

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.

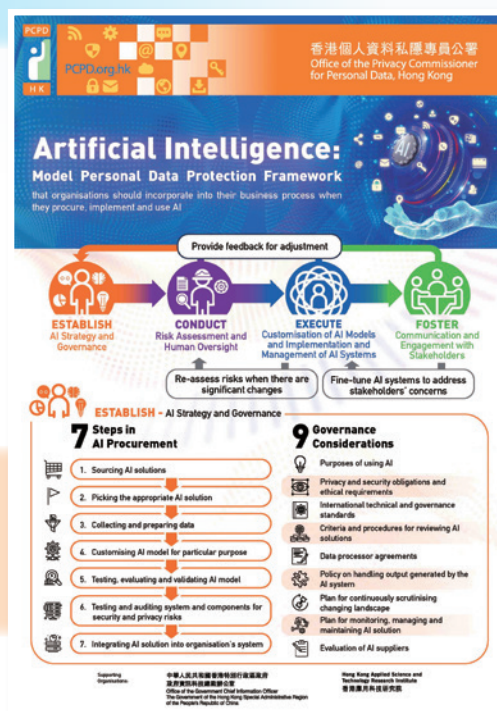
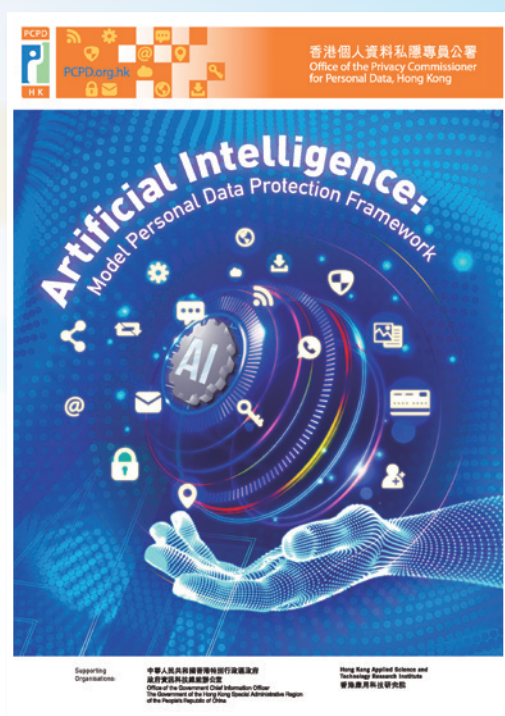


《模範框架》建基於一般業務流程，就「AI策略及管治架構」、「風險評估及人為監督」、「實行AI模型的定製與AI系統的實施及管理」，以及「促進與持份者的溝通及交流」等範疇，提供建議及最佳行事常規。

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.

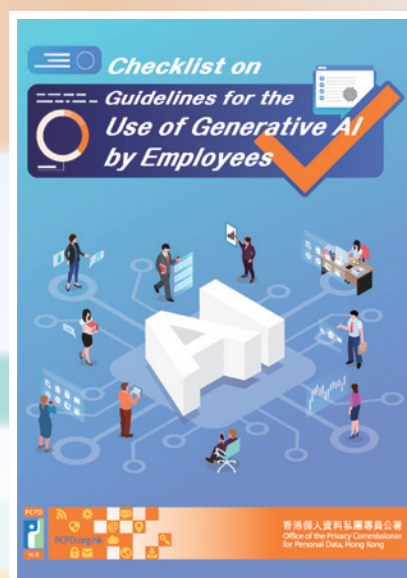


發布《僱員使用生成式AI的指引清單》

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.

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.

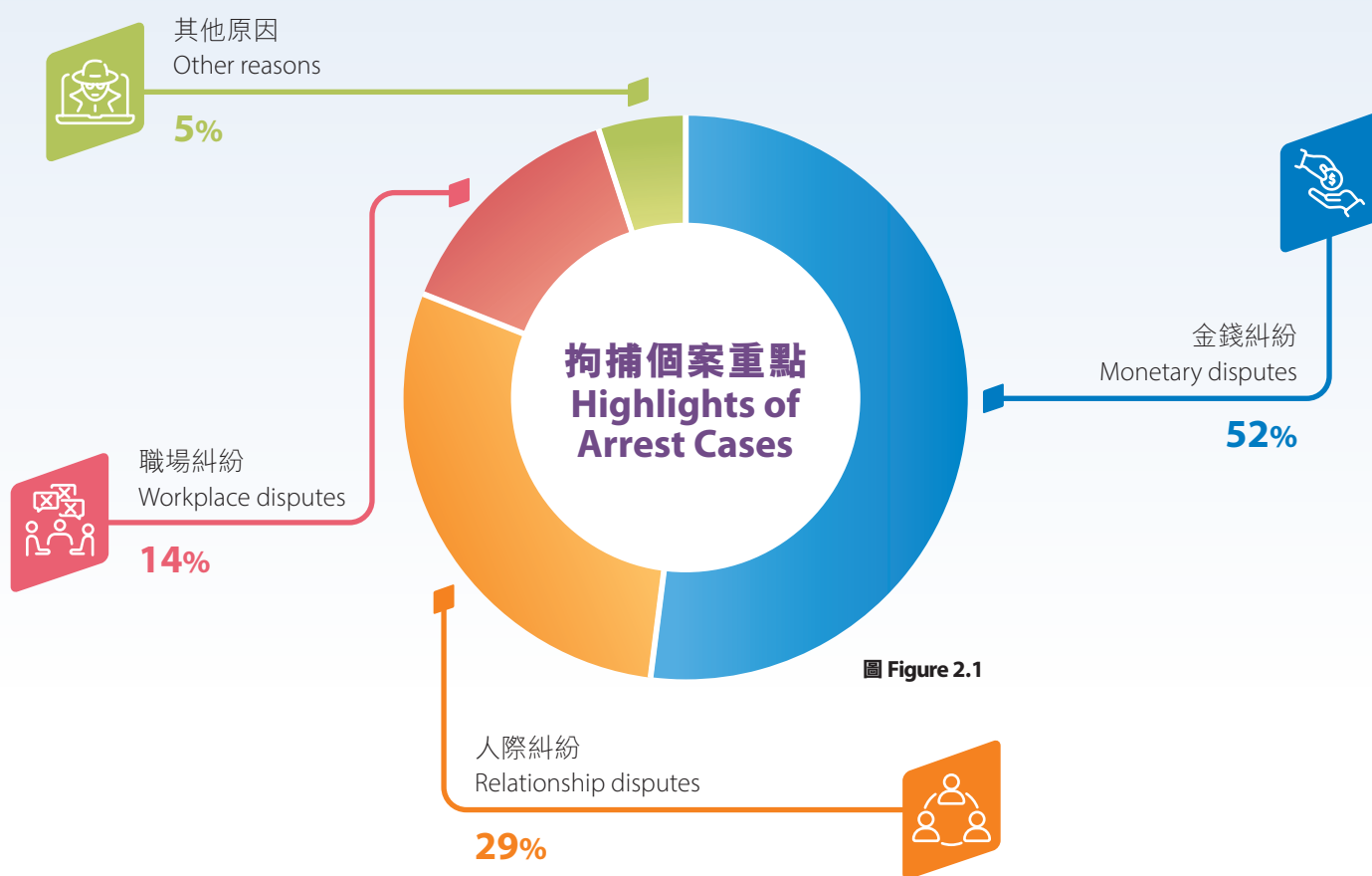


拘捕個案重點

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.

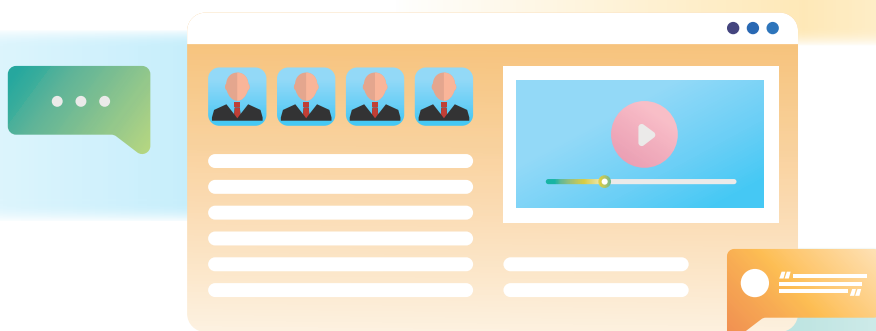
Below are four noteworthy cases involving custodial sentences:

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.

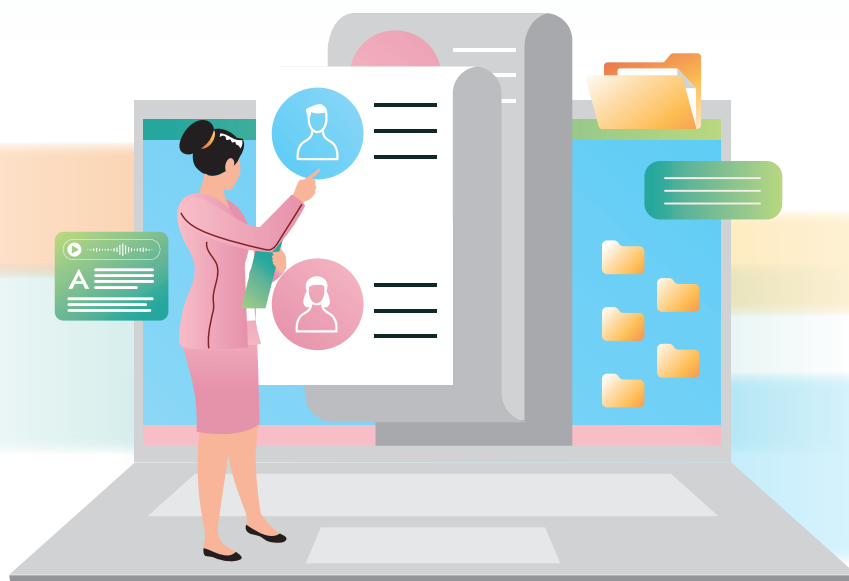


女子將一對母子「起底」

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

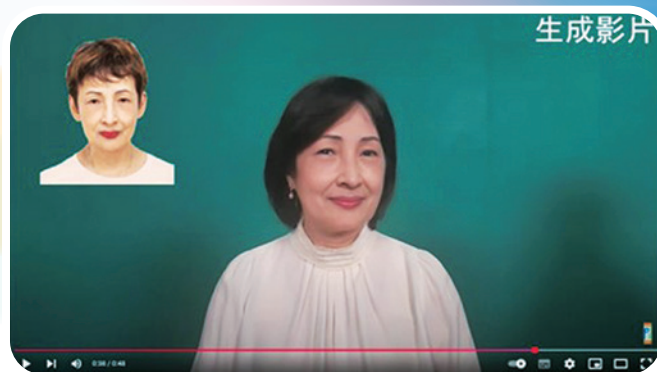
提高市民的防騙意識

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.

