# 合規
Compliance

## 回應公眾查詢

私隱專員公署在本報告年度接獲16,034宗查詢個案（圖2.1），比上年度增加了4.8%，平均每個月處理約1,300宗查詢個案，大部分（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%。

主要查詢類別為有關收集及使用個人資料的情況（例如：香港身份證號碼及／或副本）（30%）、私隱專員公署的投訴處理政策（9%）、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%）、安裝與使用閉路電視設備情況（5%）及《私隱條例》的應用（5%）。

有關誘騙個人資料的查詢持續增加，由上年度的732宗增至本年度的903宗，增幅為23%。本年度私隱專員公署接獲942宗關於「起底」的查詢，較2022-23年度的325宗增加近三倍。

## Responding to Public Enquiries

The PCPD received a total of 16,034 enquiry cases during the reporting year (Figure 2.1), an increase of 4.8% compared to the preceding reporting year. On average, around 1,300 enquiry cases were handled each month. The majority of the enquiries (84%) were made by telephone[1], while the percentages of enquiries made in writing and in person were 12% and 4% respectively.

The key areas of enquiries included the collection and use of personal data (e.g. Hong Kong Identity Card numbers and/or copies) (30%), the PCPD's complaint handling policy (9%), the handling of personal data in the context of employment (6%), the rights to access and correct personal data (6%), the installation and use of CCTV facilities (5%) and the application of the PDPO (5%).

The number of enquiries regarding personal data fraud continued to rise, from 732 in the preceding reporting year to 903 in this reporting year, representing an increase of 23%. The number of enquiries related to doxxing in this reporting year was 942, which was nearly a three-fold increase from 325 in the 2022-23 reporting year.

1 包括透過私隱專員公署的一般查詢熱線（2827 2827）、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）。

1 Including through the General Enquiries Hotline (2827 2827), 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

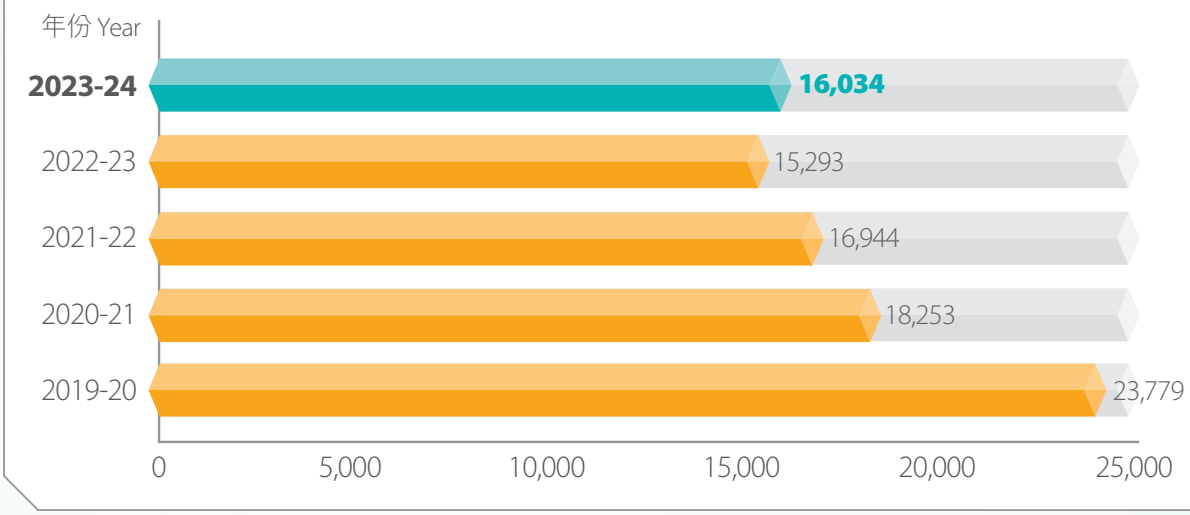



圖2.1
Figure 2.1

## 展開循規行動

當私隱專員公署發現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，私隱專員一般會向機構指出其行事方式與《私隱條例》規定不符或不足之處，並促請有關機構採取適當的補救措施，糾正違規的情況和採取預防措施，避免日後重蹈覆轍。

在報告年度內，私隱專員共進行了410次循規行動，較2022-23年度的383次多7%（圖2.2）。

## Initiating Compliance Actions

When the PCPD identifies that an organisation's practices may not comply with the requirements under the PDPO, the PCPD will initiate compliance checks or investigations. Upon completion of a compliance action, the Privacy Commissioner will generally inform the organisation of its non-compliant or deficient practices under the PDPO and urge it to take appropriate remedial measures to rectify the contraventions, and implement preventive measures to prevent the contraventions from recurring.

During the reporting year, the Privacy Commissioner carried out 410 compliance actions, an increase of 7% compared to 383 in 2022-23 (Figure 2.2).

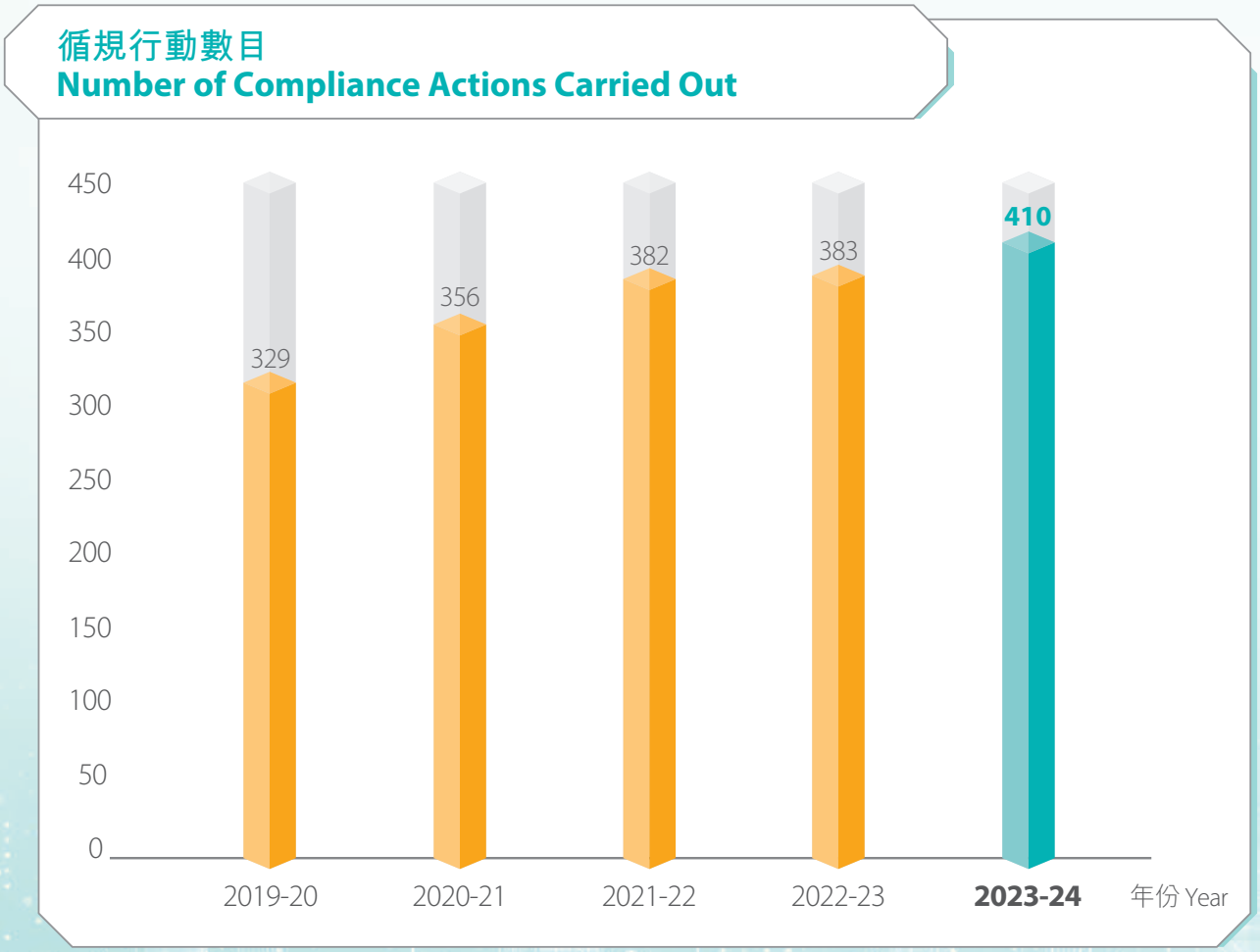



圖2.2
Figure 2.2

## 處理資料外洩事故通報

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資料當事人、私隱專員和其他相關人士。

在接獲資料外洩事故通報後，私隱專員公署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，並建議補救措施，改正其不足之處，以避免事故重演。

## Handling 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, data users are encouraged to notify the affected data subjects, the Privacy Commissioner and other relevant parties upon the occurrence 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 the initiation of a compliance check on or an investigation into the organisation involved. Upon completion of the compliance actions, the Privacy Commissioner would generally identify deficiencies of the data users and provide recommendations for remedial measures to rectify the deficiencies and to prevent recurrence of such incidents.

在報告年度內，私隱專員公署接獲169宗資料外洩事故通報（50宗來自公營機構、119宗來自私營機構），涉及約90萬名人士的個人資料。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、意外銷毀個人資料，以及系統錯誤設定等。公署對每宗事故均展開了循規審查或調查（圖2.3）。

During the reporting year, the PCPD received a total of 169 data breach notifications (50 from the public sector and 119 from the private sector), involving the personal data of around 900,000 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 of personal data by employees, accidental erasure of personal data and system misconfiguration. The PCPD conducted a compliance check on or an investigation into each of these 169 incidents (Figure 2.3).

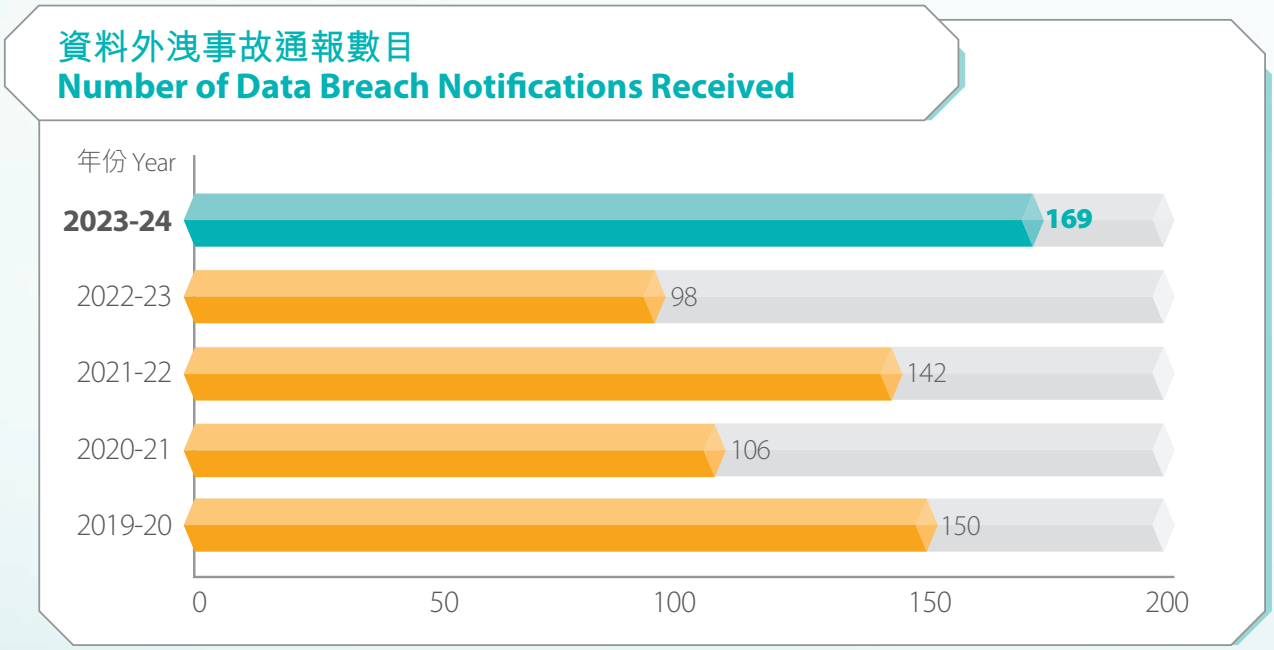



**圖2.3**
**Figure 2.3**

## 循規調查

在報告年度內，私隱專員發表了兩份有關資料外洩事故的調查報告。

### 一個網購平台的資料外洩事故

一個網購平台向私隱專員公署通報，發現一個網上論壇一則銷售訊息聲稱可出售該平台260萬名用戶的個人資料，包括324,232個香港用戶帳號的個人資料。該網購平台表示該資料外洩事故源於2022年1月系統遷移過程中出現的一個保安漏洞。私隱專員就事件展開調查。

私隱專員經調查後認為事件是由該網購平台以下的缺失導致：

(1) 未有在系統遷移前進行私隱影響評估；

(2) 不全面的編碼覆檢程序；

(3) 與系統遷移有關的安全評估有缺失；

(4) 欠缺與編碼覆檢程序相關的書面政策；及

(5) 欠缺有效的偵測措施。

## Compliance Investigations

During the reporting year, the Privacy Commissioner published two investigation reports in relation to data breach incidents.

### A Data Breach Incident of an Online Shopping Platform

An online shopping platform reported to the PCPD after discovering that a listing posted on an online forum offered for sale the personal data of its 2.6 million users, which included the personal data of 324,232 user accounts in Hong Kong. The online shopping platform stated that the data breach incident was caused by a security vulnerability that was introduced during a system migration in January 2022. The Privacy Commissioner initiated an investigation into the incident.

Upon conclusion of her investigation, the Privacy Commissioner considered that the incident had been caused by the following deficiencies of the online shopping platform:

(1) Failure to conduct a privacy impact assessment prior to the system migration;

(2) Incomprehensive code review process;

(3) Inadequate security assessment associated with the system migration;

(4) Lack of a written policy in relation to the code review process; and

(5) Lack of effective detection measures.

鑑於其缺失，私隱專員認為該網購平台沒有採取所有切實可行的步驟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。私隱專員向該網購平台送達執行通知，指示其糾正以及防止有關違規情況再次發生。

In the light of the deficiencies, the Privacy Commissioner considered that the online shopping platform had not taken 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 online shopping platform to direct it to remedy and prevent recurrence of the contravention.

私隱專員建議機構若要遷移涉及個人資料的資訊系統，應採取以下措施加強數據安全：

The Privacy Commissioner made the following recommendations on strengthening data security to organisations which may perform information system migration involving personal data:

- 進行私隱影響評估，特別是當系統或行事方式出現重大改變及引入新科技時進行有關評估；
- Carry out privacy impact assessments, especially when significant changes are made to systems or practices and upon the adoption of new technologies;
- 制訂確保數據安全的遷移計劃；
- Develop a migration plan that prioritises data protection;
- 進行有效的漏洞評估；
- Conduct effective vulnerability assessments;
- 提供相關的員工培訓；
- Provide relevant employee training;
- 實施有效的檢測機制偵測異常活動；及
- Implement an effective mechanism for detecting abnormal activities; and
- 制訂地區性政策及程序，確保遵從《私隱條例》的規定。
- Formulate localised policies and procedures to ensure compliance with the PDPO.

## 某公營機構的資料外洩事故

一間公營機構向私隱專員公署通報，指其電腦系統及檔案伺服器遭勒索軟件攻擊及惡意加密，導致超過13,000名資料當事人的個人資料外洩，當中約四成受影響人士為求職者及已離職的僱員。

私隱專員經調查該資料外洩事故後認為事件是由該機構以下的缺失導致：

(1) 資訊系統欠缺有效針對惡意攻擊的偵測措施，令黑客能成功獲取具管理員權限的帳戶憑證；

(2) 沒有為遠端存取資料啟用多重認證功能，導致黑客能利用獲取的帳戶憑證透過遠端桌面連接進入該機構的網絡；

(3) 對資訊系統進行的保安審計不足；

(4) 資訊保安政策有欠具體；及

(5) 約四成受影響人士的個人資料被不必要地保留。

## A Data Breach Incident of a Public Body

A public body reported to the PCPD that its computer systems and file servers had been attacked by ransomware and maliciously encrypted. The incident resulted in the leakage of the personal data of more than 13,000 data subjects, about 40% of whom were unsuccessful job applicants and former employees.

Upon conclusion of her investigation into the data breach incident, the Privacy Commissioner considered that the incident had been caused by the following deficiencies of the public body:

(1) Lack of effective detection measures against malicious attacks, allowing the hacker to obtain the credentials of user accounts with administrative privileges;

(2) Failure to enable multi-factor authentication for remote access to data, allowing the hacker to gain access to its network through a remote desktop connection using the credentials of a user account;

(3) Insufficient security audits of the information systems;

(4) Lack of specificity in the information security policy; and

(5) Unnecessary retention of the personal data of around 40% of the affected individuals.

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(i)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(ii)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。

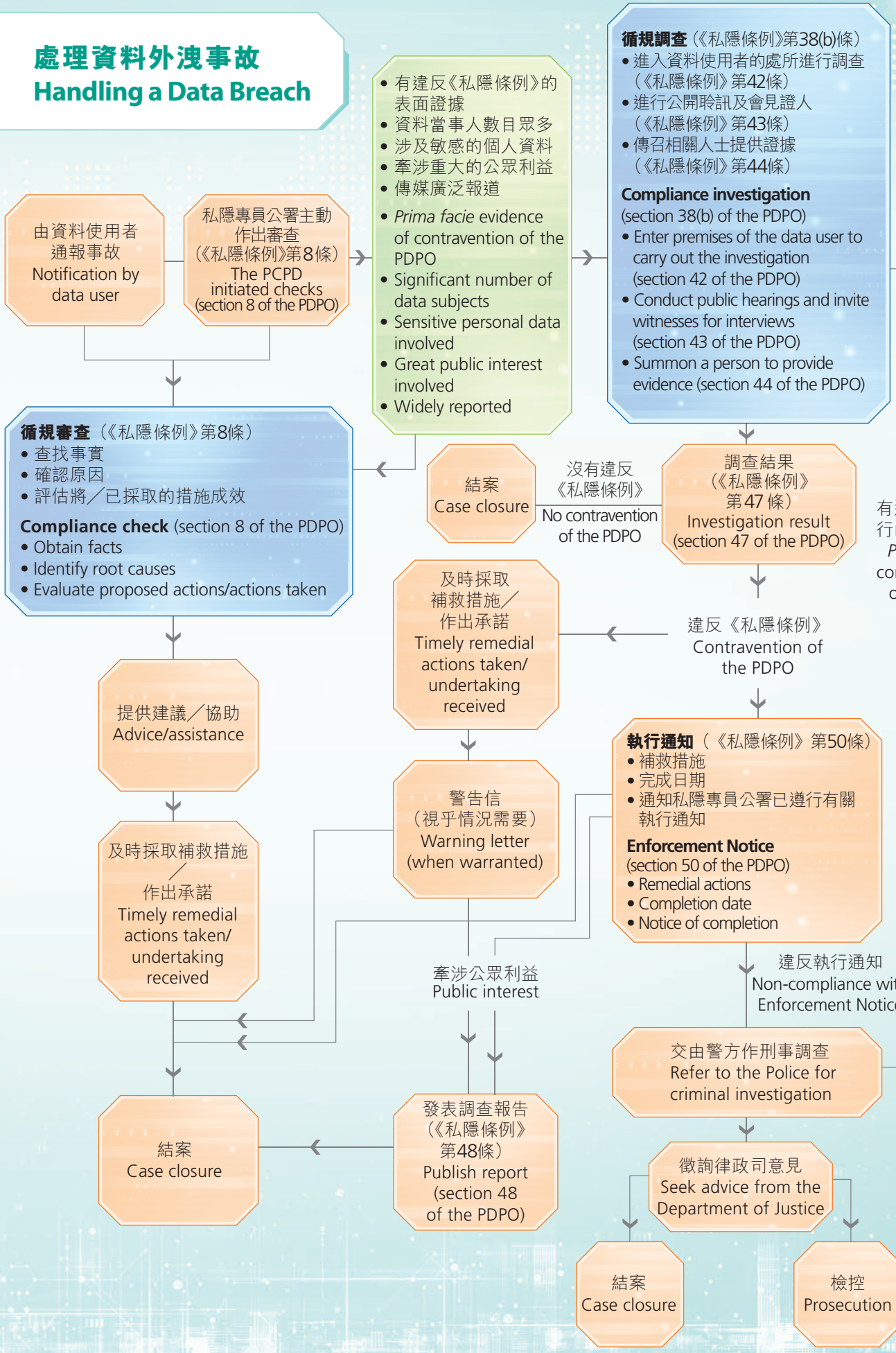
In the circumstances, the Privacy Commissioner considered that the public body had not taken all practical steps to ensure that the personal data involved was (i) protected against unauthorised or accidental access, processing, erasure, loss or use; and (ii) not kept longer than was necessary for the 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 public body to direct it to remedy and prevent recurrence of the contravention.

私隱專員向使用資訊及通訊科技處理個人資料的機構作出以下建議：

The Privacy Commissioner made the following recommendations to organisations which use information and communications technologies for processing personal data:

- 設立個人資料私隱管理系統並委任保障資料主任；
- Establish a Personal Data Privacy Management Programme and appoint data protection officer(s);
- 建立穩健的網絡保安框架；
- Establish a robust cybersecurity framework;
- 適時對資訊系統進行風險評估及保安審計；
- Conduct timely risk assessments and security audits of information systems;
- 建立重視資訊安全的企業文化；及
- Establish a corporate culture that values information security; and
- 適時刪除個人資料。
- Delete personal data in a timely fashion.

# 處理資料外洩事故
# Handling a Data Breach



## 進行視察

私隱專員公署一直致力就各界遵守《私隱條例》規定作出監察及監管，包括行使《私隱條例》第36條的權力，派員到持有大量市民個人資料的機構，實地視察其資料系統。在報告年度內，私隱專員發表了兩份視察報告。

## Conducting Inspections

The PCPD is committed to monitoring and supervising compliance with the requirements of the PDPO, including exercising the powers under section 36 of the PDPO to carry out site inspections of the data systems of organisations which handle a vast amount of personal data. During the reporting year, the Privacy Commissioner published two inspection reports.

## 某政府部門的個人資料系統

視察結果顯示，該政府部門致力實施個人資料私隱管理系統，為保障個人資料私隱建立了穩健的基礎，並持續評估及監督該系統以確保符合《私隱條例》的要求。私隱專員於視察報告中向該政府部門提出10項建議，以加強其持有的個人資料的保安。

此外，私隱專員強烈鼓勵該部門繼續努力向全體員工灌輸和維持一個優良的資料保障文化，以加強對持份者個人資料的私隱保障及保安，並展示該部門對良好數據管治及與公眾建立信任的決心。

## Personal Data System of a Government Department

The findings of the inspection revealed that the government department had made significant efforts to implement a Personal Data Privacy Management Programme and had built a robust infrastructure to protect personal data privacy, which was supported by an ongoing review and monitoring process to facilitate compliance with the requirements under the PDPO. The Privacy Commissioner also made 10 recommendations to the government department in the inspection report with a view to enhancing the security of the personal data held by the department.

In addition, the Privacy Commissioner strongly encouraged the government department to continuously strive to instil and maintain a strong culture of data protection among all staff members to better protect the privacy and security of the personal data of its stakeholders and demonstrate its commitment to good data governance and building trust with members of the public.

## 一間虛擬銀行的客戶個人資料系統

視察結果顯示，該銀行建立了個人資料私隱管理系統並委任專職的保障資料主任，有系統並負責任地建立一套遵從《私隱條例》規定的制度，循規地管理客戶的個人資料。此外，私隱專員欣悉該銀行透過實行無紙化辦公環境、舉行防範釣魚襲擊威脅的演習活動，以及推動私隱友善辦公文化等措施，致力保障個人資料私隱。整體來說，私隱專員認為該銀行在處理客戶個人資料上大致符合《私隱條例》中附表1保障資料原則的規定。

雖然如此，私隱專員建議該銀行加強對資料處理者的管理、提升資料遺失防護系統的監察能力、限制員工查閱客戶個人資料的時間、集中管理處理個人資料的內部政策及指引，並持續定期檢視其個人資料系統，以加強對客戶個人資料的保障。

## Personal Data System of a Virtual Bank

The findings of the inspection revealed that the bank had established a Personal Data Privacy Management Programme and appointed a dedicated Data Protection Officer to systematically and responsibly develop a system to comply with the requirements the PDPO and to manage customers' personal data. In addition, the Privacy Commissioner was pleased to note that the bank had been committed to protecting personal data privacy through measures such as implementing a paperless office, conducting drill exercises to prevent the threat of phishing attacks and promoting a culture of privacy in the workplace. Overall, the Privacy Commissioner considered that the bank had generally adhered to the requirements of DPPs of Schedule 1 to the PDPO in the handling of customers' personal data.

Nevertheless, the Privacy Commissioner recommended the bank to strengthen the management of its data processors, enhance the monitoring capabilities of the data loss prevention system, limit the time for staff members to access customers' personal data, centrally manage its internal policies and guidelines on the handling of personal data, and continuously and regularly review its personal data system so as to strengthen the protection of customers' personal data.

## 處理核對程序申請

核對程序是指以電子方法比較兩套因不同目的而收集的個人資料，每一項比較涉及10名或以上資料當事人的資料，而核對得出的結果可用作對有關資料當事人採取不利行動的程序。資料使用者如無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37宗核對程序申請。經審閱後，私隱專員在加入附加條件後批准了36宗申請，一宗申請不屬《私隱條例》訂明的核對程序而不獲批准。

## Processing Matching Procedure Requests

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. The result of the comparison may be used for taking adverse action against the data subjects concerned. A data user shall not carry out a matching procedure without the prescribed consent from all data subjects involved or the consent of the Privacy Commissioner.

During the reporting year, the PCPD received a total of 37 applications to carry out matching procedures. After vetting, the Privacy Commissioner approved 36 of these applications, with conditions imposed, and rejected one application which was found not to be a matching procedure as defined under the PDPO.

## 推廣合規

### 發表《數碼時代的私隱保障：比較十大網購平台的私隱設定》報告及出版《使用網購平台的保障私隱貼士》單張

公眾對網上購物已習以為常，網購為消費者帶來便利及好處，卻存在個人資料私隱的風險。在2023年6月，私隱專員公署發表《數碼時代的私隱保障：比較十大網購平台的私隱設定》報告，當中檢視及評估了10個本地消費者常用的網購平台（即Baby Kingdom — BKmall、Carousell、eBay、Fortress、HKTVmall、京東、PlayStation App、Price.com.hk香港格價網、Samsung及淘寶）的私隱設定，以了解有關平台收集及使用用戶個人資料的情況。

私隱專員公署根據檢視結果，向網購平台營運商提供保障用戶私隱的具體建議，包括允許用戶以訪客身分購物並僅收集處理交易所需的個人資料、將所有與私隱有關的選項預設為保障用戶私隱的選項，以及提高追蹤用戶活動的透明度。同時，公署出版了《使用網購平台的保障私隱貼士》單張，向網購平台用戶提供安全網購及保障個人資料私隱的貼士，包括僅提供完成註冊及交易所需的最少量資料、注意直接促銷相關的設定、刪除不再使用的帳戶等。

## Promoting Compliance

### Release of Report on "Privacy Protection in the Digital Age: A Comparison of the Privacy Settings of 10 Online Shopping Platforms" and Publication of Leaflet on "Tips for Users of Online Shopping Platforms"

Online shopping has become an integral part of daily life for many people. While online shopping offers convenience and benefits to consumers, it also poses risks to personal data privacy. In June 2023, the PCPD released a report on "Privacy Protection in the Digital Age: A Comparison of the Privacy Settings of 10 Online Shopping Platforms", which covered a review and assessment of the privacy settings of 10 online shopping platforms commonly used in Hong Kong (namely, Baby Kingdom – BKmall, Carousell, eBay, Fortress, HKTVmall, JD.COM, PlayStation App, Price.com.hk, Samsung and Taobao), to understand how these online shopping platforms collect and use the personal data of their users.

Based on the review findings, the PCPD provided specific advice to the operators of online shopping platforms regarding protection of the users' personal data. This included allowing users to shop as guests and only collecting personal data necessary to process transactions, setting all privacy-related options to protect user privacy by default, and increasing transparency in tracking users' activities. Simultaneously, the PCPD published a leaflet on "Tips for Users of Online Shopping Platforms", which provided advice to users of online shopping platforms about how to carry out online shopping safely while protecting their personal data privacy, including, for example, only providing the minimum amount of personal data required for registration and transactions, and paying attention to direct marketing settings and deleting unused accounts.

## 發表《電子點餐的私隱關注》報告及出版《在餐廳使用手機應用程式或二維碼點餐的保障私隱貼士》單張

隨着電子點餐漸趨普及，私隱專員公署在2024年1月發表《電子點餐的私隱關注》報告。公署派員走訪了60間向顧客提供手機應用程式或二維碼自助點餐的本地餐廳，實測有關餐廳在提供電子點餐服務時收集及使用顧客個人資料的情況。

私隱專員公署根據檢視結果，就加強電子點餐相關的個人資料保護，向飲食業界提供具體建議，包括向顧客提供其他不涉及收集個人資料的點餐方式，或按實際所需收集最少量的個人資料，使用顧客的個人資料作直接促銷前須徵求其同意，並不應預設該選項為「同意」。

## Release of Report on "Privacy Concerns on Electronic Food Ordering at Restaurants" and Publication of Leaflet on "Food Ordering Using Mobile Apps or QR Codes at Restaurants: Tips for Protecting Privacy"

With the increasing prevalence of electronic ordering services, the PCPD released a report on "Privacy Concerns on Electronic Food Ordering at Restaurants" in January 2024. The PCPD's representatives paid visits to 60 local restaurants which allowed customers to order food by using a mobile application or scanning a QR code, and carried out tests on the collection and use of customers' personal data by the restaurants concerned in the provision of electronic food ordering services.

According to the review results, the PCPD provided specific recommendations to the food and beverage industry regarding enhancing personal data protection when using electronic ordering services. The suggestions included providing alternative food ordering means to customers without collecting their personal data or collecting a minimal amount of personal data as needed, and seeking customers' consent to use their personal data for direct marketing purposes, in which the setting for options should not be set as "agree" by default.

與此同時，私隱專員公署出版了《在餐廳使用手機應用程式或二維碼點餐的保障私隱貼士》單張，向市民提供保障私隱的建議，包括考慮是否僅為堂食點餐功能而使用應用程式並開立帳戶、以訪客身分點餐時須考慮所需個人資料的類別是否必須，及是否可以在不提供有關資料的情況下仍可點餐等。

At the same time, the PCPD published a leaflet on "Food Ordering Using Mobile Apps or QR Codes at Restaurants: Tips for Protecting Privacy" to provide advice to citizens about privacy protection. Citizens are advised to consider whether to use the mobile apps and create an account solely for restaurant dining purposes, whether the types of personal data to be collected are necessary when ordering as a guest, as well as whether the order could be placed without providing such data, etc.