附 錄

Appendix

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。所有使用個人資料的人士(資料使用者)須依從《私隱條例》核心的六項保障資料原則。該六項原則涵蓋了個人資料由收集、保存、使用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.

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，其目的應直接與其職能或活動有關。
- 須以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。
- 收集的資料是有實際需要的，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.

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 practical 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.

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操控個人資料的收集、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4原則 — 資料保安原則

- 資料使用者須採取切實可行的步驟，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 practical 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 make generally available its personal data policies and practices, 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，私隱專員公署在三個範疇內(包括處理公眾查詢、投訴及法律協助計劃申請)的工作表現均高於服務指標，其中五個項目的所有個案更達到100%的服務水平。

私隱專員公署於兩個工作日內完成回覆電話查詢及確認收到書面查詢的比率為100%，並能夠於28個工作日內詳細回覆書面查詢。

至於處理公眾投訴方面，私隱專員公署在收到投訴後兩個工作日內發出認收通知的比率為99%(服務指標為98%)。此外，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%)。

在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，以及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 three categories (including the handling of public enquiries, complaints and applications for legal assistance) exceeded the performance target. All cases in five items even reached a 100% service standard.

The PCPD completed all replies to telephone enquiries and acknowledgements of written enquiries within two working days of receipt. All substantive replies to written enquiries were completed within 28 working days of receipt.

Regarding the handling of public complaints, the PCPD issued acknowledgement receipts within two working days of receipt in 99% of the 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%).

When handling applications for legal assistance, acknowledgement receipts were issued within two working days of receipt of all applications. All applicants were informed of the outcome within three months after submitting all the 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				
			2018	2019	2020	2021	2022
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%	100%	99%	99%	99%	99%
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%	96%	99%	99%	99%	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%	100%	100%	不適用[2] N/A[2]	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%	83%	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。
Time starts to run from the date on which the complaint is formally accepted as a complaint 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(一)

(行政上訴案件第26/2016號)

查閱資料要求 — 口頭通知查閱資料要求的結果 — 採取糾正措施 — 正確行使酌情權拒絕對投訴進行調查 — 進一步調查不能合理地預計可帶來更滿意的結果

Appeal Case Note (1)

(AAB Appeal No. 26 of 2016)

Data access request (DAR) – data subject was informed of the result of the request orally – remedial measures taken – the Privacy Commissioner's discretion not to further investigate the complaint duly exercised – further investigation cannot reasonably be expected to bring about a more satisfactory result

聆訊委員會成員:	**彭耀鴻資深大律師(主席) Mr Robert PANG Yiu-hung, SC (Chairperson)**
Coram:	**潘詠賢女士(委員) Ms Peggy POON Wing-yin (Member)**
	曾慕秋先生(委員) Mr TSANG Mo-chau (Member)
裁決理由書日期:	**2022 年 10 月 24 日**
Date of Decision:	**24 October 2022**

投訴內容

上訴人向政府部門(該部門)提交查閱資料要求,以索取(i)上訴人於指明期間寄出的信函紀錄,及(ii)上訴人於某日提交的陳述書。根據該部門答覆,該部門曾口頭告知上訴人該部門並無持有上訴人要求的(ii)陳述書,而上訴人所要求的(i)信函紀錄複本已備妥,並可在繳費後提供予上訴人。同日,該部門向上訴人發出信函告知其上述事項。在上訴人清繳有關費用後,該部門於同日向上訴人提供上述要求的文件(i)的複本。

The Complaint

The appellant made a DAR to a government department (Department) for a copy of (i) his outward mail record during a specific period and (ii) his submission of a certain date. According to the Department, the appellant was verbally informed that it did not possess item (ii) but a copy of item (i) was ready for collection upon payment of a fee. On the same day, the Department issued a letter to the appellant informing him of the aforesaid information. Upon subsequent payment of the fee, the Department provided the requested document (i) to the appellant on the same day.

上訴人其後表示並未有收到該部門發出的上述信函，故投訴該部門未有以書面方式通知其並無持有所要求的文件(ii)。

私隱專員的決定

經調查後，私隱專員認為未有足夠證據判斷上訴人曾經或未曾收到上述信函，故沒有足夠資料顯示該部門違反《私隱條例》第19(1)條的規定。就此，私隱專員引用《私隱條例》第39(2)(d)條賦予的酌情權拒絕對上訴人的投訴作進一步調查。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

上訴

委員會確認私隱專員的決定，並基於下述理由駁回該上訴：

(1) 在本案之中，委員會認同沒有足夠的證據證明該部門未有將上述信函交予上訴人。即使該部門沒有將上述信函交給上訴人，有關過錯純屬技術上的過錯，而該部門亦已於當日口頭通知上訴人並未有持有文件(ii)。

The appellant denied receiving the aforesaid letter and made a complaint against the Department for failing to inform him in writing that it did not hold the requested document (ii).

The Privacy Commissioner's Decision

Upon investigation, the Privacy Commissioner considered that there was insufficient evidence to assess whether the appellant had or had not received the said letter, and thus decided that there was insufficient information to show that the Department had breached section 19(1) of the PDPO. The Privacy Commissioner exercised the discretion provided by section 39(2)(d) of the PDPO to reject further investigation into the appellant's complaint. Dissatisfied with the Privacy Commissioner's decision, the appellant lodged an appeal with the Administrative Appeals Board (AAB).

The Appeal

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

(1) There was insufficient evidence to suggest that the Department did not pass the said letter to the appellant in this case. Even if the Department had omitted to pass the said letter to the appellant, it would have been considered only a technical breach, as the Department had already informed the appellant verbally that it did not possess item (ii) on the same day.

(2) 由於該部門已採納新措施以免日後發生同樣的爭拗，而有關上訴人所指的失誤亦未有對上訴人造成任何損害或不便，因此委員會認為私隱專員在此情況下可根據《私隱條例》第39(2)(d)條終止調查。

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
程潔美律師代表私隱專員

政府律師李希迦代表該政府部門（受到遭上訴所反對的決定所約束的人）

(2) Given that the Department had already taken new measures to avoid similar disputes in the future and the appellant had not suffered any loss or damage, the AAB considered that the discretion under section 39(2)(d) to end the investigation was properly exercised under the circumstances.

The AAB's Decision

The appeal was dismissed.

The appellant appeared in person
Ms Catherine CHING, Legal Counsel, represented the Privacy Commissioner
Ms Rachel LI, Government Counsel, represented the Government Department (the Person bound by the decision appealed against)

附錄三
Appendix 3

上訴個案簡述(二)

(行政上訴案件第5及第6/2021號)

法人身分不是成為《私隱條例》所定義的資料使用者的先決條件 — 按資料使用者指示行事的代理不屬《私隱條例》下的資料使用者 — 沒有證據支持上訴人提出的指稱及正確行使酌情權拒絕對投訴作進一步調查

Appeal Case Note (2)

(AAB Appeal Nos. 5 & 6 of 2021)

Not a prerequisite for a data user under the PDPO to be incorporated – an agent acting on the instructions of a data user is not a data user under the PDPO – the appellant's allegations were not supported by any evidence and the Privacy Commissioner's discretion not to further investigate the complaint duly exercised

聆訊委員會成員:	**張金良先生(主席) Mr CHEUNG Kam-leung (Chairperson)**
Coram:	**趙恒美女士(委員) Ms Mary Grace CHIU Hang-mei (Member)**
	唐以恒先生(委員) Mr TONG Yee-hang (Member)
裁決理由書日期:	**2022 年 4 月 25 日**
Date of Decision:	**25 April 2022**

投訴內容

上訴人是一座私人屋苑(屋苑)的居民,屋苑的業主委員會(業委會)是由屋苑業主組成的非法團組織,業委會於關鍵時間在任。業委會發出一項問卷(問卷),邀請屋苑業主就與屋苑相關的土地用途表達意見。屋苑的管理人(管理人)被委派負責收集屋苑業主填寫的問卷。

The Complaint

The appellant was a resident of a private residential development (Development). The Owners' Committee (Committee) was an unincorporated association formed by the owners of the Development and was in office at the material time. The Committee issued a questionnaire and invited the owners of the Development to state their views in respect of the land use concerning the Development (Questionnaire). The manager of the Development (Manager) was appointed with the duty to collect the completed Questionnaires from the owners.

上訴人向私隱專員作出投訴，他認為業委會透過問卷不當地收集個人資料，業委會委員應該為此負上責任。他亦投訴管理人與業委會合謀以不法手段透過問卷收集業主的個人資料。

The appellant lodged a complaint with the Privacy Commissioner against the Committee for improperly collecting personal data through the Questionnaire and contended that members of the Committee should be held responsible in this regard. The appellant also lodged a complaint against the Manager, alleging that the Manager had conspired with the Committee and resolved to unlawfully collect personal data of the owners through the Questionnaire.

私隱專員的決定

在調查期間，私隱專員留意到上訴人拒絕確認有關他作為案中資料當事人的身分，即他是否在問卷中被收集意見的屋苑業主的其中一人。

The Privacy Commissioner's Decision

During the investigation into the complaints, the Privacy Commissioner noted that the appellant refused to confirm his status as a data subject concerned in the cases, i.e. whether he was one of the owners of the Development whose views were collected in the Questionnaire.

雖然上訴人拒絕確認其身分，私隱專員仍然檢視與投訴有關的資料，並認為業委會在符合其職能及責任的情況下發出問卷，亦沒有不必要或過度收集個人資料。因此，私隱專員認為並無必要就個案作進一步調查，故行使《私隱條例》第39(2)(d)條的酌情權，決定終止調查上訴人的投訴。上訴人不滿私隱專員在兩宗投訴中所作的決定，遂向委員會提出上訴，並獲一併處理。

Despite the appellant's refusal to provide confirmation as to his identity, the Privacy Commissioner reviewed the relevant information of the complaint and considered that the Committee had acted in accordance with its functions and duties in issuing the Questionnaire, and had not unnecessarily and excessively collected personal data. On this basis, the Privacy Commissioner considered further investigation into the complaints unnecessary and exercised the discretion under section 39(2)(d) of the PDPO to terminate the investigation. Dissatisfied with the Privacy Commissioner's decision made in the respective complaints, the appellant lodged an appeal with the AAB regarding both complaints, which the AAB considered together.

上訴

委員會確認私隱專員的決定，並基於下述理由駁回該上訴：

(1) 上訴人承認自己並非該屋苑的業主，他沒有填寫過該問卷或提供任何其個人資料給業委會。因此，他並非一名資料當事人，沒有權利按照《私隱條例》第37條作出投訴。單就此原因，該上訴便應被駁回。

(2) 私隱專員的職能及權力列於《私隱條例》第8條。毫無疑問，私隱專員的職能或責任不包括處理樓宇管理爭議。

(3) 《私隱條例》內沒有條文排除業委會(作為非法人組織)成為《私隱條例》下所定義的資料使用者。同時，管理人只是業委會的代理，因此並不屬《私隱條例》下的資料使用者。

(4) 投訴人有責任提出一些證據以證實其指稱。不過，上訴人針對業委會及管理人提出的部分指稱毫無根據。私隱專員在此情況下毋需就該些指控作出調查。

The Appeal

The AAB confirmed the Privacy Commissioner's decisions and dismissed the appeals on the following grounds:

(1) The appellant admitted that he was never an owner of the Development. He did not fill in the Questionnaire nor provide any of his personal data to the Committee. Therefore, he was not a data subject and did not have the right to file a complaint under section 37 of the PDPO. For this reason alone, the appeal should be dismissed.

(2) Section 8 of the PDPO defines the functions and powers of the Privacy Commissioner. It was undoubtedly not her function or duty to deal with building management disputes.

(3) Nothing in the PDPO precludes the Committee (being an unincorporated association) from being a data user as defined under the PDPO. Meanwhile, the Manager merely acted as the Committee's agent and thus was not a data user for the purpose of the PDPO.

(4) A number of allegations made by the appellant against the Committee and the Manager respectively were not supported by any evidence. The Privacy Commissioner was not obligated to further investigate those allegations.

(5) 有關問卷要求業主填寫自己的地址以及簽名是有必要性的。這個要求是要確保每個填寫問卷的業主都只會填寫和交回一份問卷，而且那些已經完成了的問卷是反映了業主們的真實看法。

(6) 基於本案的整體情況，私隱專員終止調查的決定並不涉及不當行使《私隱條例》第39(2)(d)條的酌情權。

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
黃寶漫助理律師代表私隱專員

(5) The requirement that the Questionnaire must be signed by the owners of the Development with their address stated was necessary as the Committee needed to ensure that each owner completed and returned no more than one questionnaire, and that the completed questionnaire reflected the true views of the owners.

(6) In the circumstances of the case, the Privacy Commissioner's decision to terminate the investigation was not an improper exercise of discretion under section 39(2)(d) of the PDPO.

The AAB's Decision

The appeal was dismissed.

The appellant appeared in person
Ms Clemence WONG, Assistant Legal Counsel, represented the Privacy Commissioner

附錄三
Appendix 3

上訴個案簡述(三)

(行政上訴案件第13/2021號)

《私隱條例》讓資料當事人提出查閱資料要求的目的並非擴大文件披露的範圍 — 私隱專員毋須就無憑無據的指稱作出調查 — 正確行使酌情權拒絕對投訴作進一步調查

Appeal Case Note (3)

(AAB Appeal No. 13 of 2021)

Not the purpose of the PDPO to extend the scope of discovery by enabling a data subject to make DARs – Privacy Commissioner not obliged to investigate bare allegations – the Privacy Commissioner's discretion not to further investigate the complaint duly exercised

聆訊委員會成員:	**張金良先生(主席) Mr CHEUNG Kam-leung (Chairperson)**
Coram:	**施明耀先生(委員) Mr SY Ming-yiu (Member)**
	容慧慈女士(委員) Ms Christine YUNG Wai-chi (Member)
裁決理由書日期:	**2022 年 5 月 11 日**
Date of Decision:	**11 May 2022**

投訴內容

上訴人是一間會所(會所)的會員,會所在關鍵時間由一間公司(公司)營運。使用會所的人士需要遵從其規則及附例。公司之前曾向上訴人發出警告信,指稱他屢次違反會所的附例。上訴人否認公司的指稱,並要求公司提供在相關日子於會所涉及上訴人的閉路電視片段。

The Complaint

The appellant was a member of a clubhouse (Clubhouse) operated by a company (Company) at the material time. The use of the Clubhouse was subject to its rules and by-laws. The Company had previously issued a warning letter to the appellant, alleging that he had repeatedly breached the Clubhouse by-laws. The appellant denied these allegations and requested the Company produce CCTV footage taken at the Clubhouse involving him on the relevant date.

公司在回覆上訴人的查閱資料要求時，向他提供了一段短片，當中顯示他在相關日子離開會所的時間。上訴人向私隱專員作出投訴，指稱公司沒有遵從其查閱資料要求，及故意刪除或不法地拒絕提供其他相關影片。

In response to the appellant's DAR, the Company provided him with a short video footage which showed him leaving the Clubhouse on the relevant date. The appellant subsequently lodged a complaint with the Privacy Commissioner against the Company, alleging that the Company failed to comply with the DAR and had either deliberately deleted or unlawfully withheld the other video footage.

私隱專員的決定

經調查投訴後，私隱專員知悉公司已向上訴人提供一段拍攝到上訴人在相關時間位於會所的影片，而沒有其他證據證明上訴人的說法，即指稱公司故意刪除或不法地拒絕提供其他相關影片。

The Privacy Commissioner's Decision

Upon investigating the complaint, the Privacy Commissioner noted that the Company had provided the appellant with footage depicting the appellant in the Clubhouse at the material time. There was no other evidence supporting the appellant's allegation that the Company had either deliberately deleted or unlawfully withheld other footage.

再者，上訴人已經述明查閱資料要求的目的是取得影片以支持他可能會向公司就它對上訴人作出的不實指控而提出的民事索償。私隱專員認為《私隱條例》讓資料當事人享有有關個人資料的權利，目的是讓資料當事人查核其個人資料，而非讓資料當事人為其他的目的(例如訴訟)查找資料。

Furthermore, the appellant stated that the purpose of the DAR was to obtain footage supporting his potential civil claim against the Company for its wrongful assertion. In this regard, the Privacy Commissioner reiterated that the PDPO provides data subjects with access to their personal data to enable them to examine it, but not for other purposes, such as litigation.

因此，私隱專員認為上訴人投訴的主要目標的事宜與個人資料私隱無關，就個案作進一步調查並無必要。私隱專員因而行使《私隱條例》第39(2)(ca)條及第39(2)(d)條的酌情權，決定對上訴人的投訴終止調查。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

On this basis, the Privacy Commissioner considered the appellant's primary subject matter unrelated to personal data privacy and further investigation unnecessary. The Privacy Commissioner exercised discretion under sections 39(2)(ca) and 39(2)(d) of the PDPO to terminate the investigation. Dissatisfied with the Privacy Commissioner's decision, the appellant lodged an appeal with 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) 沒有任何證據支持上訴人的指稱，即公司故意刪除或不法地拒絕提供其他相關影片。上訴人有責任提出至少一些證據以支持其投訴，而私隱專員毋須就無憑無據的指稱作出調查。

(2) 上訴人希望獲得所有可能存在的證據，以確定他可能會向公司提出的申索的勝算。不過，《私隱條例》的目的並非擴大文件披露的範圍以讓他反駁公司就他違反附例所提出的指控。

(3) 公司已遵從上訴人的查閱資料要求，私隱專員正確行使《私隱條例》第39(2)條的酌情權終止調查。

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
黃寶漫助理律師代表私隱專員
該公司(受到遭上訴所反對的決定所約束的人)缺席應訊

The Appeal

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

(1) The appellant's allegation that the Company had either deliberately deleted or unlawfully withheld other footage was unsupported by evidence. The appellant must adduce at least some evidence to support his complaint and the Privacy Commissioner needs not investigate bare allegations.

(2) The appellant wished to have all the potentially available evidence to better determine the merit of potential claims against the Company. However, it was not the purpose of the PDPO to extend the scope of discovery to enable him to rebut the Company's allegations of breach on his part.

(3) The Company had complied with the appellant's DAR and the Privacy Commissioner properly exercised discretion under section 39(2) of the PDPO in terminating the investigation.

The AAB's Decision

The appeal was dismissed.

The appellant appeared in person
Ms Clemence WONG, Assistant Legal Counsel, represented the Privacy Commissioner
The Company (the Person bound by the decision appealed against) was absent

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

載有個人資料而未被加密的文件被發送至錯誤的電郵地址 — 保障資料第2(1)原則 — 個人資料的準確性、保障資料第4原則 — 個人資料的保安

投訴內容

投訴人與丈夫委託某律師樓辦理物業買賣手續。就有關交易，投訴人的丈夫收到一封由該律師樓發出的電郵（該電郵），當中夾附了數份交易文件。投訴人的丈夫留意到，該電郵被抄送予一個與投訴人電郵地址非常相似的電郵地址。投訴人不滿該律師樓將他們夫婦二人的個人資料外洩，遂向私隱專員公署投訴該律師樓。

結果

該律師樓解釋，發送該電郵的職員沒有與投訴人核對其手寫的電郵地址，以致該職員在發送該電郵時錯誤地輸入投訴人的電郵地址。該律師樓亦承認，該職員在透過該電郵發送文件時沒有將附件加密。

Case 1

Unencrypted documents containing personal data were sent to an incorrect email address – DPP 2(1) – accuracy of personal data and DPP 4 – security of personal data

The Complaint

The complainant and her husband appointed a law firm to handle property conveyancing procedures. As part of the transaction, the complainant's husband received an email (the Email) from the law firm, with some conveyance documents attached. The complainant's husband noticed that the Email was also sent to an email address that was highly similar to the complainant's own email address. The complainant was dissatisfied that the law firm had exposed her and her husband's personal data to others. As a result, she lodged a complaint against the law firm with the PCPD.

Outcome

According to the law firm's explanation, the staff member who sent the Email did not verify the handwritten email address with the complainant, resulting in a typographical error when entering the complainant's email address for sending the Email. The law firm also acknowledged that the staff member did not encrypt the attachments when sending the documents via the Email.

經私隱專員公署介入後，該律師樓已指示員工在發出電郵時，須小心檢查收件人地址及附件是否正確，並確保載有客戶個人資料的附件被加密及／或以密碼保護。此外，該律師樓亦就其發送電郵的標準做法為員工提供培訓。

Following the intervention of the PCPD, the law firm instructed its staff to carefully verify the recipient addresses and attachments before sending any emails, and to encrypt and/or password protect all documents containing clients' personal data sent via email. Furthermore, the law firm also provided training to its staff in relation to standard practices of email correspondence.

私隱專員公署亦就事件向該機構發出警告，要求他們務必敦促員工日後在保障及處理個人資料方面，緊遵《私隱條例》的規定，同時嚴格遵從其資料保障政策，不時提醒員工小心處理個人資料的重要性，並定時將相關的政策文件作內部傳閱。

The PCPD also issued a warning to the law firm, requiring it to instruct its staff to strictly comply with the relevant requirements under the PDPO regarding the handling and protection of clients' personal data, and to strictly adhere to its data protection policies. The firm was also instructed to regularly remind its staff about the importance of carefully handling clients' personal data, and to periodically circulate the relevant policy to its staff.

借鑑

個案是源於誤讀手寫電郵地址的人為錯誤。透過電郵與不同人士溝通，是現今十分普遍的工作活動。當員工每日都在發送電郵，他們或會不自覺地忽略了核對電郵地址的重要性。要避免發生類似本案的人為錯誤，機構應透過訂立資料保障的政策，並為員工提供培訓，藉以在員工之間建立尊重個人資料私隱的文化。

Lessons Learnt

The primary cause of the complaint was an instance of human error: the misreading of a handwritten email address. This is not an uncommon occurrence in workplaces where staff regularly communicate with various parties via email. They may unwittingly overlook the importance of verifying the accuracy of email addresses. To prevent similar human errors, organisations are advised to cultivate a culture of respect for personal data privacy. This can be achieved by establishing data protection policies and providing staff members with regular training.

附錄四
Appendix 4

個案二

機構在沒有持有投訴人所要求查閱的資料的情況下索取查閱資料費用 — 保障資料第6原則 — 查閱資料費用

投訴內容

投訴人是某機構的前職員，他在離職後向該機構提出查閱資料要求（該要求），要求查閱他人事檔案中的以下紀錄：(i)被客戶或供應商投訴、(ii)違反僱員合約或該機構向他發出警告信，及(iii)觸犯香港法例第57章《僱傭條例》而被解僱。該機構在回覆該要求時，向投訴人表示需就該要求收取港幣906.5元的查閱資料要求費用（該費用）。然而，經了解後，投訴人得知該機構事實上無持有他所要求查閱的資料。就此，投訴人向私隱專員公署投訴該機構向他收取該費用。

結果

根據《私隱條例》第28條，資料使用者可為依從查閱資料要求而徵收不超乎適度的費用，但這只限於當資料使用者藉提供所查閱的個人資料的複本以依從查閱資料要求。

Case 2

A company charged a fee for data access request notwithstanding that it did not hold the requested data – DPP 6 – charging of fee for data access request

The Complaint

The complainant, a former employee of a company, made a DAR to the company for records from his personnel file. Specifically, he requested information regarding (i) complaints made against him by customers or suppliers, (ii) breaches of the employment contract or warnings sent to him by the company, and (iii) the record of the termination of his employment due to his breach of the Employment Ordinance (Cap 57). The company responded to the DAR with a request for a fee of HK$906.5 (the Fee). However, upon further inquiry, the complainant was informed that the company did not possess the requested data. As a result, the complainant filed a complaint with the PCPD against the company for imposing the Fee on him.

Outcome

According to section 28 of the PDPO, a data user may impose a fee for complying with a DAR, provided that the fee is not excessive. This applies only when the data user complies with the DAR by providing a copy of the requested personal data.

該機構向私隱專員公署確認他們並無持有投訴人所要求查閱的資料，私隱專員公署因而認為，該機構不可為依從該要求而向投訴人徵收費用。經私隱專員公署解釋《私隱條例》的相關規定後，該機構最終以書面回覆投訴人，確認並無持有投訴人所要求查閱的資料，亦再無要求他繳付該費用。由於該機構在個案中向投訴人徵收該費用的做法不符《私隱條例》的規定，私隱專員公署亦已就事件向該機構發警告信，要求該機構日後在處理查閱資料要求方面必須遵循《私隱條例》的規定。

The company confirmed to the PCPD that it did not possess the data requested by the complainant. Consequently, the PCPD determined that the company could not charge the complainant the Fee for complying with the DAR. After explaining the relevant provisions of the PDPO to the company, the PCPD requested that the company provide a written response to the complainant affirming that it did not hold the requested data and would not collect the Fee. As the PCPD found that the imposition of the Fee in the present case did not comply with the requirements of the PDPO, the PCPD issued a warning to the company, advising it to ensure that all future DARs are handled in accordance with the PDPO.

借鑑

《私隱條例》容許資料使用者可為依從查閱資料要求而徵收不超乎適度的費用。然而，徵收費用不適用於資料使用者不持有所要求查閱資料的情況。資料使用者假如並無持有所要求查閱的資料，便必須在收到查閱資料要求後的40日內書面通知提出要求者。

Lessons Learnt

The PDPO allows a data user to impose a non-excessive fee for complying with a DAR. However, the imposition of a fee is not allowed in situations where the data user does not hold the requested data. If a data user does not hold the requested data, it is required to inform the requestor in writing within the 40-day time limit.

附錄四
Appendix 4

個案三

興趣班課程中心過度收集學員及家長的個人資料 — 保障資料第1原則 — 個人資料的收集

投訴內容

投訴人到課程中心為兒子報讀興趣班，該中心要求投訴人必須提供她的部分香港身份證號碼和其兒子的出生日期。投訴人認為該中心過度收集個人資料，遂向私隱專員公署作出投訴。

結果

該中心解釋，收集學員家長的部分香港身份證號碼，是為確定他們是學員的監護人，合符資格為未成年學員報讀課程；而收集學員的出生日期則是為向學員提供生日優惠、方便日後為學員報名參加比賽，以及按他的年齡編排班別。

私隱專員公署認為收集家長的香港身份證號碼根本無助該中心確定家長與學員的關係，而就提供生日優惠及按年齡編班的目的而言，收集學員的出生年份及月份已屬足夠。此外，該中心亦不應假設學員將會參加比賽並過早收集他們的完整出生日期作日後報名用途。

Case 3

A learning centre for interest classes collected excessive personal data from students and their parents – DPP 1 – collection of personal data

The Complaint

The complainant signed up for an interest class for her son at a learning centre (the Centre). The Centre required the complainant to provide her partial Hong Kong Identity (HKID) Card number and her son's date of birth. As a result, the complainant filed a complaint with the PCPD against the Centre for excessively collecting personal data.

Outcome

The Centre provided an explanation for collecting parents' partial HKID Card numbers, stating it was necessary to determine their capacity as guardians and eligibility to sign up for students who are minors; whereas the collection of students' date of birth was required for providing birthday offers, registering for competitions, and allocating them to classes according to age groups.

The PCPD considered the collection of the parents' HKID Card numbers would not aid the Centre in verifying their relationship with the students and that it should be sufficient to collect only the year and month of birth for providing birthday offers and class allocation. The Centre should not assume students will sign up for future competitions and collect their complete date of birth prematurely.

經私隱專員公署介入後，該中心已修改其收集個人資料的做法，停止向學員的監護人收集香港身份證號碼及改為只收集新學員的出生年份和月份，該中心亦同時銷毀經已收集的香港身份證號碼，並確保資料庫中只保存現有學員的出生年份和月份。

私隱專員公署亦就事件向該中心發出警告，要求他們日後向客人收集個人資料前，慎重考慮是否真正需要收集有關資料，確保緊遵《私隱條例》的相關規定。

借鑑

由於香港身份證號碼屬敏感的個人資料，一旦被濫用，可為當事人帶來身分被盜用等嚴重後果。為確保循規守法，機構在決定收集香港身份證號碼前應進行全面評估，以確定是否有真正需要及充分理據作出有關收集。另一方面，兒童私隱的議題在社會上日漸受到關注，致力保障和尊重兒童私隱的機構可贏得家長的信任，從而建立競爭優勢。

After the PCPD intervened, the Centre revised its practice of personal data collection such that it no longer collected guardians' partial HKID Card numbers, and only collected the month and year of birth from newly enrolled students. The Centre also destroyed the previously collected HKID Card numbers, retaining only the month and year of birth in the records of current students.

The PCPD also issued a warning to the Centre, urging it to carefully consider if it is necessary to collect the personal data before requesting it from customers and to ensure compliance with the relevant requirements under the PDPO.

Lessons Learnt

As HKID Card numbers are a piece of sensitive personal data, its misuse may result in dire consequences like identity theft to data subjects. To ensure compliance with the legal requirements, organisations should, before deciding to collect HKID Card numbers, thoroughly assess if there exists a genuine need and sufficient justification for such collection. On the other hand, in the light of the increasing concern surrounding children's privacy in society, organisations that are committed to respecting and protecting children's privacy can gain competitive edges by winning parents' trust.

附錄四
Appendix 4

個案四

員工在社交媒體不當披露客戶個人資料 — 保障資料第4原則 — 個人資料的保安

投訴內容

投訴事件發生於2019冠狀病毒病爆發期間，根據當時實施的防疫政策，抵港人士須在指定檢疫酒店接受檢疫。投訴人表示，他在社交媒體上發現一段短片(該短片)，片中出現一份入住檢疫酒店接受檢疫人士的名單(該名單)，載於該名單上的住客姓名、預訂確認編號及房間號碼等資料清晰可見。投訴人就此向私隱專員公署作出投訴。

結果

從有關社交媒體帳戶的公開內容可見，發布該短片的人士可能是一間指定檢疫酒店的員工，私隱專員公署遂向該酒店查詢。

該酒店確認短片是由一名合約外判員工發布，他因工作需要獲授權處理該名單。該員工上載該短片的原意，是為了在社交媒體分享工作地點的環境，但並沒有留意到該名單在無意中被攝入鏡頭。在私隱專員公署介入後，該員工已即時從社交媒體移除該短片。

Case 4

An employee of a hotel disclosed customers' personal data on social media without authorisation – DPP 4 – security of personal data

The Complaint

The incident under complaint happened amid the outbreak of COVID-19. According to the anti-pandemic measures in force at the material time, people arriving in Hong Kong were required to undergo quarantine at a designated quarantine hotel. The complainant alleged that from a video clip (the Clip) uploaded onto the social media, he noticed a list (the List) of hotel guests who were under hotel quarantine. The List displayed sensitive information, such as the guests' names, their booking confirmation numbers and room numbers, which could be clearly seen in the Clip. The complainant hence lodged a complaint with the PCPD.

Outcome

Based on the information posted on the social media account in question, the Clip might have been posted by an employee of a designated hotel. The PCPD hence approached the hotel for enquiry.

The hotel confirmed that the Clip was uploaded by a member of its outsourced contract staff, who was authorised to access the List for the purpose of performing his duties. The staff member had inadvertently captured the List in the Clip while attempting to show the work environment to others. After the PCPD intervened, the staff member immediately removed the Clip from social media.

該酒店並確認該員工由於拍攝及於社交媒體發布日常工作中所接觸的資訊，因而違反他們的保障客人資料政策。除向該員工發出警告，指示他日後嚴格遵循該酒店的內部指引行事，該酒店亦向所有員工提供相關培訓，提醒員工應採取的保障客人個人資料的步驟。

The hotel also confirmed that the staff member had breached its policy for protecting customers' personal data by filming and uploading work-related information to social media. In addition to warning the staff member and instructing him to strictly comply with the policy in future, the hotel provided relevant training for all staff members and reminded them of the practical steps that should be taken to protect customers' personal data.

私隱專員公署就事件向該酒店發出警告，敦促該酒店定期向相關員工發出指引，並透過培訓提高員工保障個人資料私隱的意識，確保員工以謹慎的態度處理客人的個人資料，以符合《私隱條例》的相關規定。

The PCPD also issued a warning to the hotel, requiring it to regularly issue reminders to relevant staff members, heighten their awareness of personal data protection through training, and ensure that its staff members handle customers' personal data with caution, in order to ensure compliance with the relevant requirements under the PDPO.

借鑑

隨着手機及社交媒體的廣泛使用，拍攝日常生活片段在網上分享的做法亦漸趨普遍。在趕上潮流拍攝及分享短片的同時，大家必須注意當中的個人資料私隱危機並謹慎行事，例如避免將載有個人資料的文件攝入鏡頭，並在上載短片前仔細檢查短片的內容，確定內容是適合作公開分享後才上載到社交媒體，以避免發生類似本案的事件。

Lessons Learnt

Following the prevalent use of mobile phones and social media, filming and sharing video clips of daily life has become a common practice. While catching up with this trend, we must also be mindful of potential privacy pitfalls. To avoid the occurrence of incidents similar to this case, it is important to avoid filming any records of personal data, and to carefully review the recorded content to ensure its suitability for public sharing prior to uploading to social media.

附錄四
Appendix 4

個案五

美容中心職員以不公平的方式透過錄音記錄客人於診症時的對話內容 — 保障資料第1原則 — 個人資料的收集

投訴內容

投訴人為某美容中心的客人。她就一項美容療程與該美容中心產生糾紛。投訴人按該美容中心的要求，在其職員陪同下到指定診所就她的皮膚狀況諮詢醫生意見。在過程中，投訴人發現該美容中心的職員在未有告知她的情況下將她與醫生診症時的對話內容錄音。投訴人不滿該職員以不公平的方式收集其個人資料，遂向私隱專員公署投訴該美容中心。

結果

該美容中心表示，事件乃個別職員不了解《私隱條例》的規定所致。該美容中心向私隱專員公署確認已刪除有關錄音，並向投訴人致歉。此外，該美容中心向涉事職員發出警告，告誡涉事職員不可隨意進行錄音及如有需要錄音必須先告知當事人。為避免同類情況再次發生，該美容中心承諾會安排職員參加與《私隱條例》相關的培訓，以提升職員對保障客人個人資料私隱的意識。

Case 5

A staff member of a beauty centre recorded a customer's conversation during a medical consultation by unfair means – DPP 1 – collection of personal data

The Complaint

The complainant, a customer of a beauty centre, had a dispute with the centre concerning a beauty treatment. At the request of the beauty centre, the complainant visited a designated clinic with a staff member to consult a doctor regarding her skin condition. During the consultation, the complainant discovered that a staff member from the beauty centre had audio-recorded the conversation between her and the doctor without notifying her. Dissatisfied with the staff member's unfair collection of her personal data, the complainant lodged a complaint against the beauty centre with the PCPD.

Outcome

The beauty centre attributed the incident to an individual staff member's inadequate understanding of the PDPO. After confirming with the PCPD that the recording in question had been deleted, the centre apologised to the complainant and issued a warning to the staff member involved, cautioning her against making recordings without prior notification to customers. To prevent recurrence of similar incidents, the beauty centre promised to arrange relevant PDPO training for its staff members to enhance their awareness of protecting customers' personal data privacy.

私隱專員公署向該美容中心發出警告，要求該美容中心必須確保前線職員充分了解及遵守《私隱條例》下有關收集個人資料的規定。如職員欲透過錄音記錄客人於診症過程中的對話內容，他們必須在切實可行的情況下，事先通知當事人，向他們提供「收集個人資料聲明」，包括清楚告知當事人進行錄音的目的，以緊遵《私隱條例》的有關規定。

The PCPD had issued a warning to the beauty centre, requesting it to ensure its frontline staff members fully understand and comply with the requirements of the PDPO in relation to the collection of personal data. To comply with the relevant requirements of the PDPO, if staff members intend to record customers' conversations during medical consultations, they should take all practicable steps to ensure that the customer is given prior notice and provided with a Personal Information Collection Statement, which should explicitly inform customers of the purpose of the recording.

借鑑

私隱專員公署明白機構在若干情況下需要透過錄音記錄客戶的對話內容。不過，如對話內容包含客戶的個人資料，相關錄音便會構成收集個人資料而受《私隱條例》所規管。在這情況下，機構必須先告知客戶擬進行錄音及其有關目的，以遵守《私隱條例》的保障資料第1原則下有關收集個人資料的規定。此外，涉案職員對保障客戶個人資料私隱的意識明顯不足。機構應定期向員工提供個人資料私隱的培訓，以確保員工能充分了解及遵守《私隱條例》的規定。

Lessons Learnt

The PCPD understands that organisations may have legitimate reasons for audio-recording customers' conversations under certain circumstances. However, if such conversations involve customers' personal data, the recording will amount to the collection of personal data, and the relevant requirements under the PDPO must be observed. In such situations, organisations must first notify customers of their intention to make audio recordings and the purpose of recording to comply with the requirements of DPP 1 under the PDPO regarding the collection of personal data. Additionally, the staff member involved in this case demonstrated a lack of awareness of the importance of protecting customers' personal data privacy. Organisations should provide regular personal data privacy training to their employees to ensure they fully understand and comply with the requirements of the PDPO.

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

中醫師在使用病人的個人資料作直接促銷前沒有採取指明的行動通知該病人，以及未有告知該病人她拒收直接促銷訊息的權利 —《私隱條例》第35C及35F條

Case 1

A Chinese medicine practitioner used a patient's personal data in direct marketing without taking specified actions to notify the patient and obtain her consent, and failed to notify the patient of her opt-out right – sections 35C and 35F of the PDPO

法院：	**東區裁判法院**
Court:	**Eastern Magistrates' Court**
審理裁判官：	**屈麗雯裁判官**
Coram:	**Miss WAT Lai-man, Minnie, Magistrate**
裁決日期：	**2023 年 2 月 10 日**
Date of Decision:	**10 February 2023**

投訴內容

投訴人是一間中醫診所的病人，她於2015年向該診所提供個人資料，Y中醫師亦曾是該診所的中醫師，但投訴人從未向Y中醫師問症。其後，投訴人收到Y中醫師的WhatsApp訊息，自稱為該診所的前中醫師，向投訴人發送她的工作名片，宣傳她新任職診所的中醫藥服務。

The Complaint

The complainant was a patient at a Chinese medicine clinic (the Clinic) and provided her personal data to the Clinic in 2015. Practitioner Y also worked at the Clinic as a Chinese medicine practitioner but was never consulted by the complainant. Subsequently, the complainant received a WhatsApp message from Practitioner Y, who claimed to be a former practitioner at the Clinic, containing a photo of Practitioner Y's business card promoting Chinese medicine services at a new clinic where she then worked.

結果

Y中醫師承認違反《私隱條例》第35C(1)條及第35F(1)條的控罪，即她未有採取所需步驟通知當事人及取得她的同意下，使用當事人向另一診所提供的個人資料以向她發出直接促銷訊息；亦在首次使用當事人的個人資料作直接促銷時，未有告知當事人有權要求被告在不收費的情況下，停止使用她的個人資料。Y中醫師每項控罪分別被判罰款港幣2,000元，共被判罰款港幣4,000元。

借鑑

隨着市民保障個人資料私隱的意識日漸提升，機構及其僱員須尊重客戶對其個人資料在直接促銷中如何使用的選擇。離職僱員在使用舊客戶的個人資料進行直接促銷時，更應加倍小心，除了要先取得前僱主的同意外，離職僱員還應按《私隱條例》有關直接促銷的條款，採取所需步驟通知資料當事人並取得他們的同意。

Outcome

Practitioner Y pleaded guilty to charges of sections 35C(1) and 35F(1) of the PDPO for failing to take the necessary action and obtain the data subject's consent before using her personal data that was provided to another clinic in direct marketing. She also neglected to inform the data subject of her right to request that her personal data not be used in direct marketing without charge when using it for the first time. Practitioner Y was fined HK$2,000 in respect of each charge, totalling HK$4,000.

Lessons Learnt

In view of the rising public awareness of the importance of protecting personal data privacy, organisations and their employees should respect their customers' choices regarding the use of their personal data in direct marketing. Former employees should pay close attention when using personal data of their previous clients in direct marketing. Apart from obtaining consent from their former employers, ex-employees should also take specified actions to notify the data subjects and obtain their consent in accordance with the requirements of direct marketing under the PDPO.

附錄五
Appendix 5

個案二

情侶分手後，男方在互聯網上將洩露女方的個人資料 —《私隱條例》第64(3A)條

Case 2

A man disclosed his ex-girlfriend's personal information on the internet after their breakup – section 64(3A) of the PDPO

法院：	**沙田裁判法院**
Court:	**Shatin Magistrates' Court**
審理裁判官：	**張志偉裁判官**
Coram:	**Mr CHEUNG Chi-wai, David, Magistrate**
裁決日期：	**2022 年 10 月 6 日**
Date of Decision:	**6 October 2022**

投訴內容

被告與投訴人曾短暫交往，但不久後分手。其後，被告在沒有得到投訴人的同意下，先後於四個不同的社交媒體平台上披露投訴人的個人資料，包括姓名、照片、住址、私人及辦公室電話號碼、公司名稱及職位。被告還在其中三個平台冒認投訴人開設帳戶，並指投訴人歡迎其他人到她的住址找她。後來，許多陌生人聯絡投訴人，意圖與她交朋友。

The Complaint

The complainant and the defendant had a brief relationship before breaking up. Thereafter, without the complainant's consent, the defendant disclosed the complainant's personal data, including her name, photos, residential address, office and private telephone numbers, and the name of her employer and position, on four different social media platforms. The defendant also impersonated the complainant to open accounts on three of the said platforms, stating that the complainant welcomed others to visit her at her home address. Many strangers later contacted the complainant and tried to get acquainted with her.

結果

法院在被告認罪後，裁定他七項涉及「起底」的控罪成立。法院經考慮相關報告後，判處被告監禁八個月。

借鑑

公眾人士應以合法和負責的方式處理糾紛。在互聯網上披露他人的個人資料，不但無助於解決問題，反而往往會令情況變得更壞。此外，「起底」被視為嚴重的刑事罪行。違例者一經定罪可即時監禁，最高可被處罰100萬元及監禁五年。

Outcome

The defendant pleaded guilty to seven charges of the doxxing offence. After considering the relevant reports, the court sentenced the defendant to eight months' imprisonment for unlawfully disclosing the complainant's personal data.

Lessons Learnt

The general public should handle their disputes in a lawful and responsible manner. Revealing personal data of others on the internet may amount to doxxing and does not help resolve issues. Moreover, doxxing is a serious criminal offence. Offenders are liable upon conviction to immediate imprisonment and subject to a maximum penalty of a fine up to $1,000,000 and imprisonment up to five years.

附錄五
Appendix 5

個案三

網上賣家因金錢糾紛在互聯網上洩露供應商的個人資料 —《私隱條例》第64(3A)條

Case 3

An online trader disclosed her supplier's personal information on the internet because of monetary dispute – section 64(3A) of the PDPO

法院：	**沙田裁判法院**
Court:	**Shatin Magistrates' Court**
審理裁判官：	**覃有方裁判官**
Coram:	**Mr CHUM Yau-fong, David, Magistrate**
裁決日期：	**2023 年 2 月 1 日**
Date of Decision:	**1 February 2023**

投訴內容

被告從事網上買賣，而投訴人曾是其供應商。兩人之間的商業關係因金錢糾紛而變得緊張。其後，被告在一個社交媒體平台上14個不同的群組發文，聲稱有人騙財，並在文中披露投訴人和她的丈夫的個人資料。被披露的個人資料包括投訴人和她的丈夫的中文姓名、照片和電話號碼。

The Complaint

The defendant was an online trader and the complainant was her supplier. Their business relationship turned sour after a dispute over money. Thereafter, the defendant disclosed the personal data of the complainant and her husband in 14 groups of a social media platform, along with allegations of fraudulent behaviour. The disclosed personal data included the Chinese names, photos, and phone number of the complainant and her husband.

結果

法院在被告認罪後，裁定她14項涉及「起底」的控罪成立。法院經考慮相關報告後，判處被告監禁兩個月，緩刑兩年。

借鑑

市民應循合法途徑處理糾紛，將他人「起底」是不可接受的行為，相反往往只會使衝突升級。再者，「起底」屬嚴重罪行，違例者一經定罪可即時監禁，最高可被處罰100萬元及監禁五年。

Outcome

The defendant pleaded guilty to 14 charges of the doxxing offence. After considering the relevant report, the court sentenced the defendant to two months' imprisonment, suspended for two years.

Lessons Learnt

Members of the public should resolve their disputes by lawful means. Doxxing is not an acceptable means of resolution of disputes and will only escalate the conflict. Moreover, doxxing is a serious offence and offenders are liable upon conviction to immediate imprisonment and subject to a maximum penalty of a fine up to $1,000,000 and imprisonment 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

一間教育機構因密碼管理欠佳而導致未獲授權查閱學生和家長的個人資料 — 保障資料第4原則 — 個人資料的保安

背景

一間教育機構向私隱專員公署通報，指他們的資訊管理系統遭黑客利用暴力攻擊獲取了管理員密碼，並建立了具有管理權限的新帳戶，以查閱當中的個人資料。事件影響超過24,000名家長及學生用戶的個人資料。

該機構調查後發現，是次事故源於密碼管理欠佳，未有採取行業最佳做法保護管理員帳戶所致。

Case 1

An educational institution's improper password management led to unauthorised access to the personal data of students and parents – DPP 4 – security of personal data

Background

An educational institution reported to the PCPD that a hacker had acquired the administrator password of its information management system through a brute force attack and created a new account with administrative rights to access the personal data stored in it. The incident affected the personal data of more than 24,000 parent and student users.

Investigation revealed that the incident was due to improper password management, which failed to protect the administrator account in accordance with industry best practices.

補救措施

收到該機構的通報後，私隱專員公署展開循規審查，並就《私隱條例》的相關規定向該機構提供建議。就此，該機構採取了補救措施，包括為其資訊管理系統採用雙重認證功能為系統帳戶提供額外的保護、設定高強度密碼、定期清理不必要的帳戶，以及透過加強培訓提高員工的資料保障意識。

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 relevant provisions of the PDPO. In response, the institution implemented remedial measures, including two-factor authentication for its information management system to provide an additional layer of protection for system accounts, strong passwords, regular purging of unnecessary accounts and an enhanced training programme to raise employees' awareness of data privacy protection.

借鑑

基於行政和教學用途，教育機構通常會持有大量關於學生及學生家長的個人資料。越來越多教育機構採用網上學習模式，當這些機構利用資訊科技帶來方便的同時，不應忽視隨之而來的私隱風險，特別是關乎兒童及青少年的個人資料。機構管理個人資料系統需加強警惕，制定適當的系統安全政策、措施和程序(例如善用多重認證功能及採用合適的密碼管理政策)，以減低個人資料遭未獲准許的或意外的查閱、處理、刪除、喪失或使用的風險。

Lessons Learnt

Educational institutions typically hold a large amount of personal data about students and their parents for administrative and educational purposes. There is an increasing trend of adopting online learning models by educational institutions. While reaping the benefits of information technology, these institutions should not overlook the accompanying privacy risks, especially regarding the personal data of children and youngsters. Organisations managing personal data systems need to remain vigilant and implement appropriate security policies, measures and procedures (e.g. utilising multi-factor authentication and adopting suitable password management policies) to minimise the risks of unauthorised or accidental access, processing, erasure, loss or use of personal data.

附錄六
Appendix 6

個案二

一名體育組織的職員錯誤地上載及傳送活動參加者的個人資料 — 保障資料第4原則 — 個人資料的保安

背景

一間體育組織向私隱專員公署通報，指職員在安排發放比賽資訊予參賽者時，錯誤地把載有308名活動參加者的姓名、電話號碼及電郵地址的檔案上載至該組織的網站及透過電郵發送給參加者。

補救措施

在收到該組織的通報後，私隱專員公署展開了循規審查。該組織向私隱專員公署表示，該組織已因應事件強化處理個人資料的程序，當中要求職員須妥善地為載有個人資料的檔案命名，使載有參賽者個人資料的檔案能夠被明確辨認，從而減少錯誤選取檔案的機會。此外，工作人員在安排上載或透過電郵發送載有個人資料的檔案前，須先由主管級職員加以覆核。該組織已召開全體員工會議向所有職員講解上述程序，並敦促職員需加以遵從。

Case 2

A staff member of a sports organisation accidentally uploaded and transmitted the personal data of event participants – DPP 4 – security of personal data

Background

A sports organisation reported to the PCPD that a staff member accidentally uploaded a file with the names, phone numbers and email addresses of 308 event participants to the organisation's website and sent it to participants via email while distributing competition information.

Remedial Measures

Upon receiving the notification from the sports organisation, the PCPD initiated a compliance check. The organisation informed the PCPD that it had enhanced personal data handling procedures in response to the incident. These measures included requiring staff to properly name files containing personal data for easy identification of files containing participants' personal data, reducing the likelihood of selecting the wrong file. Furthermore, managerial staff should review files containing personal data before uploading or emailing them. The organisation held a meeting with all employees to explain these procedures and urged staff to comply.

借鑑

資料外洩事故往往是由人為錯誤所引起。資料使用者應持續向員工灌輸保障資料的重要性，並向他們提供有關如何妥善處理個人資料的培訓。同時，資料使用者應在處理個人資料方面建立清晰而有效的程序和指引，並採取措施（例如定期提示及抽查）以確保他們遵從有關程序和指引。

Lessons Learnt

Data breach incidents are often caused by human errors. It is essential for data users to continuously make employees aware of the importance of data protection and provide them with training on proper personal data handling. Establishing clear and effective procedures and guidelines for handling personal data is essential, along with implementing measures (such as regular reminders and audits) to ensure adherence to these procedures.

附錄六
Appendix 6

個案三

載有學生及家長個人資料的文件夾遭意外棄置 — 保障資料第4原則 — 個人資料的保安

背景

一所學校向私隱專員公署通報，指一名工友錯誤地把一個載有超過100名學生及家長個人資料的「自動轉賬」文件夾（該文件夾）當作廢物處理，並棄置於學校附近的垃圾站。

該學校調查後發現，是次事故源於負責處理自動轉賬工作的文員將該文件夾放置在其桌下的垃圾桶上，以致工友誤以為該文件夾屬可棄置，並與其他廢物一併處理。

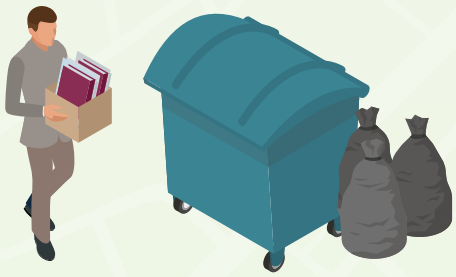
Case 3

A folder that contained personal data of students and parents was accidentally disposed of – DPP 4 – security of personal data

Background

A school reported to the PCPD that a cleaner had mistakenly treated a folder that contained auto-pay documents with personal data of over a 100 students and parents (the Folder) as waste and disposed of it at the refuse collection point near the school.

An investigation conducted by the school revealed that the clerk responsible for handling auto-pay documents placed the Folder on the rubbish bin under her desk. As a result, the cleaner disposed of the Folder together with other waste by mistake.



補救措施

收到該學校的通報後，私隱專員公署展開循規審查。因應是次事故，該學校已提醒涉事文員須謹慎處理及保管載有個人資料的文件，並向涉事工友提供有關處理廢物做法的培訓。此外，該學校將保障個人資料私隱的工作指引及注意事項納入教職員守則內，並透過會議及工作坊培訓，向員工發放已修訂的守則並講解當中要點。

Remedial Measures

Upon receipt of the notification from the school, the PCPD initiated a compliance check. In response to the incident, the school reminded the clerk of the need to exercise caution in handling and safekeeping documents containing personal data. The school also provided the cleaner with training on proper waste disposal procedures. Besides, the school incorporated guidelines and points to note on personal data protection into its staff code of conduct. The revised code of conduct was disseminated to staff through meetings and workshop training.

借鑑

無論個人資料是遭意外丟失、洩漏還是不當處置，對受影響的個人潛在的傷害不容忽視。除了制訂保障資料政策和程序外，機構應加強保安措施以保障個人資料，並採取措施及監管機制，確保僱員遵從這些政策和程序的要求行事，以及為他們提供全面的培訓，加強他們保障個人資料私隱的意識，減低人為錯誤的風險。

Lessons Learnt

Regardless of whether personal data is accidentally lost, leaked or improperly disposed of, the potential harm to the affected individuals should not be underestimated. In addition to establishing effective data protection policies and practices, organisations should strengthen security measures to safeguard personal data. This includes implementing measures and monitoring mechanisms to ensure employees comply with policies and procedures, as well as providing comprehensive training to strengthen employees' awareness of personal data protection and minimise the risk of human errors.