附錄
Appendices

附錄一 Appendix 1
保障資料原則 Data Protection Principles

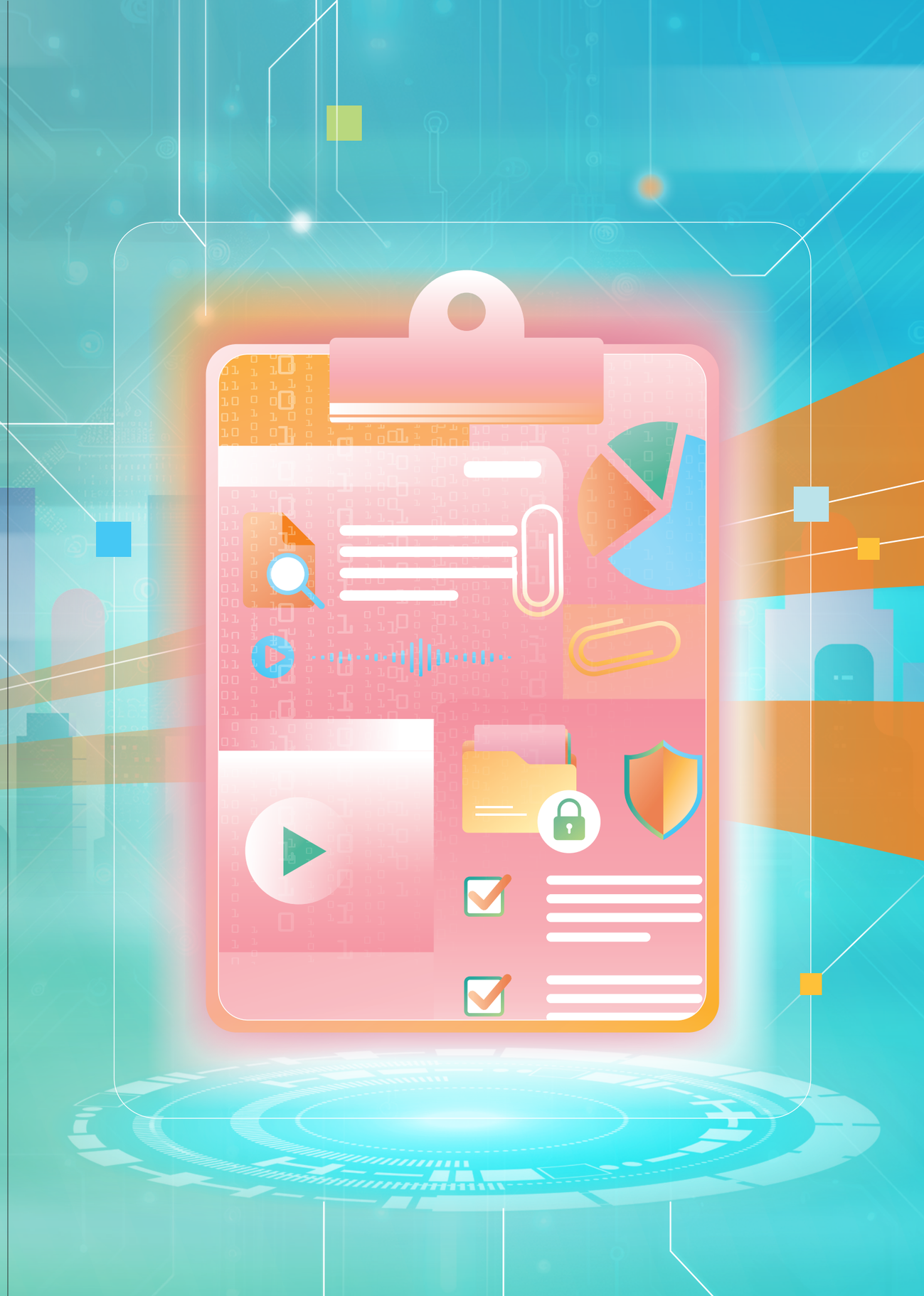
附錄二 Appendix 2
服務承諾 Performance Pledge

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周期。

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.

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。

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.

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 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實際所需。

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：	**彭耀鴻資深大律師(副主席) Mr Robert PANG Yiu-hung, SC (Deputy Chairman)**
Coram:	**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)
裁決理由書日期：	**2024年6月18日**
Date of Decision:	**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.

（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。

（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。

（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。

（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。

(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.

(3) There was insufficient evidence to show that the Personal Data Concerned was leaked from the Department and the Agency in this case.

(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.

(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.

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:

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)

裁決理由書日期：
Date of Decision:

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。

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.

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 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。

(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） 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。

(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。

The AAB's Decision

The appeal was dismissed.

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

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

吳穎軒時任高級律師代表私隱專員

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

投訴人（受到遭上訴所反對的決定所約束的人）缺席聆訊

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:**	**劉恩沛資深大律師（副主席） Ms LAU Queenie Fiona, SC (Deputy Chairman)** **張璟瑋工程師（委員） Ir Jason CHEUNG King-wai (Member)** **許繼偉教授（委員） Prof. HUI Kai-wai (Member)**
裁決理由書日期： **Date of Decision:**	**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：	**馬淑蓮女士（副主席） Ms Jay MA Suk-lin (Deputy Chairman)**
Coram:	**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)
裁決理由書日期：	**2024年12月16日**
Date of Decision:	**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。

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.

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。

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.

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。

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。

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.

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。

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。

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。

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。

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 latters' posting of doxxing messages in the said group.

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.

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。

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.

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。

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.

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。

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

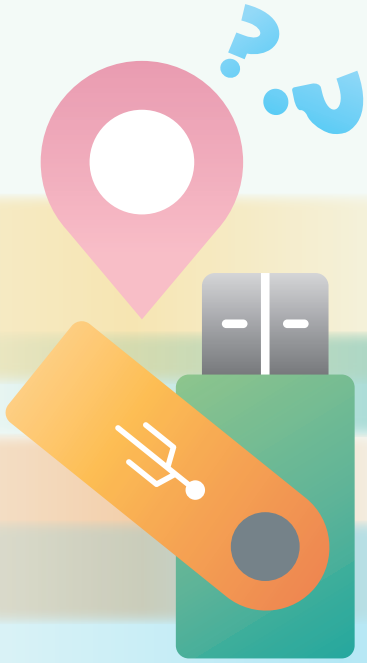
便攜式儲存裝置雖然提供一個便捷的方法儲存和轉移資料至機構系統以外的地方，但這會增加資料外洩的風險。機構應在切實可行的範圍內，避免使用便攜式儲存裝置來儲存個人資料。如有必要使用便攜式儲存裝置，應制定政策列明允許使用有關裝置的情況、可轉移到有關裝置的個人資料類別和數量、使用便攜式儲存裝置的審批程序等。機構亦應保存這類便攜式儲存裝置的清單及追蹤其使用情況和位置，並在每次使用後妥善地刪除當中的資料。

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