance for its employees. The PCPD contributes 5% of the relevant income of staff members up to the maximum mandatory contributions under the MPF Scheme. The assets of the Scheme are held separately from those of the PCPD, in funds under the control of trustee.

Payments to the MPF Scheme are charged as an expense as they fall due.

(m) Impairment of Assets

At the end of reporting period, the PCPD reviews the carrying amounts of its assets with finite useful lives to determine whether there is any indication that those assets have suffered an impairment loss. If any such indication exists, the recoverable amount of the asset is estimated in order to determine the extent of the impairment loss, if any. When it is not possible to estimate the recoverable amount of an individual asset, the PCPD estimates the recoverable amount of the cash-generating unit to which the asset belongs. When a reasonable and consistent basis of allocation can be identified, corporate assets are also allocated to individual cash-generating units, or otherwise they are allocated to the smallest group of cash-generating units for which a reasonable and consistent allocation basis can be identified.

3. 重要會計政策信息(續)

(n) 關聯方

(i) 一名人士或其近親被視為個人資料私隱專員的關聯方，如果該人士：

- (a) 能控制或共同控制個人資料私隱專員；
- (b) 能對個人資料私隱專員構成重大影響力；或
- (c) 為個人資料私隱專員的關鍵管理人員。

(ii) 一個實體可視為個人資料私隱專員的關聯方，如果該實體符合以下任何情況：

- (a) 該實體是為個人資料私隱專員或個人資料私隱專員關聯方的僱員福利而設的離職後福利計劃。
- (b) 該實體由(i)中描述的人士控制或共同控制。
- (c) (i)(a)中描述的一名人士對該實體構成重大影響，或為該實體的關鍵管理人員。
- (d) 該實體，或屬該實體一部分的任何集團成員公司，向個人資料私隱專員提供關鍵管理人員服務。

3. Material Accounting Policy Information (Continued)

(n) Related Parties

(i) A Person or a Close Member of that Person's Family is Related to the PCPD if that Person:

- (a) has control or joint control over the PCPD;
- (b) has significant influence over the PCPD; or
- (c) is a member of the key management personnel of the PCPD.

(ii) An Entity is Related to the PCPD if any of the Following Conditions Applies:

- (a) The entity is a post-employment benefit plan for the benefit of employees of either the PCPD or an entity related to the PCPD.
- (b) The entity is controlled or jointly controlled by a person identified in (i).
- (c) A person identified in (i)(a) has significant influence over the entity or is a member of the key management personnel of the entity.
- (d) The entity, or any member of a group of which it is a part, provides key management personnel services to the PCPD.

4. 重要會計推算及判斷

按照《香港財務報告準則會計準則》編制財務報表時，個人資料私隱專員管理層會為影響到資產、負債、收入及開支的會計政策的應用作出判斷、估計及假設。這些判斷、估計及假設是以過往經驗及多項其他於有關情況下視作合理的因素為基準。儘管管理層對這些判斷、估計及假設作出持續檢討，實際結果可能有別於此等估計。

有關財務風險管理的某些主要假設及風險因素載列於附註19。對於本財務報表所作出的估計及假設，預期不會構成重大風險，導致下一財政年度資產及負債的帳面值需作大幅修訂。

4. Critical Accounting Estimates and Judgement

The PCPD's management makes assumptions, estimates and judgements in the process of applying the PCPD's accounting policies that affect the assets, liabilities, income and expenses in the financial statements prepared in accordance with HKFRSs. The assumptions, estimates and judgements are based on historical experience and other factors that are believed to be reasonable under the circumstances. While the management reviews their judgements, estimates and assumptions continuously, the actual results will seldom equal to the estimates.

Certain key assumptions and risk factors in respect of the financial risk management are set out in note 19. There are no other key sources of estimation uncertainty that have a significant risk of causing a material adjustment to the carrying amounts of asset and liabilities within the next financial year.

5. 政府補助金

5. Government Subventions

		2025 \$	2024 \$
經常性及非經常性	Recurrent and non-recurrent	103,319,515	99,095,220
資本補助金(附註16)	Capital subvention fund (Note 16)	236,150	287,071
		103,555,665	99,382,291

6. 僱員薪俸

6. Staff Emoluments

		2025 \$	2024 \$
薪酬	Salaries	78,105,691	67,094,255
約滿酬金及其他津貼	Gratuities and other allowances	14,407,162	12,774,223
強積金計劃供款	Contributions to MPF Scheme	1,800,214	1,618,715
未放取年假撥備／ (撥備回撥)	Provision/(reversal of provision) for unutilised annual leave	101,333	(163,526)
		94,414,400	81,323,667

7. 主要管理人員的報酬

7. Key Management Compensation

		2025 \$	2024 \$
短期僱員薪俸	Short-term staff emoluments	18,188,848	16,040,926
約滿酬金及強積金計劃供款	Gratuities and contributions to MPF Scheme	2,294,106	2,169,423
		20,482,954	18,210,349

8. 稅項

8. Taxation

根據《個人資料(私隱)條例》附表2第6條的規定，個人資料私隱專員獲豁免課稅，因此個人資料私隱專員無須在本財務報表計提香港利得稅撥備。

No provision for Hong Kong Profits Tax has been made in the financial statements as the PCPD is exempted from taxation in respect of the Inland Revenue Ordinance by virtue of Schedule 2 Section 6 of the Personal Data (Privacy) Ordinance.

9. 物業、機器及設備

9. Property, Plant and Equipment

		擁有資產 Owned assets						使用權資產 Right-of-use assets	總計 Total
		汽車 Motor vehicle	電腦及軟件 Computer and software	辦公室設備 Office equipment	家具及固定裝置 Furniture and fixtures	租賃物業裝修工程 Leasehold improvements	小計 Sub-total	租賃土地及樓宇 Leasehold land and buildings	
		\$	\$	\$	\$	\$	\$	\$	\$
成本	Cost								
於2024年4月1日	At 1 April 2024	895,488	8,107,132	2,471,312	647,766	10,481,486	22,603,184	58,216,410	80,819,594
增加	Additions	–	274,000	87,158	1,126	97,600	459,884	2,012,458	2,472,342
處置	Disposal	–	–	–	–	(137,260)	(137,260)	–	(137,260)
注銷	Written off	–	–	–	–	–	–	(737,602)	(737,602)
於2025年3月31日	At 31 March 2025	895,488	8,381,132	2,558,470	648,892	10,441,826	22,925,808	59,491,266	82,417,074
累積折舊	Accumulated depreciation								
於2024年4月1日	At 1 April 2024	735,493	6,822,976	2,008,035	563,298	10,344,070	20,473,872	38,384,186	58,858,058
年內折舊	Charge for the year	119,996	799,565	161,775	31,023	107,119	1,219,478	7,655,582	8,875,060
處置核銷	Written back on disposal	–	–	–	–	(110,570)	(110,570)	–	(110,570)
注銷	Written off	–	–	–	–	–	–	(737,602)	(737,602)
於2025年3月31日	At 31 March 2025	855,489	7,622,541	2,169,810	594,321	10,340,619	21,582,780	45,302,166	66,884,946
帳面淨值	Net book value								
於2025年3月31日	At 31 March 2025	39,999	758,591	388,660	54,571	101,207	1,343,028	14,189,100	15,532,128
成本	Cost								
於2023年4月1日	At 1 April 2023	895,488	8,143,278	2,296,862	626,376	10,481,486	22,443,490	37,412,832	59,856,322
增加	Additions	–	119,875	190,450	21,390	–	331,715	20,803,578	21,135,293
處置	Disposals	–	(156,021)	(16,000)	–	–	(172,021)	–	(172,021)
於2024年3月31日	At 31 March 2024	895,488	8,107,132	2,471,312	647,766	10,481,486	22,603,184	58,216,410	80,819,594
累積折舊	Accumulated depreciation								
於2023年4月1日	At 1 April 2023	615,497	6,087,162	1,759,209	507,437	10,096,076	19,065,381	30,671,863	49,737,244
年內折舊	Charge for the year	119,996	891,835	264,826	55,861	247,994	1,580,512	7,712,323	9,292,835
處置核銷	Written back on disposals	–	(156,021)	(16,000)	–	–	(172,021)	–	(172,021)
於2024年3月31日	At 31 March 2024	735,493	6,822,976	2,008,035	563,298	10,344,070	20,473,872	38,384,186	58,858,058
帳面淨值	Net book value								
於2024年3月31日	At 31 March 2024	159,995	1,284,156	463,277	84,468	137,416	2,129,312	19,832,224	21,961,536

10. 銀行結存及現金

10. Bank Balances and Cash

		2025 \$	2024 \$
銀行及手頭現金	Cash at banks and on hand	41,452,600	11,287,272
短期銀行存款	Short-term bank deposits	38,463,118	32,736,547
財務狀況表及現金流量表 的銀行結存及現金	Bank balances and cash in the statement of financial position and the statement of cash flows	79,915,718	44,023,819

11. 職員約滿酬金撥備

11. Provision for Staff Gratuity

		2025 \$	2024 \$
於4月1日的結餘	Balance as at 1 April	6,609,982	5,672,020
已作出的撥備	Provision made	9,484,787	8,071,250
未動用款項撥回	Unused amounts reversed	(541,993)	(141,556)
年內支付的數額	Amount paid during the year	(7,974,338)	(6,991,732)
於3月31日的結餘	Balance as at 31 March	7,578,438	6,609,982
減：流動部分	Less: current portion	(5,378,866)	(4,805,529)
非流動部分	Non-current portion	2,199,572	1,804,453

約滿酬金撥備是為了支付由受聘日起計已完成合約的職員的約滿酬金而設立的。

Provision for staff gratuity is established for gratuity payments which become payable to those employees of the PCPD who complete their contracts commencing from the date of their employment.

12. 預收政府補助金

12. Government Subvention Received in Advance

		2025 \$	2024 \$
於4月1日的結餘	Balance as at 1 April	9,740,217	8,175,593
已收補助金	Subvention received	7,000,000	2,780,248
年內確認為收入的數額	Recognised as income in the year	(3,242,258)	(1,215,624)
於3月31日的結餘	Balance as at 31 March	13,497,959	9,740,217

預收政府補助金是關於年結日後才提供的各項服務而收取的補助金，會遞延入帳及在支出產生的期間在全面收益表確認為收入。

Government subvention received in advance represents subvention received in connection with various services to be provided after year end and is deferred and recognised as income in the statement of comprehensive income in the same periods in which the expenses are incurred.

13. 預收政府專案資助金

13. Government Project Funds Received in Advance

		2025 \$	2024 \$
已收專案資助金	Project funds received	42,764,000	–
年內確認為收入的數額	Recognised as income in the year	(12,663,265)	–
於3月31日的結餘	Balance as at 31 March	30,100,735	–

預收政府專案資助金是為粵港澳大灣區跨境信息流動便利化措施的相關工作而收取的資助金，會遞延入帳及在支出產生的期間在全面收益表確認為收入。

Government project funds received in advance represent funding received in connection with work relating to the cross-boundary data flow facilitation measures in the Guangdong-Hong Kong-Macao Greater Bay Area and is deferred and recognised as income in the statement of comprehensive income in the same periods in which the expenses are incurred.

14. 租賃負債

14. Lease Liabilities

		2025 \$	2024 \$
到期最低租賃付款額	Minimum lease payments due		
– 1年內	– Within 1 year	8,273,976	7,557,902
– 1至5年	– 1 to 5 years	6,894,980	13,537,964
		15,168,956	21,095,866
減：未來財務費用	Less : future finance charges	(576,082)	(1,209,671)
租賃負債的現值	Present value of lease liabilities	14,592,874	19,886,195
分析為：	Analysed as:		
流動部分	Current portion	7,824,824	6,868,997
非流動部分	Non-current portion	6,768,050	13,017,198
		14,592,874	19,886,195

未來財務費用所應用的加權平均遞增借貸利率為4%(2024：4.125%)。

The weighted average incremental borrowing rate applied for future finance charges is 4% (2024 : 4.125%).

15. 政府的約滿酬金補助款

15. Government Subvention for Gratuity

		2025 \$	2024 \$
於4月1日的結餘	Balance as at 1 April	3,990,784	4,086,978
年內確認的補助金	Subvention recognised for the year	(9,559,250)	(8,087,750)
沒收款	Forfeiture	541,993	141,556
已收政府的約滿酬金補助款	Gratuity subvention received from Government	8,720,000	7,850,000
於3月31日的結餘	Balance as at 31 March	3,693,527	3,990,784

這代表就個人資料私隱專員從政府收取的職員約滿酬金款項。

This represents funds received from the Government in respect of gratuity payments to staff of the PCPD.

16. 資本補助金

16. Capital Subvention Fund

		資訊科技基礎 設施檢修項目 IT Infrastructure Overhaul Project \$	更新投訴 處理系統 Case Handling System Revamp \$	購置客貨車 Procurement of van \$	電腦鑑證 Computer Forensics \$	總計 Total \$
於2023年4月1日	At 1 April 2023	46,149	109,745	223,992	226,472	606,358
撥入全面收益表 為收入，以配對：	Transfer to the statement of comprehensive income as income to match with:					
– 折舊支出	– Depreciation expense	(46,149)	(57,259)	(95,997)	(87,666)	(287,071)
於2024年3月31日 及 2024年4月1日	At 31 March 2024 and 1 April 2024	–	52,486	127,995	138,806	319,287
撥入全面收益表 為收入，以配對：	Transfer to the statement of comprehensive income as income to match with:					
– 折舊支出	– Depreciation expense	–	(52,486)	(95,997)	(87,667)	(236,150)
於2025年3月31日	At 31 March 2025	–	–	31,998	51,139	83,137
流動部分	Current portion	–	–	31,998	51,139	83,137
非流動部分	Non-current portion	–	–	–	–	–
		–	–	31,998	51,139	83,137

資本補助金為就特定計劃方案已收取但未應用的非經常性政府資本補助金的餘額。有關款項撥入全面收益表為收入，以配對相關費用。

The capital subvention fund represents the unutilised balance of non-recurrent capital subvention from the Government received for special projects. The funds are released to the statement of comprehensive income as income to match with the related costs.

17. 一般儲備

17. General Reserve

		2025 \$	2024 \$
於4月1日	At 1 April	25,518,721	30,385,007
由全面收益／(虧損) 表撥入	Transfer from statement of comprehensive income/(loss)	245,812	(1,448,092)
政府收回上年盈餘	Previous year's surplus recovered by Government	–	(3,418,194)
於3月31日	At 31 March	25,764,533	25,518,721

設立一般儲備的目的是用來應付營運上的突發事項。一般儲備由全面收益表撥入，最高限額為個人資料私隱專員年度經常補助金的25%。一般儲備是用作一般用途，個人資料私隱專員有權自行運用。盈餘如超逾儲備的協定上限，超額之數應退還政府（扣減下年度的補助金以抵銷）。

The general reserve is established to meet operational contingencies and is transferred from the statement of comprehensive income with a ceiling at 25% of the PCPD's annual recurrent subvention. The general reserve is available for general use and can be spent at the discretion of the PCPD. Any surplus in excess of the agreed reserve ceiling should be returned to the Government by way of offsetting from next year's subvention.

18. 融資活動產生的負債對帳

18. Reconciliation of Liabilities Arising from Financing Activities

下表詳述個人資料私隱專員來自融資活動的負債變動，包括現金及非現金變動。融資活動所產生的負債為現金流量或未來現金流量將於個人資料私隱專員的現金流量表中分類為融資活動的現金流量。

The table below details changes in the PCPD's liabilities from financing activities, including both cash and non-cash changes. Liabilities arising from financing activities are liabilities for which cash flows were, or future cash flows will be, classified in the PCPD's statement of cash flows as cash flows from financing activities.

		2025 \$	2024 \$
於年初	At beginning of the year	19,886,195	6,922,018
融資現金流的變動：	Changes from financing cash flows:		
已付租賃負債本金	Capital element of lease rentals paid	(7,305,779)	(7,839,401)
已付租賃負債利息	Interest element of lease rentals paid	(734,007)	(226,192)
融資現金流的變動總額	Total changes from financing cash flows	(8,039,786)	(8,065,593)
其他變動：	Other changes:	11,846,409	(1,143,575)
租賃負債利息	Interest on lease liabilities	734,007	226,192
租賃負債增加	Increase in lease liabilities	2,012,458	20,803,578
其他變動總額	Total other changes	2,746,465	21,029,770
於年末	At end of the year	14,592,874	19,886,195

19. 金融工具

個人資料私隱專員將其金融資產分為以下類別：

19. Financial Instruments

The PCPD has classified its financial assets in the following categories:

		2025 \$	2024 \$
按攤銷成本計量的金融資產	Financial assets at amortised cost		
應收款項及按金	Accounts receivable and deposits	141,049	236,979
銀行結存及現金	Bank balances and cash	79,915,718	44,023,819
		80,056,767	44,260,798

個人資料私隱專員將其金融負債分為以下類別：

The PCPD has classified its financial liabilities in the following categories:

		2025 \$	2024 \$
按攤銷成本計量的金融負債	Financial liabilities at amortised cost		
應付款項及應計費用	Accounts payable and accruals	242,996	180,049
政府的約滿酬金補助款	Government subvention for gratuity	3,693,527	3,990,784
租賃負債	Lease liabilities	14,592,874	19,886,195
		18,529,397	24,057,028

所有金融工具的帳面值相對2024年及2025年3月31日時的公平值均沒有重大差別。

All financial instruments are carried at amounts not materially different from their fair values as at 31 March 2025 and 2024.

19. 金融工具(續)

個人資料私隱專員的風險管理目標、政策和流程主要側重於透過密切監控個別風險承擔，最大限度地減低信貸風險、流動資金風險及市場風險對其財務表現及狀況的潛在不利影響。

(a) 信貸風險

個人資料私隱專員並無信貸風險相當集中的情況，而最高信貸風險相等於金融資產所載有關帳面值。銀行存款的信貸風險是有限，因接受存款的銀行均為受香港《銀行業條例》規管的財務機構。

(b) 流動資金風險

個人資料私隱專員的流動資金風險是金融負債。個人資料私隱專員對資金作出謹慎管理，維持充裕的現金及現金等值，以滿足持續運作的需要。

19. Financial Instruments (Continued)

The PCPD's risk management objectives, policies and processes mainly focus on minimising the potential adverse effects of credit risk, liquidity risk and market risk on its financial performance and position by closely monitoring the individual exposure.

(a) Credit Risk

The PCPD has no significant concentration of credit risk. The maximum exposure to credit risk is represented by the carrying amount of the financial assets. The credit risk on bank deposits is limited because the counterparties are authorised financial institutions regulated under the Hong Kong Banking Ordinance.

(b) Liquidity Risk

The PCPD is exposed to liquidity risk on financial liabilities. It manages its funds conservatively by maintaining a comfortable level of cash and cash equivalents in order to meet continuous operational need. The PCPD ensures that it maintains sufficient cash which is available to meet its liquidity.

19. 金融工具(續)

(b) 流動資金風險(續)

下表載列個人資料私隱專員的金融負債於報告期末的剩餘合約年期。該等金融負債是根據合約未貼現現金流量(包括使用已訂合約利率或按報告期末的利率(如屬浮息)計算所付的利息)以及個人資料私隱專員可能被要求付款的最早日期編製：

		帳面值 Carrying amount \$	合約未貼現 現金流總額 Total contractual undiscounted cash flow \$	一年內 或按要求 Within 1 year or on demand \$	一年後 但五年內 Over 1 year but within 5 years \$
2025	2025				
應付款項及 應計費用	Accounts payable and accruals	242,996	242,996	242,996	–
政府的約滿酬金 補助款	Government subvention for gratuity	3,693,527	3,693,527	–	3,693,527
租賃負債	Lease liabilities	14,592,874	15,168,956	8,273,976	6,894,980
		18,529,397	19,105,479	8,516,972	10,588,507
2024	2024				
應付款項及 應計費用	Accounts payable and accruals	180,049	180,049	180,049	–
政府的約滿酬金 補助款	Government subvention for gratuity	3,990,784	3,990,784	–	3,990,784
租賃負債	Lease liabilities	19,886,195	21,095,866	7,557,902	13,537,964
		24,057,028	25,266,699	7,737,951	17,528,748

(c) 市場風險

利率風險

個人資料私隱專員的利率風險主要來自銀行存款。個人資料私隱專員沒有對所產生的利率風險作敏感性分析，因為管理層評估此風險對個人資料私隱專員的財務狀況不會產生重大影響。

(d) 以公平值計量的金融工具

在報告期末，個人資料私隱專員並沒有金融工具以公平值列帳。

19. Financial Instruments (Continued)

(b) Liquidity Risk (Continued)

The details of remaining contractual maturities at the end of the reporting period of the financial liabilities, which are based on contractual undiscounted cash flows (including interest payments computed using contractual rates or, if floating, based on rates current at the end of the reporting period) and the earliest date the PCPD can be required to pay are as follows:

(c) Market Risk

Interest Rate Risk

The PCPD's exposure on interest rate risk mainly arises from its cash deposits with bank. No sensitivity analysis for the PCPD's exposure to interest rate risk arising from deposits with bank is prepared since based on the management's assessment the exposure is considered not significant.

(d) Financial Instrument at Fair Value

At the end of reporting period, there were no financial instruments stated at fair value.

20. 已頒佈但於年內尚未生效的《香港財務報告準則會計準則》

以下是已頒佈但於年內尚未生效的《香港財務報告準則會計準則》，這些準則或與個人資料私隱專員的營運及財務報表有關：

20. HKFRS Accounting Standards Issued but not yet Effective for the Year

HKFRSs that have been issued but are not yet effective for the year include the following HKFRSs which may be relevant to the PCPD's operations and financial statements:

於以下年度開始或以後生效 Effective for annual periods beginning on or after		
《香港會計準則》第21號及《香港財務報告準則》第1號之修訂 缺乏可兌換性	HKAS 21 and HKFRS 1, <i>Lack of Exchangeability (amendments)</i>	2025年1月1日 1 January 2025
《香港財務報告準則》第9號及《香港財務報告準則》第7號之修訂 金融工具分類和計量的修訂	HKFRS 9 and HKFRS 7, <i>Classification and Measurement of Financial Instruments (amendments)</i>	2026年1月1日 1 January 2026
《香港財務報告準則》第1號、《香港財務報告準則》第7號、《香港財務報告準則》第9號、《香港財務報告準則》第10號及《香港會計準則》第7號 《香港財務報告準則會計準則》年度改進 — 第11卷	HKFRS 1, HKFRS 7, HKFRS 9, HKFRS 10 and HKAS 7, <i>Annual Improvements to HKFRS Accounting Standards – Volume 11</i>	2026年1月1日 1 January 2026
《香港財務報告準則》第18號 財務報表之呈列及披露(新準則)	HKFRS 18, <i>Presentation and Disclosure in Financial Statements (new standard)</i>	2027年1月1日 1 January 2027
《香港財務報告準則》第19號 非公共受託責任附屬公司：披露(新準則)	HKFRS 19, <i>Subsidiaries without Public Accountability: Disclosures (new standard)</i>	2027年1月1日 1 January 2027
香港詮釋第5號(經修訂)財務報表的呈列 — 借款人對包含按要求償還條款之定期貸款之分類	Hong Kong Interpretation 5 <i>Presentation of Financial Statements – Classification by the Borrower of a Term Loan that Contains a Repayment on Demand Clause (amendments)</i>	2027年1月1日 1 January 2027
《香港財務報告準則》第10號及《香港會計準則》第28號之修訂 投資者與其聯營公司或合營公司之間之資產出售或注資	HKFRS 10 and HKAS 28, <i>Sale or Contribution of Assets between an Investor and its Associate or Joint Venture (amendments)</i>	尚未釐定 To be determined

個人資料私隱專員在本年內並未採納該等《香港財務報告準則會計準則》。初步評估顯示採納該等《香港財務報告準則會計準則》不會對個人資料私隱專員首次採納年度的財務報表產生重大影響。個人資料私隱專員將繼續評估該等《香港財務報告準則會計準則》及其他就此識別的重大變動的影響。

The PCPD has not early adopted these HKFRSs. Initial assessment has indicated that the adoption of these HKFRSs would not have a significant impact on the PCPD's financial statements in the year of initial application. The PCPD will be continuing with the assessment of the impact of these HKFRSs and other significant changes may be identified as a result.

21. 批准財務報表

本財務報表已於2025年7月31日獲個人資料私隱專員授權刊發。

21. Approval of Financial Statements

These financial statements were authorised for issue by the PCPD on 31 July 2025.



附錄

Appendices

附錄一 Appendix 1

保障資料原則 Data Protection Principles

附錄二 Appendix 2

服務承諾 Performance Pledge

附錄三 Appendix 3

上訴個案簡述 Appeal Case Notes

附錄四 Appendix 4

投訴個案選錄 • 以作借鑑

Summaries of Selected Complaint Cases – Lessons Learnt

附錄五 Appendix 5

定罪個案選錄 • 以作借鑑

Summaries of Selected Conviction Cases – Lessons Learnt

附錄六 Appendix 6

循規行動個案選錄 • 以作借鑑

Summaries of Selected Compliance Action Cases – Lessons Learnt



附錄一

Appendix 1

保障資料原則

《私隱條例》旨在保障個人(資料當事人)在個人資料方面的私隱權。所有收集、持有、處理或使用個人資料的人士(資料使用者)須依從《私隱條例》下的六項保障資料原則。該六項原則為《私隱條例》的核心，涵蓋了個人資料由收集以至銷毀的整個生命週期。

個人資料

指符合以下說明的任何資料：(1)直接或間接與一名在世的個人有關的；(2)從該資料直接或間接地確定有關的個人的身分是切實可行的；及(3)該資料的存在形式令予以查閱及處理均是切實可行的。

資料使用者

指獨自或聯同其他人或與其他人共同控制個人資料的收集、持有、處理或使用的人士。資料使用者作為主事人，亦須為其聘用的資料處理者的錯失負上法律責任。

Data Protection Principles

The objective of the PDPO is to protect the privacy rights of a person (Data Subject) in relation to his personal data. A person who collects, holds, processes or uses the data (Data User) should follow the six Data Protection Principles (DPPs) under the PDPO. The DPPs represent the normative core of the PDPO and cover the entire life cycle of a piece of personal data, from collection to destruction.

Personal Data

means any data (1) relating directly or indirectly to a living individual; (2) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (3) in a form in which access to or processing of the data is practicable.

Data User

means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data. The data user is liable as the principal for the wrongful act of any data processor engaged by it.

第1原則 — 收集資料原則

- 資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應為合法，而直接與其職能或活動有關。
- 須以所有切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。
- 收集的資料就該目的而言，是必需及足夠，而不超乎適度。

DPP 1 – Data Collection Principle

- Personal data must be collected in a lawful and fair way, and for a lawful purpose directly related to a function or activity of the data user.
- All practicable steps must be taken to notify the data subjects of the purpose for which the data is to be used, and the classes of persons to whom the data may be transferred.
- Personal data collected should be necessary and adequate but not excessive in relation to the purpose of collection.

第2原則 — 資料準確、儲存及保留原則

- 資料使用者須採取所有切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的实际所需。

DPP 2 – Accuracy and Retention Principle

- A data user must take all practicable steps to ensure that personal data is accurate and not kept for a period longer than is necessary to fulfil the purpose for which it is used.

第3原則 — 使用資料原則

- 個人資料只限用於收集時述明的目的或直接相關的目的；除非得到資料當事人自願和明確的同意。

DPP 3 – Data Use Principle

- Personal data is used only for the purpose for which the data is collected or for a directly related purpose; voluntary and explicit consent must be obtained from the data subject if the data is to be used for a new purpose.

第4原則 — 資料保安原則

- 資料使用者須採取所有切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

DPP 4 – Data Security Principle

- A data user must take all practicable steps to protect personal data from unauthorised or accidental access, processing, erasure, loss or use.

第5原則 — 透明度原則

- 資料使用者須採取所有切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

DPP 5 – Openness Principle

- A data user must take all practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

第6原則 — 查閱及改正原則

- 資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

DPP 6 – Data Access and Correction Principle

- A data subject is entitled to have access to his personal data and to make corrections where the data is inaccurate.

附錄二

Appendix 2

服務承諾

在報告年度內，私隱專員公署在處理公眾查詢、投訴及法律協助計劃申請方面的工作表現均高於服務指標。

私隱專員公署在處理公眾查詢時，均能夠在兩個工作日內回覆所有電話查詢及確認收到所有書面查詢，並在28個工作日內詳細回覆所有書面查詢。

在處理公眾投訴方面，所有個案均能夠在收到投訴後兩個工作日內發出認收通知（服務指標為98%）；而在決定結束投訴個案當中，98%的個案都能夠在180日內結案（服務指標為95%）。

至於處理法律協助計劃申請方面，所有個案均能夠在收到申請後兩個工作日內發出認收通知，並在申請人遞交法律協助申請的所有相關資料後三個月內通知他們申請結果。

Performance Pledge

During the reporting year, the PCPD's performance in the handling of public enquiries, complaints, and applications for legal assistance exceeded the performance target.

In handling public enquiries, the PCPD responded to all telephone enquiries and written enquiries within two working days of receipt. Substantive replies to all written enquiries were also completed within 28 working days of receipt.

In respect to public complaints, acknowledgement receipts were issued within two working days of receipt in all cases (our performance target is 98%). In closing a complaint case, 98% of the cases were closed within 180 days of receipt (our performance target is 95%).

As regards handling applications for legal assistance, acknowledgement receipts were issued within two working days of receipt of all applications, with all applicants being informed of the outcome within three months after submitting all relevant information for their applications.



服務標準 Service Standard		服務指標 (個案達到服務水平的百分比) Performance Target (% of Cases Meeting Standard)	工作表現 Performance Achieved				
			2020	2021	2022	2023	2024
處理公眾查詢 Handling Public Enquiries							
回覆電話查詢 Call back to a telephone enquiry	收到電話查詢後 兩個工作日內 Within two working days of receipt	99%	100%	100%	100%	100%	100%
確認收到書面查詢 Acknowledge receipt of a written enquiry	收到書面查詢後 兩個工作日內 Within two working days of receipt	99%	100%	100%	100%	100%	100%
詳細回覆書面查詢 Substantive reply to a written enquiry	收到書面查詢後 28個工作日內 Within 28 working days of receipt	95%	100%	100%	100%	100%	100%
處理公眾投訴 Handling Public Complaints							
確認收到投訴 Acknowledge receipt of a complaint	收到投訴後 兩個工作日內 Within two working days of receipt	98%	99%	99%	99%	100%	100%
結束投訴個案 Close a complaint case	收到投訴後 180日內 ¹ Within 180 days of receipt ¹	95%	99%	99%	98%	97%	98%
處理法律協助計劃申請 Handling Applications for Legal Assistance							
確認收到法律協助計劃申請 Acknowledge receipt of an application for legal assistance	收到申請後 兩個工作日內 Within two working days of receipt	99%	不適用 ² N/A ²	100%	100%	100%	100%
通知申請人申請結果 Inform the applicant of the outcome	申請人遞交法律協助申請的所有相關資料後三個月內 Within three months after the applicant has submitted all the relevant information for the application for legal assistance	90%	100%	100%	100%	100%	100%

1 由投訴被正式接納為《私隱條例》第37條下的投訴後開始計算。
From the date on which the complaint is formally recognised under section 37 of the PDPO.

2 於2020年沒有收到申請。
No application was received in 2020.

附錄三

Appendix 3

上訴個案簡述 Appeal Case Notes

上訴個案簡述(一)

(行政上訴案件第48/2015號)

姓名及職銜被傳媒刊登 — 沒有證據證明
是被投訴者外洩資料 — 行使調查權力 —
《私隱條例》第44條及46條 — 保障資料第3及
4原則

Appeal Case Note (1)

(AAB Appeal No. 48 of 2015)

Name and post title being published by the media – no evidence that
the information was leaked from the persons being complained against –
exercise of investigative powers – sections 44 and 46 of the PDPO – DPPs
3 and 4

聆訊委員會成員：

Coram:

裁決理由書日期：

Date of Decision:

彭耀鴻資深大律師(副主席) Mr Robert PANG Yiu-hung, SC (Deputy Chairman)

郭岳忠先生(委員) Mr Dick KWOK Ngok-chung (Member)

何玉慧女士(委員) Ms Joan HO Yuk-wai (Member)

2024年6月18日

18 June 2024

投訴內容

上訴人是某政府部門(該部門)的高級職員。
上訴人不滿傳媒在報道某執法機構(該執法
機構)在其所屬部門的辦公室進行搜查及檢
取證物的行動時刊登了他的姓名及職銜(該
等個人資料)，因而向私隱專員投訴。上訴
人指稱該部門及／或該執法機構未有獲得
其同意而向傳媒披露該等個人資料，違反保
障資料第3原則的規定，以及該部門及／或
該執法機構未有採取所有切實可行的步驟保
障上訴人的個人資料不受未獲准許的或意外
的查閱、喪失或使用所影響，違反保障資料
第4原則的規定。

The Complaint

The Appellant was a senior officer of a government department (the Department). He complained to the Privacy Commissioner that his name and post title (the Personal Data Concerned) were published by the media in relation to an operation being conducted by a law enforcement agency (the Agency) at his office at the Department to search and seize evidence. The Appellant alleged that the Department and/or the Agency had disclosed the Personal Data Concerned to the media without his consent, thereby contravening DPP 3, and the Department and/or the Agency had failed to take all practicable steps to protect against unauthorised or accidental access, loss, or use of the Personal Data Concerned, thereby contravening DPP 4.



私隱專員的決定

調查期間，該部門及該執法機構均否認曾向傳媒披露該等個人資料。在上訴人未能提供相反證據下，私隱專員認為沒有足夠證據證明上訴人所指稱該部門及該執法機構有違反保障資料第3及4原則的行為。私隱專員認為，即使有人曾向傳媒披露該等個人資料，該披露涉及新聞活動及公眾利益，故亦獲《私隱條例》第61(2)條豁免而不受保障資料第3原則規限。

再者，私隱專員亦留意到曾有大批該執法機構人員到該部門進行搜查，故不能排除傳媒的消息來源可能是目擊該執法機構行動的人士。假如有關資料是經口頭訊息傳遞而未經記錄於文件當中，便不構成《私隱條例》下的「資料」。

上訴人不滿私隱專員的決定，遂向行政上訴委員會(委員會)提出上訴。

上訴

委員會確認私隱專員的決定，並基於下述理由駁回上訴：

- (1) 私隱專員進行調查時可行使廣泛的酌情權。至於行使一項或多項調查權力與否則屬私隱專員的酌情範圍內。私隱專員可以就調查諮詢投訴人，如她信納此做法有助其調查，但她沒有必須這樣做的義務。

The Privacy Commissioner's Decision

During the investigation, the Department and the Agency denied having disclosed the Personal Data Concerned to the media. In the absence of contrary evidence adduced by the Appellant, the Privacy Commissioner concluded that there was insufficient evidence to support the Appellant's allegation that the Department and the Agency had contravened DPPs 3 and 4. The Privacy Commissioner considered that even if there had been disclosure of the Personal Data Concerned to the media, such disclosure pertaining to news activities and the public interest could be exempted under section 61(2) of the PDPO from the application of DPP 3.

Furthermore, the Privacy Commissioner observed that there had been a large party of officers of the Agency entering the Appellant's office at the Department to conduct the search. Hence, it could not rule out that the media's source of information could be a person who had witnessed the Agency's operation. If the relevant information was conveyed orally and not recorded in a document, it would not fall within the definition of "data" under the PDPO.

Dissatisfied with the Privacy Commissioner's decision, the Appellant appealed to the Administrative Appeals Board (AAB).

The Appeal

The AAB affirmed the Privacy Commissioner's decision and dismissed the appeal on the following grounds:

- (1) The Privacy Commissioner has wide discretion in the conduct of investigations. Whether to utilise one or more of her investigative powers is a matter within her discretion. Whilst the Privacy Commissioner may consult a complainant if she thinks that it would be of assistance, there is no obligation to do so.

- | | |
|--|---|
| <p>(2) 就是否根據《私隱條例》第44條傳召傳媒的人員以質詢其資料的來源，私隱專員需要考慮及平衡多項因素。針對傳媒所得的資料行使這種權力的決定可能會影響言論及新聞自由，故必須謹慎行事，而委員會認為不應在本案的情況下行使有關權力。</p> | <p>(2) Whether or not to summon a member of the press under section 44 of the PDPO to divulge the source of the information would be surrounded by a number of considerations which have to be balanced. The decision to exercise such power against journalistic materials should not be taken lightly since it would engage the rights of freedom of expression and the press. The AAB did not consider that such power should be exercised in the circumstances of the case.</p> |
| <p>(3) 在本案中沒有足夠證據證明該等個人資料是由該部門及該執法機構外洩。</p> | <p>(3) There was insufficient evidence to show that the Personal Data Concerned was leaked from the Department and the Agency in this case.</p> |
| <p>(4) 《私隱條例》保障資料第4原則沒有要求資料使用者負上絕對責任確保個人資料的保安，只要求資料使用者採取所有合理地切實可行的步驟以確保個人資料的保安。本案沒有足夠證據證明該部門及該執法機構有違反保障資料第4原則的規定。</p> | <p>(4) It is not a requirement under DPP 4 of the PDPO for a data user to provide an absolute guarantee for the security of personal data held by it as long as all reasonably practicable steps have been taken to ensure the security of personal data. There was insufficient evidence of contravention of DPP 4 on the part of both the Department and the Agency.</p> |
| <p>(5) 至於上訴人投訴私隱專員未有在調查過程中向上訴人披露該部門及／或該執法機構的回覆，委員會認為《私隱條例》第46(2)條沒有對私隱專員施加法定責任須向上訴人披露每項調查結果。</p> | <p>(5) In respect of the Appellant's complaint against the Privacy Commissioner's non-disclosure of the replies from the Department and/or the Agency during the investigation process, the AAB held that section 46(2) of the PDPO does not impose a statutory duty on the Privacy Commissioner to disclose every investigation finding to the Appellant.</p> |

行政上訴委員會的決定

委員會駁回本上訴。

上訴人親身應訊

陳淑音時任律師代表私隱專員

麥敬時大律師受張秀儀唐滙棟羅凱栢律師行延聘代表該部門及該執法機構（受到遭上訴所反對的決定所約束的人）

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person

Ms Cindy CHAN, the then Legal Counsel, represented the Privacy Commissioner

Mr Robin MCLEISH, instructed by Messrs Cheung Tong & Rosa Solicitors, represented the Department and the Agency (the Persons bound by the decision appealed against)

上訴個案簡述(二)

(行政上訴案件第 46/2022號)

個人資料的使用 — 收購品牌後客戶個人資料的跨品牌查閱及使用 — 《私隱條例》第63B條下盡職審查的豁免 — 《私隱條例》第65(3)條下的抗辯 — 程序不當 — 正確行使酌情權發出執行通知

Appeal Case Note (2)

(AAB Appeal No. 46 of 2022)

Use of personal data – cross-brand access to and use of personal data of clients post-acquisition – due diligence exemption under section 63B of the PDPO – defence under section 65(3) of the PDPO – procedural irregularities – discretion to issue Enforcement Notice duly exercised

聆訊委員會成員：

Coram:

裁決理由書日期：

Date of Decision:

孫靖乾資深大律師(副主席) Mr Jenkin SUEN, SC (Deputy Chairman)

陳浩升先生(委員) Mr Ernest CHAN Ho-sing (Member)

容慧慈女士(委員) Ms Christine YUNG Wai-chi (Member)

2025年2月26日

26 February 2025

投訴內容

本上訴源於兩宗針對上訴人所收購的品牌的投訴。在首宗投訴個案中，投訴人帶同其女兒到品牌A向某醫生求診。其後，投訴人得悉其女兒的個人資料在該醫生加入上訴人旗下另一品牌時被轉移至該品牌。在另一宗投訴個案中，投訴人向品牌B提供了個人資料，但其後發現上訴人旗下另一品牌的職員曾查閱其個人資料。

The Complaint

The appeal arose from two complaints against brands acquired by the Appellant. In one complaint, the complainant took her daughter to Brand A to consult a doctor. She was later informed that her daughter's personal data had been transferred to another brand under the Appellant, to which the doctor switched at work. In another complaint, the complainant provided his personal data to Brand B and discovered later that the staff from another brand under the Appellant had accessed his personal data.

私隱專員的決定

經調查後，私隱專員發現上訴人在收購品牌A及品牌B後，將兩者客戶的個人資料儲存在上訴人的統一系統(該系統)中，並將客戶的部分個人資料供旗下28個品牌透過該系統互用。此安排令不同品牌的前線職員能夠查閱相關的個人資料，惟上訴人不曾就該安排向客戶徵求訂明同意。上訴人亦沒有以任何方式通知被收購的品牌的既有客戶有關收購的事宜，更未有向他們提供上訴人的私隱政策。

The Privacy Commissioner's Decision

Upon investigation, the Privacy Commissioner found that the Appellant, having acquired Brand A and Brand B, stored the personal data of the clients of these two brands in its integrated system (the System) and shared parts of the personal data among the 28 brands of the Appellant via the System. This arrangement enabled the frontline staff of various brands to have access to the relevant personal data, despite no prescribed consent being sought by the Appellant from the clients for such an arrangement. Likewise, the Appellant never informed the existing clients of the acquired brands of the relevant acquisition by any means, nor did it provide those clients with its privacy policy.

私隱專員認為，上述安排與當初收集投訴人的個人資料的目的不一致，因而上訴人違反了保障資料第3原則的規定。私隱專員向上訴人發出執行通知，指示上訴人糾正其違反事項，以及防止同類違反的行為再發生。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

上訴

委員會確認私隱專員的決定，並基於下述理由駁回上訴人的上訴：

- (1) 委員會同意私隱專員的調查結果，認為上訴人旗下品牌的前線職員能透過上訴人的統一系統，使用及跨品牌查閱客戶的個人資料。
- (2) 委員會強調，品牌A或品牌B所收集的個人資料原擬使用於由該等品牌所提供的服務，而非用於由同一服務領域內或同一集團內其他品牌所提供的服務。此外，由於其他品牌查閱個人資料並無便利品牌A或品牌B提供服務，因此，個人資料的互用與原先的收集目的並無直接關聯。雖然上訴人的收集個人資料聲明(該聲明)允許跨品牌查閱個人資料，但該聲明僅適用於就其給予了同意的新客戶，而並不適用於相關品牌在被上訴人收購前所收集的個人資料。

The Privacy Commissioner found that the Appellant had contravened the requirements of DPP 3, as the aforementioned arrangement was inconsistent with the original purpose of collection of the complainants' personal data. The Privacy Commissioner issued an Enforcement Notice, directing the Appellant to remedy and prevent recurrence of the relevant contraventions. Dissatisfied with the Privacy Commissioner's decision, the Appellant lodged an appeal to the AAB.

The Appeal

The AAB confirmed the Privacy Commissioner's decision and dismissed the appeal on the following grounds:

- (1) The AAB agreed with the Privacy Commissioner's finding that frontline staff of the Appellant's brands were able to use and make cross-brand access to the clients' personal data in the System.
- (2) The AAB stressed that the personal data collected by Brand A or Brand B was intended for the provision of services by those brands only, not by other brands within the same field of services or within the same group. Furthermore, since access to personal data by other brands did not facilitate the provision of services by Brand A or Brand B, the sharing of personal data was not directly related to the original purpose of collection. The Personal Information Collection Statement (PICS) of the Appellant, which permitted access to personal data across different brands, would only apply to new customers who consented to the PICS, but not to personal data collected by the brands concerned before they were acquired by the Appellant.



- (3) 由於本案涉及的是上訴人作出收購後使用個人資料的情況，與盡職審查並不相關，因此《私隱條例》第63B條並不適用於本案。《私隱條例》第65(3)條亦不適用，因為問題並非源於僱員所作出的作為或從事的行為本身，而是源於該系統的設計及功能。
- (4) 委員會駁回了上訴人提出有關程序不當的指控。委員會指出，私隱專員並無法定責任提前披露執法行動及建議。此外，私隱專員已向上訴人提前提供了調查報告擬稿的相關部分，當中詳述了其調查結果及理由。委員會確認，私隱專員在進行調查及取得任何資料時擁有靈活及廣泛的酌情權，能按其認為合適的方式作出相關查詢。
- (3) Section 63B of the PDPO did not apply since this case did not involve a due diligence exercise, but rather the post-acquisition use of personal data. Section 65(3) was also not applicable, as the underlying problem stemmed not from the acts or practices of employees per se, but from the design and features of the System.
- (4) The AAB rejected the Appellant's allegations of procedural irregularities. It was observed that the Privacy Commissioner is not under a statutory duty to disclose enforcement actions and recommendations in advance. Furthermore, the Privacy Commissioner had already provided the Appellant with a draft of the relevant parts of the investigation report setting out her findings and reasoning in great detail. The AAB affirmed that the Privacy Commissioner has a flexible and wide discretion as to the conduct of investigations and how she may be furnished with information, and can make such enquiries as she thinks fit.

行政上訴委員會的決定

委員會駁回本上訴。

黃繼兒大律師及管致行大律師受胡百全律師事務所延聘代表上訴人

吳穎軒時任高級律師代表私隱專員

投訴人(受到遭上訴所反對的決定所約束的人)缺席聆訊

The AAB's Decision

The appeal was dismissed.

Mr Stephen WONG and Mr Jay KOON, instructed by Messrs P.C. Woo & Co., represented the Appellant

Ms Hermina NG, the then Senior Legal Counsel, represented the Privacy Commissioner

The complainants (the Persons bound by the decision appealed against) were absent

上訴個案簡述(三)

(行政上訴案件第 13/2024號)

委員會的管轄權 — 指明調查 — 《行政上訴委員會條例》—《私隱條例》第66S條

Appeal Case Note (3)

(AAB Appeal No. 13 of 2024)

Jurisdiction of the AAB – specified investigation – Administrative Appeals Board Ordinance – section 66S of the PDPO

聆訊委員會成員：

Coram:

裁決理由書日期：

Date of Decision:

劉恩沛資深大律師(副主席) Ms LAU Queenie Fiona, SC (Deputy Chairman)

張璟璋工程師(委員) Ir Jason CHEUNG King-wai (Member)

許繼偉教授(委員) Prof. HUI Kai-wai (Member)

2025年3月18日

18 March 2025

投訴內容

上訴人因涉嫌被「起底」而向私隱專員投訴。私隱專員根據《私隱條例》第66C條展開指明調查，但最終因證據不足而終止調查，並根據《私隱條例》第66S條以書信形式告知上訴人調查結果。上訴人就私隱專員的決定提出上訴，而私隱專員則質疑委員會對該上訴是否有管轄權。

The Complaint

The Appellant lodged a doxxing complaint with the Privacy Commissioner. The Privacy Commissioner commenced a specified investigation pursuant to section 66C of the PDPO but eventually terminated the investigation due to insufficient evidence, and informed the Appellant of the result by way of a letter pursuant to section 66S of the PDPO. The Appellant appealed against the Privacy Commissioner's decision. The Privacy Commissioner questioned the AAB's jurisdiction to hear the appeal.



上訴

就管轄權問題作出裁決時，委員會同意私隱專員的陳詞，認為該委員會沒有審理此上訴的管轄權，其理由如下：

- (1) 委員會是根據《行政上訴委員會條例》（香港法例第442章）《行政上訴委員會條例》成立的，其管轄範圍僅限於列入《行政上訴委員會條例》附表中的決定，以及任何以委員會作為審理上訴機構的其他決定。然而，有關《私隱條例》第66S條中就私隱專員須告知投訴人指明調查結果的決定並不屬於附表範圍內的決定。
- (2) 委員會是負責處理與行政決定相關上訴的機構，而《私隱條例》第66S條的相關決定並非一項行政決定。

行政上訴委員會的決定

由於委員會沒有審理該上訴的法定權力，本上訴因此被駁回。

上訴人親身應訊

周沅瑩律師代表私隱專員

The Appeal

In ruling on the issue of jurisdiction, the AAB agreed with the Privacy Commissioner's submissions that the AAB does not have jurisdiction to hear the appeal for the following reasons:

- (1) The AAB was established in accordance with the Administrative Appeals Board Ordinance (Chapter 442 of the Laws of Hong Kong) (Administrative Appeals Board Ordinance). Its jurisdiction is limited to the decisions listed in the schedule to the Administrative Appeals Board Ordinance and any other decision in respect of which an appeal lies to the AAB. However, the decision relating to section 66S of the PDPO regarding the obligation of the Privacy Commissioner to inform the complainant of the result of a specified investigation does not fall under the said schedule.
- (2) While the AAB is an institution responsible for handling appeals concerning administrative decisions, the decision relating to section 66S of the PDPO is not an administrative decision.

The AAB's Decision

Since the AAB does not have the statutory authority to hear the appeal, the appeal was dismissed.

The Appellant appeared in person

Ms Stephanie CHAU, Legal Counsel, represented the Privacy Commissioner

上訴個案簡述(四)

(行政上訴案件第 27/2024號)

為依從查閱資料要求而徵收的費用 — 是否超乎適度 — 是否高於資料使用者採用其他形式依從查閱資料要求而徵收的最低費用 — 《私隱條例》第28(3)條及28(4)條

Appeal Case Note (4)

(AAB Appeal No. 27 of 2024)

Fee imposed for complying with data access request – whether excessive – whether higher than the lowest fee the data user imposes for complying with the request in other form – sections 28(3) and 28(4) of the PDPO

聆訊委員會成員：

Coram:

裁決理由書日期：

Date of Decision:

馬淑蓮女士(副主席) Ms Jay MA Suk-lin (Deputy Chairman)

陳俊濠先生(委員) Mr William CHAN Chun-ho (Member)

蔡靜瑜女士(委員) Ms TSAI Ching-yu (Member)

2024年12月16日

16 December 2024

投訴內容

上訴人是一名公開試考生。主辦該公開試的機構(該機構)表示，自2023年起，查閱資料要求申請人將不會獲發所要求的資料的實體複本。該機構會發送一封內含密碼及連結的電郵，供申請人下載所要求的個人資料，包括評分紀錄及試卷。基於發放所查閱資料的形式有所改變，上訴人認為查閱資料的費用應當下調，惟該機構就每個首科查閱資料要求徵費的下調幅度僅為港幣20元，每個附加科目查閱資料要求徵費則維持不變。上訴人遂向私隱專員投訴該機構過度收取查閱評分紀錄及試卷費用，違反《私隱條例》第28(3)條有關為依從查閱資料要求而徵收的費用不得超乎適度的規定。

The Complaint

The Appellant was a candidate of a public examination. According to the administrating body of the examination (the Administrator), starting from 2023, the data access requestor would not be provided with a hard copy of the requested data. Instead, the Administrator would issue an email to the requestor with a password and a link for downloading the requested personal data, including marking records and examination scripts. The Appellant considered that, in view of the change in the form of provision of requested data, the fee imposed for accessing the data should be reduced. However, the fee imposed by the Administrator for the first data access application was reduced by only HK\$20, whereas the fee for accessing the data of each additional subject remained unchanged. The Appellant thus lodged a complaint with the Privacy Commissioner against the Administrator for imposing excessive fees for accessing marking records and examination scripts, in violation of section 28(3) of the PDPO which stipulates that no fee imposed for complying with a data access request shall be excessive.

此外，上訴人亦投訴該機構於2023年前在能夠發放電子複本的情況下，仍選擇以成本較高的實體複本來依從查閱資料要求，並以此作計算徵收的費用，違反《私隱條例》第28(4)條的規定。

私隱專員的決定

經調查後，私隱專員發現該機構為依從查閱資料要求而徵收的費用均低於其直接有關及必須的成本，包括員工薪酬開支、電腦操作時間費及其他開支。因此，私隱專員認為該機構為依從查閱資料要求而徵收的費用沒有超乎適度，並沒有違反《私隱條例》第28(3)條的規定。

此外，私隱專員認為《私隱條例》第28(4)條的規定建基於資料使用者可以採用兩種或以上形式中的其中一種，提供查閱資料要求所關乎的個人資料的複本。由於該機構在相關時間只能以一種形式（即實體複本）提供相關資料，因此《私隱條例》第28(4)條並不適用，該機構並沒有違反有關規定。

In addition, the Appellant also complained against the Administrator for violating section 28(4) of the PDPO by choosing to comply with data access requests by providing hard copies of the data at a higher cost and calculating the fees imposed on that basis before 2023, when it was able to provide electronic copies of the requested data.

The Privacy Commissioner's Decision

Upon investigation, the Privacy Commissioner found that the fees imposed by the Administrator for complying with data access requests were lower than the necessary and directly related costs incurred in complying with the data access request. Such costs included labour costs, computer operating time costs and other costs. As such, the Privacy Commissioner found that the fees imposed by the Administrator for complying with data access requests were not excessive and the Administrator had not contravened section 28(3) of the PDPO.

Furthermore, the Privacy Commissioner found that the relevant requirement under section 28(4) of the PDPO is premised on the fact that a data user may provide a copy of the personal data to which a data access request relates in one of two or more forms. As the Administrator could only provide copies of the relevant data in one form (that is, in the form of hard copies) in the relevant period, the Privacy Commissioner considered that section 28(4) of the PDPO was not applicable and the Administrator had not contravened the relevant requirement.



上訴

委員會確認私隱專員的決定，並基於下述理由駁回上訴人的上訴：

- (1) 私隱專員向該機構所作的調查充足。調查期間，私隱專員從該機構取得該機構為依從查閱資料要求所產生的工序及成本資料，當中並無充足證據顯示該些工序及成本不屬直接相關及必須。
- (2) 考慮到該機構持有龐大數量的個人資料及有嚴謹處理有關資料的需要，該機構表示於相關時間向考生發放電子複本並非可行和穩妥的解釋，並非不合理。委員會亦同意上訴人認為以電郵方式傳送文件所需成本較低的指稱欠缺證據支持。

行政上訴委員會的決定

委員會駁回本上訴。

上訴人親身應訊

陳世皓律師代表私隱專員

黃文傑資深大律師受霍金路偉律師行延聘代表該機構(受到遭上訴所反對的決定所約束的人)

The Appeal

The AAB confirmed the Privacy Commissioner's decision and dismissed the appeal on the following grounds:

- (1) The Privacy Commissioner's investigation against the Administrator was adequate. During the investigation, the Privacy Commissioner sought and obtained information on the steps involved and costs incurred by the Administrator for complying with data access requests, and there was insufficient evidence showing that such steps and costs are not necessary or directly related.
- (2) The Administrator's explanation that it was unable to provide electronic copies of marking records and examination scripts in the relevant period due to feasibility and security reasons was not unreasonable, particularly in view of the vast amount of personal data that the Administrator possessed and the Administrator's need to exercise caution. The AAB also agreed that there was no evidence supporting the Appellant's allegation that transmitting electronic copies of the documents by email would involve lower costs.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person

Mr Kevin CHAN, Legal Counsel, represented the Privacy Commissioner

Mr Anson WONG, SC, instructed by Messrs Hogan Lovells, represented the Administrator (the Person bound by the decision appealed against)

附錄四

Appendix 4

投訴個案選錄 • 以作借鑑 Summaries of Selected Complaint Cases – Lessons Learnt

個案一

床上用品公司強制網上購物客戶同意將個人資料作直接促銷用途 — 保障資料第1原則 — 收集個人資料的目的及方式

投訴內容

投訴人在一間床上用品公司(該公司)的網站購物並進入付款的頁面時，發現顧客必須剔選指定方格以同意該公司按其私隱政策使用顧客的個人資料作促銷用途，否則將不能付款以完成交易。投訴人就此向私隱專員公署投訴。

結果

該公司向私隱專員公署解釋，即使顧客剔選其指定方格，他們亦不會被視為同意直接促銷，並跟從公署的意見修改網站的付款交易頁面，令顧客可於頁面選擇是否剔選同意該公司使用其個人資料作促銷用途的方格。

借鑑

不論資料使用者的直接促銷活動是否與收集資料的原本目的(即為向客戶提供所尋求的基本服務)直接有關，客戶應可自行決定是否同意資料使用者使用其個人資料作直接促銷。若資料使用者透過服務申請表向客戶收集個人資料，而表格的設計令客戶無法拒絕其個人資料用於直接促銷用途(即「綑綁式同意」的情況)，這種做法可被視為以不公平方法收集個人資料。

Case 1

A bedding product company mandated online shoppers to consent to the use of personal data for direct marketing purposes – DPP 1 – purpose and manner of collection of personal data

The Complaint

When the complainant visited the online shop of a bedding product company (the Company), he noted on the checkout page that customers were required to check the designated box to indicate consent to the use of their personal data in direct marketing in accordance with the Company's privacy policy, or else the payment would not go through to complete the purchase. The complainant hence lodged a complaint with the PCPD.

Outcome

The Company explained to the PCPD that even if customers checked the designated box, they would not be deemed to have consented to direct marketing. With the PCPD's advice, the Company revised the checkout page of the website so that customers would be provided with an option to choose whether to check the box for providing consent to the use of their personal data for direct marketing purposes.

Lessons Learnt

Irrespective of whether the direct marketing activities of the data user are directly related to the original purpose of collection of the customer's personal data (namely for the primary service of the data user provided for its customers), customers shall have the right to decide whether to consent to the use of their personal data by the data user for the purpose of direct marketing. If a data user collects personal data from customers through a service application form which is designed in such a way that renders it impracticable for its customers to refuse the use of their personal data for direct marketing purposes (i.e. under a "bundled consent" situation), such collection of personal data may be deemed an unfair collection of personal data.

個案二

金融機構過量收集外判員工的個人資料，且未有提供收集個人資料聲明及過度保留個人資料——保障資料第1原則——收集個人資料的目的及方式——保障資料第2原則——個人資料的保留期間

投訴內容

投訴人任職一間資訊科技公司，並被安排於一間金融機構的場所工作。投訴人並非受僱於該金融機構，但被要求提交其個人資料，當中包括其出生日期，且得悉與該金融機構結束關係後，其個人資料會被該金融機構保留七年。投訴人遂向私隱專員公署投訴該金融機構過量收集其個人資料、向其收集個人資料之時或之前沒有向他提供收集個人資料聲明，以及保留他的個人資料時間過長。

結果

該金融機構向私隱專員公署表示，收集投訴人的出生日期僅為了在其電腦系統中建立投訴人的個人帳戶，以便行政安排。該金融機構確認，由於當時未可透過系統或既定的溝通渠道提供有關資訊，他們向投訴人收集個人資料之時或之前難以採取切實可行的措施與投訴人溝通，故並未向投訴人提供收集個人資料聲明的相關內容。

此外，該金融機構確認在事發時並沒有就外判員工的每項個人資料因應其個別目的而制定獨立的保留期限，而是劃一要求保留所有個人資料七年。然而，基於投訴人只是該金融機構的外判員工，而非由該金融機構直接聘用，私隱專員公署認為該金融機構理應無須就任何僱傭原因（包括稅務或強積金供款安排）或其他目的而需要保留投訴人的香港身份證號碼長達七年之久。另外，由於該金融機構並非必須收集投訴人的出生日期，因此亦無須保存其出生日期。

Case 2

A financial institution collected excessive personal data from outsourced staff without providing a PICS and retained personal data for a period longer than necessary – DPP 1 – purpose and manner of collection of personal data – DPP 2 – retention of personal data

The Complaint

The complainant worked for an information technology company and was assigned to work at the premises of a financial institution. Although the complainant was not employed by the financial institution, he was required to provide his personal data, including his date of birth, to the institution. The complainant noticed that his personal data would be retained for seven years from the date of termination of his relationship with the financial institution. The complainant therefore lodged a complaint with the PCPD against the financial institution for excessive collection of his personal data, failure to provide him with a PICS on or before the collection of personal data, and retention of his personal data for a prolonged period of time.

Outcome

The financial institution explained to the PCPD that the collection of the complainant's date of birth was merely for the purpose of creating a personal account of the complainant in its computer system for administrative purposes. The financial institution confirmed that, since it was not possible to provide the relevant information through the system or any designated channel of communication at that time, it was impracticable to communicate with the complainant on or before the collection of personal data, and therefore the financial institution did not provide the complainant with the relevant contents of the PICS.

Moreover, the financial institution confirmed that at the time of the incident, it did not set out an independent retention period for each item of the personal data of its outsourced staff according to its individual reasons and purposes. Instead, it required the retention of all personal data for seven years in a uniform manner. However, given that the complainant was only an outsourced staff member of the financial institution and was not directly employed by the institution, the PCPD considered that the financial institution was not bound to retain the complainant's Hong Kong Identity Card (HKID Card) number for any employment reasons (including taxation or MPF contribution arrangements) or other purposes for a lengthy period of seven years. Additionally, given that it was not necessary for the financial institution to collect the complainant's date of birth, it was also not necessary to retain his date of birth.

經私隱專員公署介入後，該金融機構確定不再需要收集外判公司員工的出生日期，並會妥善地刪除就建立員工帳戶而收集的外判公司現職及前員工的出生日期，並已制定收集個人資料聲明以提供予各部門、供應商及合作公司僱用的外判員工和借調人員，提醒員工在向資料當事人收集個人資料之時或之前提供有關聲明的重要性。該金融機構亦已獨立檢視因應不同原因及目的而從外判員工收集所得的各項個人資料的保留期限，並更新了個人資料保留政策內各項資料的保留期限。

基於上述情況，私隱專員認為該金融機構在個案中違反了保障資料第 1(1)、1(3)及 2(2)原則的規定。考慮到個案的情況，包括但不限於該金融機構採取的改善措施，私隱專員公署就有關投訴事項向該金融機構發出警告信，要求該金融機構日後須緊遵《私隱條例》的相關規定。

借鑑

透過分判形式（包括透過第三者）聘用職員時，機構需要特別注意其處理個人資料的情況。此類情況的例子包括透過職業介紹所聘請員工，或職員受聘於一間公司但卻代表另一間公司工作。

由於這些機構與有關人士並無直接簽訂僱傭合約，一般而言，機構需要向分判職員收集的個人資料會較直接聘用的職員為少。若有關個人資料是直接向分判職員收集，機構應向相關職員提供收集個人資料聲明。此外，這些機構只能在符合收集分判職員的個人資料時所述明的收集目的，或有合理可能性再度聘用有關職員擔任後續工作的情況下，方可繼續保留其個人資料。

After the intervention of the PCPD, the financial institution confirmed that it was no longer necessary to collect the dates of birth of outsourced staff, and that the institution would properly delete the dates of birth of current and former outsourced staff collected for the purpose of creating employee accounts. The institution formulated a PICS for all departments and outsourced staff, as well as seconded staff employed by suppliers and collaborators, and reminded the staff of the importance of providing the PICS on or before the collection of personal data from data subjects. The financial institution also independently reviewed the retention period of each item of personal data collected from its outsourced staff for its individual reasons and purposes, and updated the retention period of each item of personal data in the personal data retention policy.

Based on the above, the Privacy Commissioner was of the view that the financial institution had contravened DPPs 1(1), 1(3) and 2(2) in this case. Taking into account the circumstances of the case, including but not limited to the remedial measures taken by the financial institution, the PCPD issued a warning letter to the financial institution in response to the complaint, requiring the financial institution to comply with the relevant requirements of the PDPO in the future.

Lessons Learnt

When employing staff through sub-contracting (including through third parties), organisations should pay particular attention to the handling of personal data. Examples of such situation would include employment through an employment agency, or staff employed by one company but who undertake work on behalf of another company.

As these organisations do not enter into a direct employment contract with the individual concerned, they would, in general, collect less personal data from those subcontracted staff than from their own staff. If personal data is collected directly from the subcontracted staff, the organisations should provide a PICS for the concerned staff. In addition, these organisations can only continue to retain the personal data of subcontracted staff for the purposes for which the data was collected, or where there is a reasonable likelihood that such staff may be re-engaged for subsequent work.

個案三

政府部門使用申請人的舊地址 郵寄信件 — 保障資料第2原則 — 個人資料的準確性

投訴內容

投訴人是某政府部門(該部門)兩項不同公共服務的申請人，在申請兩項服務時均曾向該部門提供通訊地址。投訴人不滿該部門在他透過香港政府一站通平台(一站通)更改他在該部門的通訊地址後，仍將信件郵寄至投訴人的舊地址，遂向私隱專員公署投訴該部門。

結果

該部門表示，投訴人所使用的兩項服務由該部門內的不同組別負責。兩項服務的申請人資料分別儲存於兩個獨立的電腦系統，由相關組別各自更新，而兩項服務更新地址的手續亦不相同。該部門解釋，投訴人透過一站通更新的地址只適用於其中一項服務。由於投訴人沒有通知負責另一項服務的組別更改地址，該組別遂根據其系統中的紀錄，將信函寄到投訴人的舊地址。

經私隱專員公署介入後，該部門已擬備新的表格以供更改另一項服務的相關地址，並更改現有資料更新表格及相關的電郵及信函回覆範本，從而清楚向服務使用者說明地址更新只適用於個別相關服務的紀錄，並提醒服務使用者須另行通知相關的負責組別，以更新他們在該部門其他服務的地址紀錄。

Case 3

A government department posted a letter to an applicant's obsolete address – DPP 2 – accuracy of personal data

The Complaint

The complainant was an applicant for two public services offered by a government department (the Department), and he provided his address to the Department when he applied for both services. The complainant was dissatisfied that, after he had submitted an address update to the Department through the GovHK platform (GovHK), the Department still posted a letter to the complainant's obsolete address. The complainant hence lodged a complaint with the PCPD against the Department.

Outcome

According to the Department, the two services used by the complainant were managed by different teams within the Department. The two teams stored applicants' information for the two services in two separate systems and updated their respective information independently, with different address update procedures. The Department explained that the address update made by the complainant via GovHK was only applicable to one of the two services. Since the complainant did not update his address with the team responsible for the other service, that other team thus referred to the address record in its system and sent a letter to the complainant's obsolete address.

Upon the intervention of the PCPD, the Department prepared a new form for updating the relevant address for the other service and revised the existing personal data update form, along with the relevant email and letter templates, so as to explicitly inform service users that the address update would only be applicable to the individual relevant service, and to remind them to notify the relevant team(s) if they needed to change the address record for other services within the Department.

借鑑

機構或會基於他們的運作需要，安排機構內不同單位負責不同的計劃或服務。雖然有關的分工安排屬常見情況，但服務使用者一般不會理解機構內不同單位各自存有其獨立的通訊地址紀錄的安排。就此，如機構就不同計劃或服務制定不同的個人資料更新程序，應該向服務使用者清楚說明在不同服務下更新個人資料的程序，確保服務使用者充分知悉相關安排，以避免出現誤會並確保個人資料的準確性。

Lessons Learnt

Organisations may assign different teams to manage different projects or services according to their operational needs. While division of work within an organisation is a common practice, service users may not realise that different teams within an organisation would maintain their independent address records. If an organisation puts in place different procedures for updating personal data for different projects or services, the organisation should convey clear messages to service users about the arrangement in order to ensure that the service users are fully aware of how to update their personal data for different services. This can help avoid misunderstanding and maintain the accuracy of personal data.



附錄五

Appendix 5

定罪個案選錄 • 以作借鑑 Summaries of Selected Conviction Cases – Lessons Learnt

個案一

汽車公司在未有採取所需步驟通知兩名當事人及取得他們的同意下向他們發出直接促銷訊息，以及未有告知該兩名當事人他們拒收直接促銷訊息的權利——《私隱條例》第35C及35F條

Case 1

A car company failed to take the necessary actions to notify the two data subjects and obtain their consents before using their personal data in direct marketing, and failed to notify the data subjects of their opt-out rights – sections 35C and 35F of the PDPO

法院：	東區裁判法院
Court:	Eastern Magistrates' Court
審理裁判官：	曾宗堯裁判官
Coram:	Mr TSANG Chung-yiu, Magistrate
裁決日期：	2024年7月2日
Date of Decision:	2 July 2024

投訴內容

兩名投訴人各自於2023年11月收到來自一間汽車公司(該公司)的促銷信件，信件中載有投訴人的英文姓名及居住地址。兩名投訴人均曾致電該公司作出查詢，並獲告知該公司是透過運輸署的紀錄獲得投訴人的個人資料並用作發出上述信件。投訴人認為該公司在未經他們同意的情況下，使用他們的個人資料向他們發出直接促銷訊息，遂向私隱專員公署作出投訴。

The Complaint

Each of the two complainants received a marketing letter from an automobile company (the Company) by post in November 2023. The letters contained the complainants' English names and addresses. Both complainants called the Company to make enquiries and were informed by its staff that their personal data had been collected from the records of the Transport Department for the purpose of issuing the letters. The complainants considered that the Company had used their personal data for direct marketing without their consents, thus they lodged complaints with the PCPD.

結果

警方落案起訴該公司四項違反《私隱條例》第35C(1)條及第35F(1)條的罪行。根據案情，該公司在未有採取所需步驟通知兩名投訴人及取得他們的同意下，從運輸署的紀錄取得投訴人的個人資料並向他們分別發出直接促銷訊息。該公司亦在首次使用投訴人的個人資料作直接促銷時，未有分別告知投訴人他們有權要求該公司在不收費的情況下，停止使用他們的個人資料。該公司承認傳票控罪，每張傳票分別被判罰款港幣2,500元，合共港幣10,000元。

借鑑

資料使用者（不論個人或機構）擬進行任何產品或服務類別的直接促銷前，必須採取指明行動通知資料當事人並獲得其同意，方可使用其個人資料作直接促銷。此外，資料使用者在首次使用他人的個人資料作直接促銷時，亦應告知當事人有權在不收費的情況下，要求停止在直接促銷中使用其個人資料，否則資料使用者便可能要負上刑事責任。違反第35C(1)條及第35F(1)條的規定均屬刑事罪行，違例者一經定罪，每項罪行最高刑罰是港幣50萬元及監禁三年。

Outcome

The Police laid four charges under sections 35C(1) and 35F(1) of the PDPO against the Company. According to the facts of the case, the Company failed to take the necessary actions to notify the two complainants and obtain their consents before using their personal data obtained from the records of the Transport Department in direct marketing. The Company also failed to inform the two complainants, when using their personal data in direct marketing for the first time, of their rights to request the Company not to use their personal data in direct marketing without charge. The Company pleaded guilty to the charges and was fined HK\$2,500 for each summons, totalling HK\$10,000.

Lessons Learnt

Prior to carrying out any direct marketing activity for any goods or services, a data user (whether an individual or an organisation) must take specified actions to notify the data subject and obtain his consent on the intended use of his personal data for the said purpose. Moreover, the data user should inform the data subject, when using his personal data in direct marketing for the first time, of the data subject's right to request the data user to cease to use the data in direct marketing without charge. Otherwise, the data user may incur criminal liability. Failure to comply with the requirements of sections 35C(1) and 35F(1) constitutes a criminal offence. The offender is liable to a fine up to HK\$500,000 and imprisonment for three years.



個案二

女子建立網上群組供他人發布「起底」訊息 — 協助及教唆他人干犯《私隱條例》第64(3A)條

Case 2

A female created an online discussion group for others to post doxxing messages – aiding and abetting others for committing offences under section 64(3A) of the PDPO

法院：	東區裁判法院
Court:	Eastern Magistrates' Court
審理裁判官：	鍾穎詩暫委裁判官
Coram:	Ms CHUNG Wing-sze, Deputy Magistrate
裁決日期：	2024年11月26日
Date of Decision:	26 November 2024

投訴內容

被告在社交媒體平台開設一個公開群組，供他人發布「起底」訊息。被告在本案中被控協助及教唆同案另外兩名被告在上述群組發布「起底」訊息。

The Complaint

The defendant opened a public discussion group on a social media platform for others to post doxxing messages. The defendant was charged with having aided and abetted the other two defendants of the same case for the latter's posting of doxxing messages in the said group.

結果

於2024年11月，被告經審訊後被裁定干犯五項「協助及教唆他人在未獲資料當事人同意下披露個人資料罪」的罪名成立，法院於同年12月判處被告120小時社會服務令。

Outcome

In November 2024, the defendant was convicted of five charges of the offence of "aiding and abetting to disclose personal data without data subject's consent" after trial. The court sentenced the defendant to 120 hours of community service in December 2024.

借鑑

提供平台及／或建立群組以供他人作出「起底」行為，足以構成協助及教唆他人干犯「起底」罪行，此舉同屬犯罪。

Lessons Learnt

Providing a platform and/or creating a group for others to engage in doxxing activities may constitute aiding and abetting others to commit the crime of doxxing, which is also considered as a criminal act.

個案三

的士司機在互聯網上披露行家的個人資料 —《私隱條例》第64(3A)條

Case 3

A taxi driver disclosed personal data of a counterpart on the Internet – section 64(3A) of the PDPO

法院：	沙田裁判法院
Court:	Sha Tin Magistrates' Court
審理裁判官：	鄭紀航署理主任裁判官
Coram:	Mr CHEANG Kei-hong, Acting Principal Magistrate
裁決日期：	2024年11月28日
Date of Decision:	28 November 2024

投訴內容

事主是一名的士司機，2023年9月起向被告租用的士，並將其香港身份證副本交予被告作身分認證。及至同年11月，雙方同意終止租賃安排，但事後事主及被告發生糾紛。同年12月，被告在一個社交媒體平台的一個公開群組發布了一條對事主作出指控的帖文，並附上一張略去部分內容，屬於事主的香港身份證副本，當中展示了事主的個人資料。

結果

於2024年11月，被告在認罪下被裁定干犯兩項《私隱條例》第64(3A)條「在未獲同意下披露個人資料」的罪名成立，法院於同年12月判處被告120小時社會服務令。

借鑑

身份證載有屬敏感的個人資料，隨意或惡意在未經當事人的同意下披露或轉載身份證副本，可以構成「起底」罪行。違例者一經定罪，最高可被處罰款港幣100萬元及監禁五年。

The Complaint

The victim, who is a taxi driver, rented a taxi from the defendant since September 2023, and provided the defendant with a copy of his HKID Card for identity verification purposes. Later in November 2023, the rental arrangement was terminated upon the parties' mutual agreement. Disputes, however, subsequently ensued between the parties. In December 2023, the defendant posted a message containing allegations against the victim in an open discussion group on a social media platform, alongside a partly redacted copy of his HKID Card which showed particulars of his personal data.

Outcome

In November 2024, the defendant was convicted of two charges of contravening section 64(3A) of the PDPO, "disclosing personal data without consent", upon his guilty plea. The court sentenced the defendant to 120 hours of community service in December 2024.

Lessons Learnt

Identity cards contain sensitive personal data. Disclosing or reposting copies of identity cards without the consent of the data subject concerned, either arbitrarily or maliciously, may constitute a doxxing offence. An offender is liable on conviction to a fine of up to HK\$1,000,000 and imprisonment of up to five years.

附錄六

Appendix 6

循規行動個案選錄 • 以作借鑑 Summaries of Selected Compliance Action Cases – Lessons Learnt

個案一

遺失載有個人資料的可攜式儲存裝置 — 保障資料第4原則 — 個人資料的保安

背景

一個政府部門（該部門）向私隱專員公署通報，指該部門委託一間服務承辦商協助管理社區會堂，惟該服務承辦商的一名員工在未經授權的情況下，將載有數百名申請者的姓名、電話號碼及僱主名稱的場地預約紀錄儲存至一枚USB記憶體內，而該員工於翌日發現遺失了該記憶體。

補救措施

在收到有關的資料外洩事故通報後，私隱專員公署展開了循規審查。因應該事件，該部門採取了一系列措施以防止類似事件再次發生，包括更換該服務承辦商提供的所有電腦，以確保該些電腦不能使用USB端口及不能連接至網絡；制定承辦商保障個人資料的指引，當中建議避免使用便攜式儲存裝置儲存個人資料；及承諾把該指引的規定納入未來的報價及招標程序，以確保承辦商妥善處理個人資料。

Case 1

Loss of portable storage device containing personal data – DPP 4 – security of personal data

Background

A government department (the Department) reported to the PCPD that it had engaged a service contractor to assist in managing a community complex, and that a staff member of the service contractor had stored the reservation records on a USB storage device without authorisation. The device, which contained the names, contact numbers and names of employers of a few hundred applicants, was discovered to be missing the next day.

Remedial Measures

Upon receiving the relevant data breach notification, the PCPD initiated a compliance check. In response to the incident, the Department implemented various measures to prevent recurrence of similar incidents. These included replacing computers provided by the service contractor, with computers that restrict the use of USB ports and which internet access are disabled; formulating a guideline for its contractors regarding the safeguard of personal data, including advising them to avoid storing personal data on portable storage devices; and incorporating the said guideline into future quotation and tender exercises to ensure proper handling of personal data by contractors.

借鑑

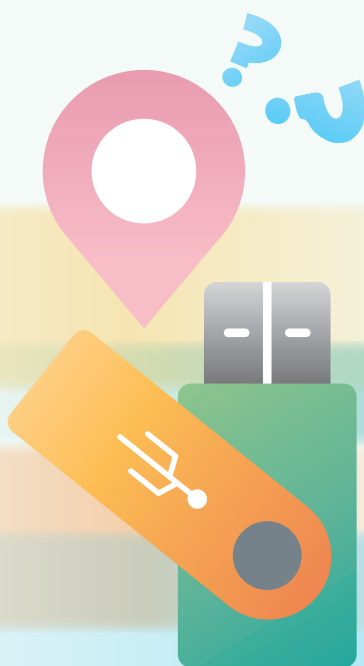
便攜式儲存裝置雖然提供一個便捷的方法儲存和轉移資料至機構系統以外的地方，但這會增加資料外洩的風險。機構應在切實可行的範圍內，避免使用便攜式儲存裝置來儲存個人資料。如有必要使用便攜式儲存裝置，應制定政策列明允許使用有關裝置的情況、可轉移到有關裝置的個人資料類別和數量、使用便攜式儲存裝置的審批程序等。機構亦應保存這類便攜式儲存裝置的清單及追蹤其使用情況和位置，並在每次使用後妥善地刪除當中的資料。

另一方面，如果機構委託第三方資料處理者，則應採用合約規範或其他方式，防止轉移給資料處理者進行處理的個人資料未經授權或意外存取、處理、刪除、遺失或使用。

Lessons Learnt

While portable storage devices offer a convenient means to store and transfer data outside of an organisation's system, they are susceptible to data security incidents. Organisations should avoid the use of portable storage devices to store personal data wherever practicable. If it is necessary to use portable storage devices, organisations should establish policies that set out the circumstances under which portable storage devices may be used, the types and amount of personal data that may be transferred, and the approval process of the use of portable storage devices, etc. Organisations should also keep an inventory of portable storage devices and track their uses and whereabouts, as well as erase data in portable storage devices securely after each use.

On the other hand, if organisations engage a third-party data processor, contractual or other means should be adopted to prevent unauthorised or accidental access, processing, erasure, loss or use of the personal data transferred to the data processor for processing.



個案二

會員數據庫遭未獲授權查閱 — 保障資料第4原則 — 個人資料的保安

背景

一間學會向私隱專員公署通報，指黑客利用其外掛程式的保安漏洞，在未經授權下獲得儲存於網絡伺服器的會員數據庫之存取權限，並竊取了約1,000名會員的個人資料，包括他們的姓名、地址、電郵地址及手機號碼等個人資料。

補救措施

接獲該學會的通報後，私隱專員公署展開循規審查，並就《私隱條例》的相關規定向該學會提供建議。事故發生後，該學會已停用涉事的外掛程式，並停止把個人資料儲存於涉事的數據庫。此外，該學會檢視所有外掛程式原始碼及修補漏洞，並透過建立新的監察機制，監控會員數據庫的數據變化。

借鑑

雖然外掛程式為資訊系統提供便利，但也帶來各種資料保安風險，包括安全漏洞、惡意程式碼及不當的權限管理等，而這些風險足以導致資料外洩事故發生。如機構選擇在資訊系統中使用外掛程式，便應採取措施減少有關風險，包括僅從可信來源安裝外掛程式、對外掛程式進行定期的更新及漏洞檢測、進行有效的權限管理，並檢視機構本身在資料保安方面已經採取的機構性及技術性措施是否足夠對應使用外掛程式所帶來的額外風險。

Case 2

Unauthorised access to membership database – DPP 4 – security of personal data

Background

An educational institution (the Institution) reported to the PCPD that a hacker had exploited a security vulnerability of its plugin software to gain unauthorised access to a membership database on its web server, thereby exfiltrating the personal data of around 1,000 members, including their names, addresses, email addresses, and mobile phone numbers.

Remedial Measures

Upon receipt of the notification from the Institution, the PCPD initiated a compliance check and provided recommendations to the Institution to ensure compliance with the provisions of the PDPO. In response to the incident, the Institution suspended the use of the plugin software and ceased storing personal data in the database involved. In addition, the Institution conducted a review on all its plugin source code and patched the vulnerabilities, along with the deployment of a monitoring mechanism on the change of data in the membership database.

Lessons Learnt

While plugin software brings benefits and convenience to information systems, it also increases the risks of information security, including security vulnerabilities, malicious code and improper access control, which may lead to data breach incidents. Organisations with plugin software incorporated in their information systems should take measures to minimise such risks, including installing plugin software only from trusted sources, performing periodic updates and vulnerability scanning exercises for the plugin software, implementing effective access control, and evaluating whether the organisational and technical measures for data security that are originally in place are adequate to mitigate the extra risks associated with the use of plugin software.

個案三

一名寵物美容公司前員工利用現職員工的帳戶存取網上零售系統 — 保障資料第4原則 — 個人資料的保安

背景

一間寵物美容公司(該公司)向私隱專員公署通報，指一名前員工多次利用其他現職員工的帳戶，登入載有過千名客戶個人資料的網上零售系統(該系統)，並向有關客戶發出訊息，邀請他們光顧另一間寵物美容公司。涉及的個人資料包括姓名、香港身份證號碼、出生日期、電郵地址、電話號碼、僱傭資料及社交媒體帳戶資料。

該事件源於該公司在設立員工帳戶時，以員工的電話號碼預設為帳戶密碼，並僅以口頭方式提醒員工須在首次登入帳戶後自行更改密碼。由於該前員工知悉該公司的密碼管理模式，故在離職後仍能利用其他員工的帳戶密碼(亦即員工的電話號碼)遙距登入該系統。

補救措施

收到該公司的通報後，私隱專員公署展開循規審查，並就《私隱條例》的相關規定向該公司提供建議。為避免類似事件再次發生，該公司已更改所有員工的帳戶密碼，而所有員工須每半年在主管見證下更改密碼。此外，該公司將新員工帳戶的預設密碼改為由八位英文字母及數字隨機組成的密碼，亦禁止了該系統的遙距存取功能。

借鑑

在密碼管理方面，機構應避免以員工的個人資料(如姓名、出生日期、電話號碼等)作為預設密碼，並應實施有效措施以管理用戶密碼，包括強制密碼長度和複雜性、密碼歷史紀錄，並確保用戶遵循關於密碼保安的最佳行事方式。機構亦應考慮制定帳戶鎖定閾值策略來限制資訊及通訊系統允許登入失敗的次數，並在達到次數上限時封鎖帳戶一段特定的時間。

Case 3

A former employee of a pet grooming company accessed the online retail system via the accounts of existing employees – DPP 4 – security of personal data

Background

A pet grooming company (the Company) reported to the PCPD that a former employee had accessed its online retail system (the System), which contained the personal data of more than a thousand customers, by using the login credentials of existing employees. The former employee subsequently sent messages to the customers inviting them to patronise another pet grooming company. The personal data involved included names, HKID Card numbers, dates of birth, email addresses, telephone numbers, employment records, and social media account information.

The Company revealed that the phone numbers of employees were used as default account passwords during account creation of the System. The employees, however, were verbally reminded to change the default passwords after the first login. The former employee, who was aware of the password management practice, exploited the passwords of other employees (i.e. their phone numbers) to gain remote access to the System after his departure from the Company.

Remedial Measures

Upon receipt of the notification from the Company, the PCPD initiated a compliance check and provided recommendations to the Company to ensure compliance with the provisions of the PDPO. To prevent the recurrence of similar incidents, the Company changed the account passwords of all employees, who would be further required to change their passwords under the witness of their supervisors on a half-yearly basis. In addition, randomly generated passwords comprising eight letters and numbers would be allocated to new recruits. Remote access to the System was also disabled.

Lessons Learnt

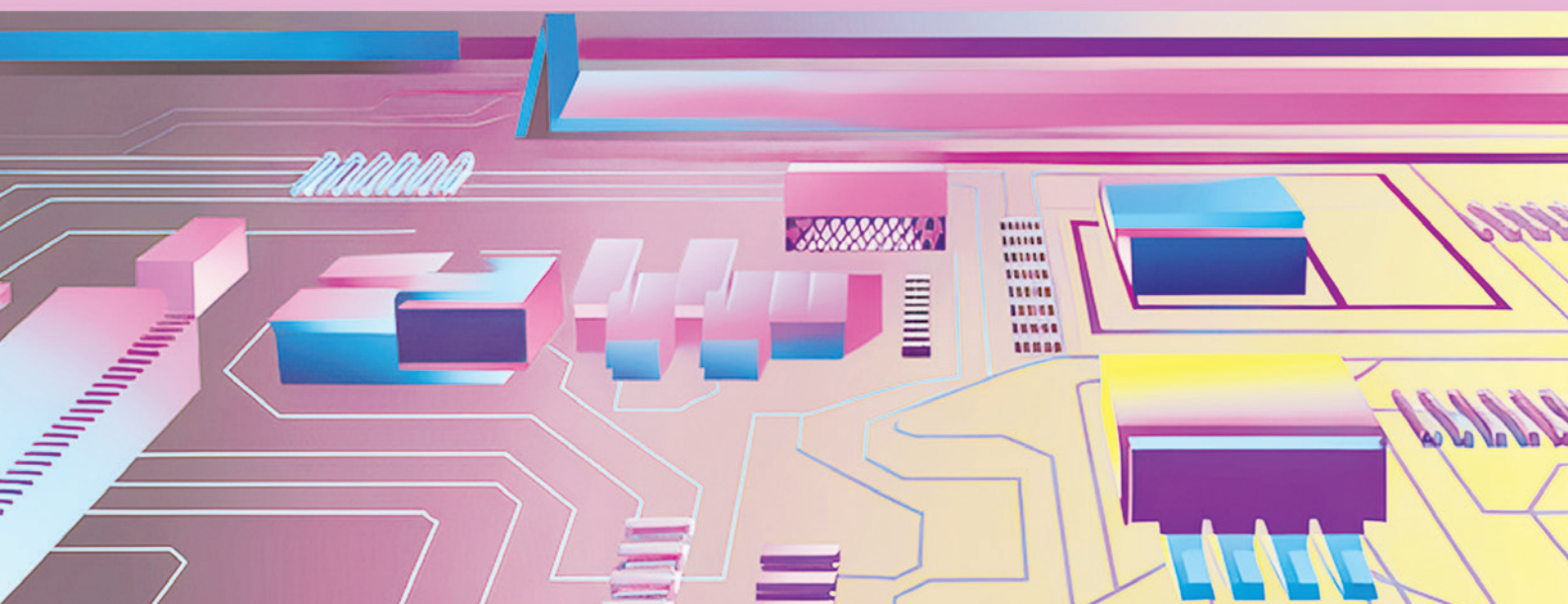
With regard to password management, organisations should avoid using personal data (such as names, dates of birth and phone numbers, etc.) of staff members as default account passwords and should implement effective measures to manage user passwords. This includes setting rules for password length, complexity, and history, and ensuring that users follow best practices for password security. Organisations should also consider setting an account lockout threshold policy to limit the number of failed logins to information and communications systems, and to lock out the user accounts for a pre-determined period of time when the threshold has been reached.



PCPD



H K





香港灣仔皇后大道東248號大新金融中心13樓1303室
Unit 1303, 13/F., Dah Sing Financial Centre,
248 Queen's Road East, Wanchai, Hong Kong

電話 Tel : 2827 2827
傳真 Fax : 2877 7026
電郵 E-mail : communications@pcpd.org.hk
網站 Website : www.pcpd.org.hk



私隱專員公署
網站
PCPD Website



下載本年報
Download this
Annual Report



本刊物使用署名4.0國際(CC BY 4.0)的授權條款，只要你註明原創者為香港個人資料私隱專員公署，便可自由分享或修改本刊物。詳情請瀏覽creativecommons.org/licenses/by/4.0/deed.zh-hant。

This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.