# 附錄
# Appendices

# 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.

### 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，是必需及屬足夠，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 longer than is necessary to fulfil the purpose for which it is used.

## 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 personal data. The data user is liable as the principal for the wrongful act of any data processor engaged by it.

### 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。

在回覆電話查詢及確認收到書面查詢方面，私隱專員公署均能夠在兩個工作日內完成所有個案，並於28個工作日內詳細回覆書面查詢。

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%）。此外，在決定結束投訴個案當中，公署能夠在180日內結案的比率為97%（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，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 the handling of public enquiries, complaints and applications for legal assistance exceeded the performance target.

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 also completed within 28 working days of receipt.

In handling public complaints, acknowledgement receipts were issued within two working days of receipt of all cases (our performance target is 98%). In closing a complaint case, 97% 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 and all applicants were informed of the outcome within three months after they had submitted all the relevant information for the applications.

| | 服務標準<br>Service Standard | 服務指標（個案達到服務水平的百分比）<br>Performance Target (% of cases meeting standard) | 工作表現<br>Performance Achieved | | | | |
|---|---|---|---|---|---|---|---|
| | | | 2019 | 2020 | 2021 | 2022 | 2023 |
| **處理公眾查詢 Handling Public Enquiries** | | | | | | | |
| **回覆電話查詢**<br>**Call back to a telephone enquiry** | 收到電話查詢後兩個工作日內<br>Within two working days of receipt | 99% | 100% | 100% | 100% | 100% | 100% |
| **確認收到書面查詢**<br>**Acknowledge receipt of a written enquiry** | 收到書面查詢後兩個工作日內<br>Within two working days of receipt | 99% | 100% | 100% | 100% | 100% | 100% |
| **詳細回覆書面查詢**<br>**Substantive reply to a written enquiry** | 收到書面查詢後28個工作日內<br>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**<br>**Acknowledge receipt of a complaint** | 收到投訴後兩個工作日內<br>Within two working days of receipt | 98% | 99% | 99% | 99% | 99% | 100% |
| **結束投訴個案**<br>**Close a complaint case** | 收到投訴後180日內[1]<br>Within 180 days of receipt[1] | 95% | 99% | 99% | 99% | 98% | 97% |
| **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**<br>**Acknowledge receipt of an application for legal assistance** | 收到申請後兩個工作日內<br>Within two working days of receipt | 99% | 100% | 不適用[2]<br>N/A[2] | 100% | 100% | 100% |
| **通知申請人申請結果**<br>**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<br>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。
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3/2023號)

投訴表格收集的個人資料及使用目的 — 處理投訴 — 抄送投訴結果信函予被投訴方 — 投訴人的合理期望 — 正確行使酌情權拒絕對投訴作進一步調查

## Appeal Case Note (1)

(AAB Appeal No. 3 of 2023)

Purpose of collection and use of personal data in a complaint form – complaint handling – copying decision letter to the party complained against – reasonable expectation of the complainant – discretion not to further investigate the complaint duly exercised

**聆訊委員會成員：** **劉恩沛女士(副主席) Miss LAU Queenie Fiona (Deputy Chairman)**
**Coram:** **陳詠琪女士(委員) Ms Winky CHAN Wing-ki (Member)**
**姚逸明先生(委員) Mr Edmond YEW Yat-ming (Member)**

**裁決理由書日期：** **2023年10月11日**
**Date of Decision:** **11 October 2023**

### 投訴內容

上訴人不滿某公立醫院醫生就上訴人親人的傷殘津貼申請所作的醫療評估結果，並向某政府決策局(該決策局)作出申訴。該決策局回覆上訴人，表示其不會介入公立醫院的日常運作及管理，並會把上訴人的投訴轉介醫院管理局處理。上訴人不滿該決策局的回覆，遂向申訴專員作出投訴。

經查訊後，申訴專員認為該決策局的回覆並不涉及任何行政失當，因而結案。同時，申訴專員把決定信函抄送給該決策局局長。上訴人因不滿申訴專員將載有其個人資料的信件抄送予該決策局而向私隱專員作出投訴。

### The Complaint

The Appellant was dissatisfied with the result of a medical assessment conducted by a doctor at a public hospital in relation to his relative's disability allowance application, and he lodged a complaint with a government bureau (the Bureau). The Bureau replied to the Appellant that it would not intervene in the daily operation and management of public hospitals and would refer his complaint to the Hospital Authority for handling. Dissatisfied with the Bureau's reply, the Appellant lodged a complaint with the Ombudsman.

Upon inquiry, the Ombudsman did not find any maladministration on the part of the Bureau and terminated the complaint case. At the same time, the Ombudsman copied the decision letter to the Secretary of the Bureau. The Appellant was dissatisfied that the decision letter containing his personal data was copied to the Bureau and lodged a complaint with the Privacy Commissioner.

## 私隱專員的決定

經初步查詢後，私隱專員認為申訴專員透過投訴表格收集個人資料，目的是作處理上訴人投訴之用。其後，雖然申訴專員的結論是該決策局並沒有行政失當，但把其對案件的評論和結果抄送給該決策局仍然屬處理投訴的一部分。

私隱專員認為在作出投訴時，上訴人已經簽署並同意申訴專員在處理投訴時可以複製投訴表格及在表格內所提交的任何資料（包括個人資料）以轉交任何人士／機構。故此，私隱專員認為申訴專員在取得上訴人披露個人資料的同意後，就處理投訴目的而把載有個人資料的信件抄送予該決策局，並沒有違反《私隱條例》保障資料第3原則，故行使《私隱條例》第39(2)(d)條賦予的酌情權，決定不就上訴人的個案作進一步調查。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

## The Privacy Commissioner's Decision

Upon preliminary enquiry, the Privacy Commissioner considered that the purpose of collecting personal data in the complaint form by the Ombudsman was to handle the Appellant's complaint. Although the Ombudsman subsequently found that there was no maladministration on the part of the Bureau, the Privacy Commissioner took the view that copying the Ombudsman's comments and findings of the case to the Bureau was a part of the complaint handling process.

The Privacy Commissioner considered that the Appellant had signed the complaint form when he filed the complaint thereby agreeing that the Ombudsman might copy and transfer the information (including his personal data) stated in the form to any person or organisation. Hence, the Privacy Commissioner found that the Ombudsman had not contravened DPP 3 of the PDPO by copying the decision letter which contained personal data to the Bureau upon obtaining the Appellant's consent for disclosing his personal data. The Privacy Commissioner therefore exercised the discretion under section 39(2)(d) of the PDPO not to conduct further investigation into the Appellant's complaint. 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) 申訴專員收集上訴人的個人資料的目的是為了處理上訴人的投訴。至於申訴專員其後把載有上訴人個人資料的信件抄送予該決策局，委員會認為申訴專員在抄送覆函時並沒有違反保障資料第3原則，因為所牽涉的個人資料均是用作處理投訴之用。

(2) 就上訴人提出「合理期望」的論點，委員會認為申訴專員已經在投訴表格內列明資料可以在投訴期間轉移給相關的人士或機構，而上訴人亦的確有在表格上簽署，同意披露有關資料。況且，上訴人在填寫表格時是可以選擇不同意其資料被披露給該決策局。委員會認為申訴專員並沒有超越上訴人就着自己的資料如何被使用的合理期望。

## The Appeal

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

(1) The purpose of collecting the Appellant's personal data by the Ombudsman was to handle the Appellant's complaint case. The AAB affirmed that the Ombudsman had not contravened DPP 3 by copying the decision letter which contained the Appellant's personal data to the Bureau as the personal data concerned was used for handling his complaint case.

(2) As regards the argument about "reasonable expectation" put forward by the Appellant, the AAB opined that the Ombudsman had already clearly stated in the complaint form that the information contained therein could be transferred to the relevant person or organisation for the purpose of handling the complaint, and the Appellant had indeed signed the complaint form and consented to such disclosure. Moreover, the Appellant could have selected not to disclose his personal data to the Bureau in the form. The AAB therefore considered that the use of personal data by the Ombudsman had not exceeded the reasonable expectation of the Appellant.

(3) 委員會認為上訴人並不能夠依賴「以往投訴」以支持其提出合理期望的說法。申訴專員解釋過去沒有抄送上訴人的「以往投訴」結果給相關決策局，是因為該些投訴被申訴專員評為「不予跟進」或「不展開調查」，故對涉事的決策局參考價值不大。相反，在本案中，申訴專員的確把上訴人的案件評為「可跟進」，並就上訴人的投訴展開了初步查訊。委員會認為申訴專員擁有酌情權去決定究竟把案件的結果信件抄送予相關的決策局是否有助促進公共行政的質素和水平，而該決定亦純屬申訴專員內部的行政決定。

(3) The Appellant could not rely on his "previous complaints" to support his line of argument on reasonable expectation for use of his personal data. The Ombudsman explained that the Appellant's "previous complaints" had not been copied to the relevant government bureaux because those previous complaint cases were either assessed by the Ombudsman as "not to be pursued" or "not to conduct investigation" and there was limited reference value to the government bureaux concerned. On the contrary, the Ombudsman had assessed the present case as one that could be "followed-up", and the Ombudsman had indeed conducted a preliminary inquiry on the Appellant's complaint case. The AAB was of the view that the Ombudsman had discretion to determine whether copying the decision letter to the relevant bureau might facilitate the improvement in the quality and standard of public administration, and it was purely the Ombudsman's internal administrative decision.

**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*
*吳凱欣署理律師代表私隱專員*

*申訴專員（受到遭上訴所反對的決定所約束的人）缺席聆訊*

**The AAB's Decision**

The appeal was dismissed.

*The Appellant appeared in person*
*Ms Annabel NG, Acting Legal Counsel represented the Privacy Commissioner*
*The Ombudsman (the Person bound by the decision appealed against) was absent*

# 附錄三
# APPENDIX 3

## 上訴個案簡述(二)

(行政上訴案件第7/2023號)

業主立案法團張貼包含上訴人個人資料的通告 — 採取補救措施 — 發出警告信 — 沒有送達執行通知 — 保障資料第3原則和《私隱條例》第50條

## Appeal Case Note (2)

(AAB Appeal No. 7 of 2023)

Posting of public notices containing the Appellant's personal data by Incorporated Owners – remedial measures taken – warning letter issued – no Enforcement Notice served – DPP 3 and section 50 of the PDPO

**聆訊委員會成員：** **馬嘉駿資深大律師(副主席) Mr Johnny MA Ka-chun, SC (Deputy Chairman)**
**Coram:** **許嘉俊先生(委員) Mr HASSAN Ka-chun (Member)**
**葉思進先生(委員) Mr YIP Sze-tsun (Member)**

**裁決理由書日期：** **2024年1月22日**
**Date of Decision:** **22 January 2024**

### 投訴內容

上訴人是某屋邨的居民(該屋邨)，並與該屋邨的業主立案法團(該業主立案法團)發生一些糾紛。上訴人投訴該業主立案法團在該屋邨的公共地方張貼通告(該通告)，當中披露他的姓氏、居住的大廈、其曾任該業主立案法團主席的事實，以及該業主立案法團與他之間發生的事情。

### The Complaint

The Appellant was a resident of an estate and was involved in some disputes with the Incorporated Owners of the estate. The Appellant complained that the Incorporated Owners displayed in public areas of the estate notices (the Notices) that disclosed his surname, the building he resided in, the fact that he was the Chairman of the Incorporated Owners and some past incidents that happened between the Incorporated Owners and himself.

## 私隱專員的決定

私隱專員認為該屋邨的居民能夠從該通告載有的資料中知悉上訴人的身分，因此，該業主立案法團在該通告中披露了上訴人的個人資料。

就上訴人個人資料的使用而言，私隱專員認為該業主立案法團當初收集上訴人的個人資料的目的是為了處理有關屋邨的管理事宜，而在該通告中披露上訴人的個人資料則是為了回應上訴人對該業主立案法團提出的指控，及向其他居民交待上訴人與該業主立案法團之間的糾紛。該披露的目的與當初收集上訴人個人資料的目的並非一致或直接有關，因此該業主立案法團被裁定違反《私隱條例》保障資料第3原則的規定。

考慮到該業主立案法團已經移除該通告，並同意不會在日後的通告披露上訴人的身分，私隱專員決定向該業主立案法團發出警告信，而沒有送達執行通知。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

## 上訴

上訴人指稱該業主立案法團並未於所聲稱的日期移除該通告。然而，委員會指出上訴人所依賴的證據是在他提出上訴後才提出的，而且不足以支持他的指控。

## The Privacy Commissioner's Decision

The Privacy Commissioner found that the Incorporated Owners had disclosed the personal data of the Appellant in the Notices as residents of the estate were able to ascertain the identity of the Appellant from the information contained in the Notices.

In relation to the use of the Appellant's personal data, the Privacy Commissioner considered that the original purpose of the collection of the Appellant's personal data was for the handling of matters relating to the management of the estate. On the other hand, the disclosure of the Appellant's personal data in the Notices was for the purpose of responding to the Appellant's allegations against the Incorporated Owners and explaining to other residents the disputes between the Appellant and the Incorporated Owners. The purpose of such disclosure was not consistent with or directly related to the original purpose of collection of the Appellant's personal data. Hence, the Incorporated Owners was found to have contravened the requirements of DPP 3 of the PDPO.

Having considered that the Incorporated Owners had already removed the Notices in question and agreed not to disclose the Appellant's identity in future notices, the Privacy Commissioner decided to issue a warning letter to the Incorporated Owners without serving an Enforcement Notice. Dissatisfied with the Privacy Commissioner's decision, the Appellant lodged an appeal with the AAB.

## The Appeal

The Appellant alleged that the Notices were not removed on the date claimed by the Incorporated Owners. However, the AAB noted that the evidence the Appellant sought to rely on in this regard was only raised after he had lodged the appeal, and was, in any event, insufficient to support his allegation.

就私隱專員是否應根據《私隱條例》第50條向該業主立案法團送達執行通知，私隱專員表示，在決定不向該業主立案法團送達執行通知前，已經考慮該案件的所有相關情況，包括按《私隱條例》第50(2)條，考慮該通告所關乎的違反是否已對或相當可能會對屬該違反所關乎的個人資料的資料當事人，造成損害或困擾。

委員會同意私隱專員的決定，認為沒有足夠證據顯示上訴人遭受的任何困擾或不便，是由於該業主立案法團在該通告中披露其個人資料而造成的。鑑於該業主立案法團已採取補救措施，委員會認為發出執行通知也不會達致實際或更佳的效果，並確認私隱專員不根據《私隱條例》第50條發出執行通知的決定。

**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*
*馮學晴署理律師代表私隱專員*

*該業主立案法團（受到遭上訴所反對的決定所約束的人）缺席聆訊*

Regarding whether an Enforcement Notice should have been served on the Incorporated Owners under section 50 of the PDPO, the Privacy Commissioner submitted that she had already considered all relevant circumstances of the case, including whether the contravention to which the Notices related had caused or was likely to cause damage or distress to the data subject concerned by the contravention as specified under section 50(2) of the PDPO, before coming to the decision not to serve an Enforcement Notice on the Incorporated Owners.

The AAB agreed with the Privacy Commissioner that there was insufficient evidence to show that any distress or inconvenience suffered by the Appellant was caused by the Incorporated Owners' disclosure of his personal data in the Notices. In view of the remedial measures taken by the Incorporated Owners, the AAB noted that the issuing of an Enforcement Notice would not bring about any practical effect or a more satisfactory result and upheld the Privacy Commissioner's decision not to issue an Enforcement Notice under section 50 of the PDPO.

**The AAB's Decision**

The appeal was dismissed.

*The Appellant appeared in person*
*Ms Dorothy FUNG, Acting Legal Counsel, represented the Privacy Commissioner*
*The Incorporated Owners (the Person bound by the decision appealed against) was absent*

# 附錄三
# APPENDIX 3

## 上訴個案簡述(三)

(行政上訴案件第9/2023號)

不公平及過度收集個人資料 — 個人資料的保安 — 保障資料第4原則 — 採取合理切實可行的保安措施 — 沒有發出執行通知

## Appeal Case Note (3)

(AAB Appeal No. 9 of 2023)

Unfair and excessive collection of personal data – security of personal data – DPP 4 – take reasonably practicable steps to safeguard personal data – no Enforcement Notice issued

**聆訊委員會成員：** **劉恩沛女士(副主席) Miss LAU Queenie Fiona (Deputy Chairman)**
**Coram:** **曾思進博士(委員) Dr TSANG Sze-chun (Member)**
**黃朝龍先生(委員) Mr Dennis WONG Chiu-lung (Member)**

**裁決理由書日期：** **2023年12月6日**
**Date of Decision:** **6 December 2023**

### 投訴內容

上訴人曾向某政府部門(該部門)提交一項申請。某日，上訴人的丈夫收到該部門的一名醫務社工來電，表示希望透過他聯絡上訴人以跟進上訴人的申請。上訴人提交該申請時並沒有向該部門提供其丈夫的手提電話號碼(該電話號碼)。上訴人認為該名醫務社工是從醫院管理局(醫管局)的電腦系統(該電腦系統)中取得該電話號碼，故向私隱專員投訴該部門(個案一)及醫管局(個案二)。

### The Complaint

The Appellant made an application to a government department (the Department). One day, the Appellant's husband received a phone call from a medical social worker of the Department who advised that he would like to contact the Appellant to follow up on her application. The Appellant had not provided her husband's mobile phone number when she submitted her application to the Department. She considered that the medical social worker might have obtained her husband's phone number from the computer system (the Computer System) of the Hospital Authority (the HA) and therefore lodged a complaint with the Privacy Commissioner against the Department (Complaint Case 1) and the HA (Complaint Case 2) respectively.

## 私隱專員的決定

### *個案一*

調查期間，該部門向私隱專員表示，該名醫務社工未能與上訴人取得聯絡，因此透過該電腦系統取得該電話號碼，致電上訴人的丈夫，希望透過他盡快與上訴人聯絡，以跟進上訴人的申請。

私隱專員認為該部門在上述情況下透過該電腦系統取得該電話號碼的做法屬於不公平，亦屬超乎適度，而事件中並無資料顯示該部門或該名醫務社工有任何急切性必須刻意從該電腦系統中查閱上訴人丈夫的電話號碼並透過他聯絡上訴人。因此，私隱專員認為該部門有關做法違反《私隱條例》下保障資料第1(1)及1(2)原則的規定，並向該部門發出警告信。該部門在事後亦採取改善措施，故私隱專員不擬就這宗個案向該部門發出執行通知。

### *個案二*

與此同時，私隱專員亦對醫管局展開了初步查詢。私隱專員審視了醫管局提供的資料，認為醫管局已採取合理切實可行的措施保障其電腦系統內病人的個人資料，因而並無違反保障資料第4原則的規定，故此私隱專員認為在此情況下毋須向醫管局發出執行通知。

上訴人不滿私隱專員的決定，遂向委員會提出上訴。

## The Privacy Commissioner's Decision

### *Complaint Case 1*

In the course of its investigation, the Department informed the Privacy Commissioner that the medical social worker had tried to contact the Appellant but in vain, and thus he had obtained her husband's phone number through the Computer System and attempted to contact the Appellant through her husband to follow up on her application.

The Privacy Commissioner considered that the Department's practice of collecting the husband's phone number through the Computer System was unfair and excessive in the circumstances, and there was no urgency for the Department or the medical social worker to obtain the husband's phone number through the Computer System to contact the Appellant. The Privacy Commissioner therefore concluded that the Department had contravened DPP 1(1) and 1(2) of the PDPO and issued a warning letter to the Department. Having considered the remedial actions taken by Department, the Privacy Commissioner decided not to issue an Enforcement Notice against the Department.

### *Complaint Case 2*

At the same time, the Privacy Commissioner conducted a preliminary enquiry with the HA. Having carefully examined the information provided by the HA, the Privacy Commissioner found that the HA had already taken reasonably practicable steps to safeguard the patients' personal data stored in the Computer System and there was no contravention of the requirements of DPP 4, and thus it was unnecessary to issue an Enforcement Notice against the HA.

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) 根據行政上訴案件2015年第54號的決定，保障資料第4原則下的責任，只是要求資料使用者「採取合理地切實可行的步驟」保障個人資料，而並非要不計算代價和可行性去採取任何步驟。

(2) 委員會認為個案涉及個別職員不當地收集個人資料，而並非源自醫管局系統的缺失，而醫管局已經有既定程序和指引處理違規行為，包括向違規職員作出訓示及督導。因此，委員會認為醫管局已採取合理切實可行的措施保障該電腦系統內病人的個人資料，並無違反保障資料第4原則的規定，故此委員會認為私隱專員在此情況下毋須向醫管局發出執行通知。

(3) 就上訴人提出的建議（即醫管局應在有關病人提出有關要求後才列印或轉移有關的個人資料予該部門，而並非將整個系統的存取權開放予該部門）（該建議），委員會認同私隱專員的決定，在醫管局沒有違反保障資料第4原則的情況下，醫管局是否更改其現行做法或採納上訴人的建議，純粹屬於醫管局的內部決定。

## The Appeal

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

(1) According to the decision in AAB No. 54 of 2015, DPP 4 only requires a data user to take all "reasonably practicable steps" in safeguarding the security of personal data and does not require a data user to take every step irrespective of the cost and feasibility.

(2) The AAB took the view that the incident was caused by the unfair collection of personal data by an individual staff member but not deficiencies in the HA's system. The HA had already put in place relevant procedures and guidelines to handle cases involving misuse of personal data (such as warning the staff involved and implementing enhanced supervision). Hence, the AAB considered that the HA had taken reasonably practicable steps in safeguarding patients' personal data stored in the Computer System and there was no contravention of DPP 4 on the part of the HA. Therefore, the AAB agreed that it was unnecessary for the Privacy Commissioner to issue an Enforcement Notice in such circumstances.

(3) Regarding the suggestion put forward by the Appellant (i.e. the HA should print or transfer the relevant personal data to the Department upon the request of the patient, instead of granting full access to the entire system) (the Suggestion), the AAB agreed with the Privacy Commissioner's decision that, in the absence of any contravention of DPP 4 by the HA, the decision of whether to change its existing arrangement or adopt the Appellant's Suggestion remained an internal decision of the HA.

(4) 即使上訴人不同意私隱專員所引用的統計數據(即該部門每年需要處理醫務社會服務的申請數目龐大)以反駁上訴人提出的指稱及該建議，委員會認為這項爭議並不足以推翻私隱專員的決定。

**行政上訴委員會的決定**

委員會駁回本上訴。

*上訴人授權他人代表應訊*

*周沅瑩律師代表私隱專員*

*該部門及醫管局(受到遭上訴所反對的決定所約束的人)缺席聆訊*

(4) Even if the Appellant disagreed with the statistical data quoted by the Privacy Commissioner (i.e. the number of medical social services applications handled by the Department annually was substantial) to rebut the Appellant's allegation and the Suggestion, the AAB was of the view that this dispute was insufficient to overturn the Privacy Commissioner's decision.

**The AAB's Decision**

The appeal was dismissed.

*The Appellant authorised another person to appear on her behalf*

*Ms Stephanie CHAU, Legal Counsel, represented the Privacy Commissioner*

*The Department and the Hospital Authority (the Persons bound by the decision appealed against) were absent*

# 附錄三
# APPENDIX 3

## 上訴個案簡述(四)

(行政上訴案件第15/2023號)

《私隱條例》第48及50條賦予私隱專員酌情權 — 衡量私隱專員的決定是否原則上犯錯或在任何方面屬於過度

## Appeal Case Note (4)

(AAB Appeal No. 15 of 2023)

Sections 48 and 50 of the PDPO confer discretionary power on the Privacy Commissioner – consider whether the Privacy Commissioner's decision is either wrong in principle or in any way excessive

**聆訊委員會成員：** **馬淑蓮女士(副主席) Ms Jay MA Suk-lin (Deputy Chairman)**
**Coram:** **李慕潔女士(委員) Miss Rebecca LEE Mo-kit (Member)**
**陳德鳴先生(委員) Mr CHAN Tak-ming (Member)**

**裁決理由書日期：** **2024年1月12日**
**Date of Decision:** **12 January 2024**

### 投訴內容

上訴人為某服務視障人士的機構(該機構)的會員。於2022年某日，上訴人致電電台，並在財政司司長答問大會上表達意見，期間提及該機構於疫情期間的表現。其後，該機構在其「資訊通服務系統」(一般熱線)中向會員發布通告，交代及回應有關上訴人於電台節目中的言論(該通告)，當中披露了上訴人的姓名及其作為該機構會員代表的身分。

上訴人不滿該機構的做法，遂向私隱專員作出投訴。

### The Complaint

The Appellant was a member of an organisation that serves people with visual impairments (the Organisation). On a day in 2022, the Appellant called in to a radio station and expressed his opinion about the Organisation, including its performance during the pandemic, during the Financial Secretary's question-and-answer session. Subsequently, the Organisation published a notice (the Notice) to its members through its information service hotline (the General Hotline) addressing and responding to the Appellant's opinion made on the radio programme. The Notice disclosed the Appellant's name and identity as a representative of members of the Organisation.

The Appellant was dissatisfied with the Organisation's actions and lodged a complaint with the Privacy Commissioner.

## 私隱專員的決定

經考慮調查所得的相關資料及證據後，私隱專員認為該通告提及上訴人的姓名、該機構會員代表的身分及上述事件的經過，披露了上訴人的個人資料，該披露的目的與當初收集上訴人個人資料的目的並非一致或直接有關，而且該機構亦沒有必要在該通告中披露上訴人的個人資料。因此，私隱專員認為該機構違反《私隱條例》下保障資料第3原則的規定。

然而，考慮到該機構已從一般熱線中移除該涉及上訴人的通告，糾正了違反保障資料第3原則的行為，並向私隱專員作出書面確認，日後在類似本個案的情況下，除非已取得資料當事人的訂明同意，否則不會將其個人資料披露予其他與事件無關的人士（包括該機構的會員），並只會按「需要知道」的原則，將足夠但不得超乎適度的資料披露予有需要知悉有關資料的會員，私隱專員不擬向該機構發出執行通知，並決定向該機構發出警告信，促請該機構日後須緊遵《私隱條例》的相關規定。

上訴人認為私隱專員應該發出執行通知，並公開調查報告，遂向委員會提出上訴。

## The Privacy Commissioner's Decision

After considering the relevant information and evidence obtained from the investigation, the Privacy Commissioner was of the view that, by including the Appellant's name and identity as a representative of the members of the Organisation, as well as the details of the abovementioned incident, the Organisation had disclosed the Appellant's personal data with a purpose different from, and not directly related to, the purpose of collection of his personal data, and it was not necessary for the Organisation to disclose the Appellant's personal data on the Notice. Thus, the Privacy Commissioner considered that the Organisation had contravened DPP 3 under the PDPO.

That said, having considered that the Organisation had removed the Notice relating to the Appellant from the General Hotline and rectified the contravention of DPP 3, and provided written confirmation to the Privacy Commissioner that, should they encounter similar incidents in the future, they would not disclose personal data of data subjects to individuals unrelated to the incident (including members of the Organisation) unless with the data subject's prescribed consent, and would only disclose the data that was adequate and not excessive to members on a need-to-know basis, the Privacy Commissioner decided not to issue any Enforcement Notice to the Organisation but instead issued a warning letter, urging compliance with the relevant requirements under the PDPO.

The Appellant was of the view that the Privacy Commissioner should have issued an Enforcement Notice and published an investigation report, and subsequently 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該上訴：

(1) 《私隱條例》第48及50條均說明了私隱專員可採取合適的做法發出執行通知或公開調查報告。這說明了私隱專員根據條例獲賦予相關的酌情權。但酌情權並不是絕對的，行使酌情權需符合法例的真正原意及意思，私隱專員只能為着達到條例相關目的而有效地行使酌情權，而在行使酌情權作出決定時，私隱專員只能考慮相關的因素並須排除無關的因素。

(2) 即使委員會在行使相關條例賦予委員會的酌情權時，委員會在接納遭上訴的決定前也須衡量私隱專員的決定是否原則上犯錯或在任何方面屬於過度。根據案例，委員會在作出衡量時需要考慮私隱專員在作出決定時有否不合理或不合比例地行使其酌情權。

## The Appeal

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

(1) Sections 48 and 50 of the PDPO stated that the Privacy Commissioner may take appropriate actions in issuing Enforcement Notices or publishing investigation reports. They showed that discretionary power had been conferred upon the Privacy Commissioner under the PDPO. However, the discretionary power was not absolute. The exercise of discretionary power depended on the true intent and meaning of the empowering statute. The Privacy Commissioner could only validly exercise the discretion for reasons relevant to the achievement of the purpose of the statute, and upon exercising the discretion in making a decision, the Privacy Commissioner should take into account the relevant considerations and exclude irrelevant ones.

(2) Even when the AAB exercised the discretionary power conferred upon it by the relevant provisions, the AAB would also need to consider whether the Privacy Commissioner's decision, which is the subject of the appeal, was wrong in principle or in any way excessive before accepting the decision being appealed against. According to case laws, the AAB would need to consider whether the Privacy Commissioner had exercised the discretionary power unreasonably or disproportionately in making the decision.

(3) 就不發出執行通知的決定而言，委員會認為由於該機構已將該通告刪除，所以即使私隱專員根據《私隱條例》第50條向該機構發出執行通知，該執行通知也不能帶來更有效及更滿意的效果。委員會亦觀察到私隱專員在作出其決定前及在處理案件時所考慮的事項，認為私隱專員在作出該決定而行使酌情權的時候沒有任何原則上犯錯或在任何方面屬於過度。

(3) Regarding the decision not to issue an Enforcement Notice, the AAB was of the view that since the Organisation had removed the Notice, even if the Privacy Commissioner issued an Enforcement Notice to the Organisation in accordance with section 50 of the PDPO, the Enforcement Notice would not have led to a more effective and satisfactory result. The AAB also noted the factors that the Privacy Commissioner had taken into consideration before making the decision as well as the handling of the incident and considered that the exercise of discretionary power by the Privacy Commissioner was neither wrong in principle nor in any way excessive.

(4) 委員會同意其司法管轄權並不包括私隱專員不公開調查報告的決定。而即使委員會有這方面的司法管轄權，委員會亦認為私隱專員在行使酌情權不公開相關調查報告的決定並沒有不合理或不合比例之處。

(4) The AAB agreed that its jurisdiction did not include the Privacy Commissioner's decision not to publish the investigation report. Even if the AAB had jurisdiction over the issue, the AAB considered that the Privacy Commissioner's exercise of discretionary power in not publishing the investigation report was neither unreasonable nor disproportionate.

**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*
*周沅瑩律師代表私隱專員*

*該機構（受到遭上訴所反對的決定所約束的人）缺席聆訊*

**The AAB's Decision**

The appeal was dismissed.

*The Appellant appeared in person*
*Ms Stephanie CHAU, Legal Counsel, represented the Privacy Commissioner*
*The Organisation (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

### 僱主在未確定聘任求職者前收集其香港身份證及銀行卡副本 — 保障資料第1原則 — 個人資料的收集

### Case 1

### Collection of copies of Hong Kong Identity Card and bank card from a job applicant by an employer prior to the acceptance of employment offer – DPP 1 – collection of personal data

**投訴內容**

投訴人於某公司的分店應徵工作並進行面試。完成面試後，職員要求影印投訴人的香港身份證及銀行卡（該些文件），以便將該些文件的副本交予人事部處理合約及安排值勤。其後，投訴人曾聯絡該公司了解申請結果惟沒有回音。投訴人不滿該公司於未確定聘用他的情況下收集該些文件的副本，遂向私隱專員公署投訴。

**The Complaint**

The complainant applied and interviewed for a job at a branch of a company. After the interview, the staff of the company requested to make a copy of the complainant's Hong Kong Identity Card (HKID Card) and bank card (the Documents) in order to submit the same to the Human Resources Department for contract preparation and job allocation purposes. Thereafter, the complainant asked the company about the outcome of his job application but did not receive any response. The complainant was dissatisfied that the company collected the copies of the Documents prior to confirming his employment offer, and hence lodged a complaint with the PCPD.

**結果**

該公司向私隱專員公署表示投訴人已在分店通過面試，而分店經理就此認為投訴人已獲取錄，故即時影印了該些文件供區域經理批核。然而，在區域經理批核投訴人的申請時，由於當時人手已經足夠，故沒有接納投訴人的申請。

**Outcome**

The company explained to the PCPD that the complainant had passed the interview at the branch, and the branch manager considered the application successful. In the circumstances, the Documents were copied and passed to the district manager for vetting purposes. However, during the vetting process, the district manager considered that the company had sufficient manpower and the complainant's application was thus rendered unsuccessful.

經私隱專員公署介入後，該公司修訂收集求職者個人資料方面的指引，訂明直至與獲聘的求職者簽約或員工履新時，才會收集該些文件的副本。

Upon the PCPD's intervention, the company revised its guidelines relating to the collection of personal data from job applicants. According to the revised guidelines, the company would only collect copies of the Documents at the time the selected job applicant signed the contract or during the onboarding process.

私隱專員公署就事件向該公司發出警告信，要求該公司定期向職員傳閱已修訂的指引，確保職員緊遵有關收集求職者個人資料方面的規定。

The PCPD also issued a warning letter to the company, requesting it to recirculate the revised guidelines regularly to ensure that staff adhered to the relevant requirements regarding the collection of personal data from job applicants.

**借鑑**

根據私隱專員公署發出的《身份證號碼及其他身份代號實務守則》(該守則)，雖然僱主可根據該守則收集僱員的身份證副本，以證明僱主有遵守《入境條例》(香港法例第115章)第17J條的規定，即在聘用僱員前已核查該名僱員的身份證。然而，該守則亦清楚指出，直至成功聘用有關求職者前，僱主不應收集其身份證副本。此外，私隱專員公署發出的《人力資源管理實務守則》中亦同樣重申，僱主不應在招聘過程中收集求職者的身份證副本，除非及直至有關求職者已接受聘任。

**Lessons Learnt**

In accordance with the "Code of Practice on the Identity Card Number and Other Personal Identifiers" (the Code) issued by the PCPD, employers are permitted to collect a copy of a HKID card in order to provide proof of compliance with section 17J of the Immigration Ordinance (Chapter 115 of the Laws of Hong Kong), which provides that the employer shall inspect the HKID Card of a prospective employee before employing him/her. However, it is also highlighted in the Code that the employer shall not collect any HKID Card copy until the applicant is successfully recruited. In addition, as reiterated in the "Code of Practice on Human Resource Management" issued by the PCPD, an employer should not collect a copy of the HKID Card of a job applicant during the recruitment process unless and until the applicant has accepted an offer of employment.

香港身份證副本載有重要及敏感的個人資料，各機構應以此案為鑑，確保負責招聘程序的職員不會在求職者接受聘任前收集其香港身份證副本。同樣地，如求職者並未接受聘任，機構無必要收集其銀行戶口資料以作發薪之用。

A HKID Card copy contains important and sensitive personal data. Organisations shall take this case as an example to ensure the recruitment staff shall not collect the HKID Card copy of a job applicant unless and until the job applicant has accepted an offer of employment. Similarly, if a particular applicant has not accepted an offer of employment, it is not necessary to collect the bank account information for payroll purposes.

# 附錄四
# APPENDIX 4

## 個案二

### 流動Wi-Fi數據機租借公司對客戶個人資料所採取的保安措施不足 — 保障資料第4原則 — 個人資料的保安

**投訴內容**

投訴人是一家流動Wi-Fi數據機租借公司(該公司)的客戶。他在該公司位於香港國際機場的櫃台提取Wi-Fi數據機時留意到，該公司使用的簽收表格讓客戶在簽收時可以查閱到其他簽收客戶的個人資料，包括英文全名、租借時段及目的地。另一方面，該公司亦在非營業時間未有安排員工當值時，將該簽收表格放置在櫃台供客戶自行簽收，以致客戶的個人資料有可能被他人查閱。

**結果**

經私隱專員公署介入後，該公司已修改共用簽收表格的格式，當中包括移除表格上目的地一欄，而姓名一欄中只顯示客戶的姓氏和名字的首字母，令他人不能從簽收表格上有限的資料確定客戶身分。此外，該公司並以非透明的紙張遮蓋簽收表格上其他人士的資料，以防他人意外地查閱到簽收表格上的客戶個人資料。

## Case 2

### Mobile Wi-Fi device rental company took inadequate security measures to protect customers' personal data – DPP 4 – security of personal data

**The Complaint**

The complainant was a customer of a mobile Wi-Fi device rental company (the Company). While picking up a Wi-Fi device at the Company's counter located at the Hong Kong International Airport (the Counter), the complainant noticed that the acknowledgment of receipt form (the Form) allowed him to access personal data of other customers, including their full English names, rental periods and destinations. The Company also left the Form unattended at the Counter during non-business hours and customers were required to acknowledge receipt of the Wi-Fi devices on their own. This situation might lead to unauthorised access to customers' personal data.

**Outcome**

After the PCPD's intervention, the Company revised the format of the Form, namely, removing the "destination" column and displaying only the customer's family name with the initial of the given name so that the identity of the customer could not be ascertained from the limited information available on the Form. In addition, the Company covered the Form with non-transparent sheets to avoid accidental access to customers' personal data on the Form.

私隱專員公署亦就事件向該公司發出勸諭信，要求他們採取切實可行的措施，以確保客戶的登記資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用。同時要求他們提供員工培訓，以提高員工對保障個人資料私隱的意識。

The PCPD issued an advisory letter to the Company in response to the incident, requesting it to take all practicable measures to protect the registration data of customers against unauthorised or accidental access, processing, erasure, loss or use. Meanwhile, the Company was requested to provide training to staff to raise their awareness of personal data privacy protection.

## 借鑑

資料使用者採用共用表格登記個人資料的做法非鮮見，惟有關做法或會令客戶查閱到早前已登記人士的個人資料，以致客戶的個人資料外洩，做法不可取。私隱專員公署明白在個案中，有關的資料使用者鑑於其實際營運模式難以安排員工24小時當值以協助客戶完成簽收程序，在這情況下，資料使用者更應從簽收表格的格式著手，只顯示簽收所須的資料，以減低客戶資料外洩的風險。同時，資料使用者亦可考慮將簽收程序電子化，以電腦系統取代實體的共用簽收表格，避免客戶在簽收時查閱到其他客戶的資料，以確保客戶的個人資料私隱受到更妥善的保障。

## Lessons Learnt

The use of common forms by data users to record personal data is not uncommon. However, this practice is not advisable as it may lead to customers accessing the personal data of previous registrants, resulting in leakage of customers' personal data. Considering the business operation model in the present case, the PCPD understands that it may be impracticable for the Company to arrange staff to be available around the clock to complete the pick-up procedures. To minimise the risk of personal data leakage, data users should focus on the format of the acknowledgment form by displaying only the necessary information for the purpose of acknowledging receipt. Meanwhile, data users may consider digitising such processes by using a computer system instead of physical common forms. As such, customers would not have access to other customers' personal data when completing the acknowledgment procedures, thereby ensuring better protection of customers' personal data privacy.

# 附錄四
# APPENDIX 4

## 個案三

### 網店透過未加密的網絡連結向客戶發送載有個人資料的訂單發票 — 保障資料第4原則 — 個人資料的保安

**投訴內容**

投訴人在一間網上家電店(該網店)購物後，收到由該網店提供載有其訂單發票的網絡連結(該連結)。投訴人發現該連結未有加密，只要通過修改該連結尾段的五位數字，便可閱覽該網店其他客戶的訂單發票，當中載有他們的姓名、電話號碼、電郵地址、送貨地址和購物詳情等訂單資料。投訴人認為該網店對客戶的個人資料保安不足，遂向私隱專員公署投訴該網店。

**結果**

經私隱專員公署介入後，該網店已即時糾正有關問題，任何人士均不能再透過該連結或修改該連結的數字，閱覽任何訂單發票上的資料。同時，為避免同類情況再次發生，該網店承諾日後會以可攜式文件格式(即PDF)向客戶發送訂單發票，以取代以網絡連結提供訂單發票的做法。

## Case 3

### An online store sent invoices containing personal data to customers via unencrypted weblinks – DPP 4 – security of personal data

**The Complaint**

The complainant received an unencrypted weblink (the Weblink) to access his invoice after making a purchase at an online store for home appliances (the Store). The complainant discovered that the weblink was not encrypted, and by modifying the last five digits of the Weblink, he could gain access to other customers' invoices, which contained order information including their names, phone numbers, email addresses, delivery addresses and purchase details. The complainant was of the view that the Store had failed to safeguard the customer's personal data and hence lodged a complaint against the Store with the PCPD.

**Outcome**

After the PCPD's intervention, the Store promptly rectified the problem. External access to the information contained in the invoices was no longer possible by clicking on the Weblink or modifying the digits of the Weblink. To prevent the recurrence of similar incidents, the Store pledged that invoices containing personal data would be sent to customers in portable document format (PDF) in the future, instead of providing them with weblinks.

私隱專員公署就事件向該網店發出警告信，要求該店日後在處理客戶的個人資料時務必緊遵《私隱條例》的規定，採取所有切實可行的步驟，以確保持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。

The PCPD issued a warning letter to the Store, requiring it to strictly comply with the relevant requirements of the PDPO on handling customers' personal data by taking all practicable steps to ensure that any personal data held by it was protected against unauthorised or accidental access, processing, erasure, loss or use.

## 借鑑

本案源於該網店以網絡連結向客戶發送訂單發票時，未有採取嚴謹的保安措施，防止指定客戶以外的人士閱覽發票上所載的個人資料，亦沒有察覺藉修改網絡連結的數字可導致其他客戶的訂單資料遭查閱的漏洞。機構在實施任何涉及處理個人資料的程序前，應對個人資料在傳輸和儲存方面進行全面的風險評估，例如採用適當的加密工具保障所傳送的個人資料，藉此識別任何數據安全的漏洞，以減低個人資料外洩的風險及恪守《私隱條例》的相關規定。

## Lessons Learnt

The primary cause of the complaint pertaining to the use of weblinks to provide customers with their respective invoices stemmed from the Store's failure to adopt stringent security measures to protect the personal data of designated customers from any unauthorised access, or to detect the vulnerability arising from the modification of the weblinks. Prior to engaging in any practices that would involve the handling of personal data, organisations should conduct thorough risk assessments regarding the transmission and storage of personal data. This may include using adequate encryption tools to safeguard the transmitted personal data thereby identifying any vulnerabilities in their data security. This can minimise the risk of exposing the customers' personal data and ensure compliance with the relevant requirements under the PDPO.

# 附錄四
# APPENDIX 4

## 個案四

### 學校在處理個人資料時的不當行為 — 保障資料第1原則 — 個人資料的收集 — 保障資料第3原則 — 個人資料的使用 — 保障資料第5原則 — 公開個人資料方面的政策及實務

## Case 4

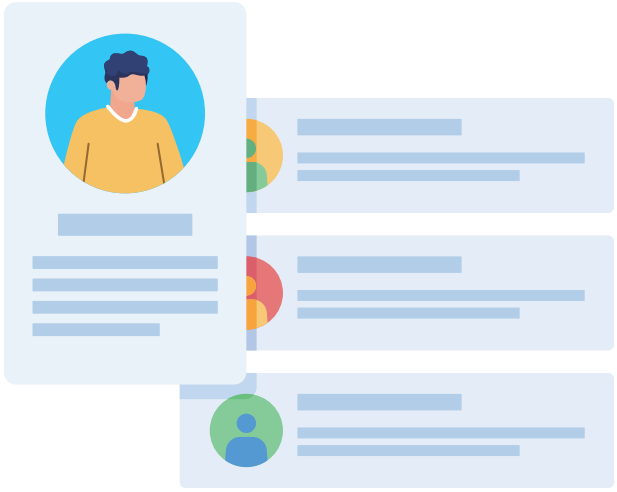
### A school's malpractice in handling personal data – DPP 1 – manner of collection of personal data – DPP 3 – use of personal data – DPP 5 – make personal data policies and practices known

**投訴內容**

投訴人對他們子女就讀的學校(該學校)作出投訴，指該學校使用不同表格(該些表格)收集個人資料以用作處理入學申請、記錄進出及問卷調查時，並未告知資料當事人(即該學校的學生、家長及校友)該些表格收集個人資料的目的。投訴人亦指出該學校在未取得他們同意的情況下將投訴人子女的照片披露在該學校的網站上。此外，該學校未有提供一份清晰的私隱政策述明校方會如何使用在學生學習期間所收集的個人資料。

**The Complaint**

The complainants lodged a complaint against the school (the School) attended by their children for using different forms (the Forms) to collect personal data for school admissions, visit records and a questionnaire, and that the data subjects, namely, students, parents and alumni, were not informed of the purposes of the personal data collection via the Forms. They also complained that the School disclosed photos of their children on the School's website without their consent. Furthermore, the School did not have a clear privacy policy specifying how the data collected during the students' attendance would be used.



## 結果

根據所得資料，私隱專員公署認為該學校違反了《私隱條例》下的保障資料第1(3)原則、第3原則及第5原則，詳情如下：

私隱專員公署檢視了該些表格，發現他們未有以收集個人資料聲明或等同文件的方式，提供保障資料第1(3)原則所規定的全部或部分的資訊。因此，該學校違反了保障資料第1(3)原則。

有關未經同意在該學校的網站上發布學生照片一事，私隱專員公署認為在拍攝照片時，學生及／或其家長或未有預期其照片會被發布及公開披露。因此，學生的個人資料被學校用於新目的，但該學校未有就該新目的取得當事人同意，因而違反了保障資料第3原則。

另一方面，私隱專員公署發現該學校在相關時間並沒有在其網站上提供私隱政策聲明或其等同文件，以確保資料當事人獲悉該學校在處理個人資料方面的私隱政策及實務，因此違反了保障資料第5原則。

## Outcome

Based on the information obtained, the PCPD found that the School had contravened DPP 1(3), DPP 3 and DPP 5 of the PDPO in the following ways:

The PCPD reviewed the Forms and found that the requisite information as stipulated under DPP 1(3), either in the form of a Personal Information Collection Statement (PICS) or its equivalent, was missing in part or in whole from the Forms. As such, the School had contravened DPP 1(3).

Regarding the publication of the students' photos on the School's website without consent, the PCPD considered that the students and/or their parents might not expect those photos would be published and made available to the public when they were taken. Therefore, the students' personal data had been used for a new purpose by the School. As no consent was obtained for such new purpose, the School had contravened DPP 3.

Moreover, the PCPD discovered that the School did not have a Privacy Policy Statement (or its equivalent) available on the School's website at the material time to allow the data subjects to be informed of its privacy policies and practices in relation to the personal data it handled, and hence was in contravention of DPP 5.

經私隱專員公署介入後，該學校採取了以下補救措施：

- 修改該些表格並加入收集個人資料聲明以提供以下相關必要資訊：(i)收集資料的目的；(ii)填表人士是否必須抑或可自願提供該等資料，以及不提供該等資料的後果；及(iii)該等人士要求查閱及改正資料的權利，以及處理該等要求的負責人的聯絡資料；

- 從該學校網站上移除相關學生的照片，並向所有家長發出了一份附回條的通告，以獲取家長同意在該學校網站及刊物上使用學生的照片及作品；

- 在該學校的網站上公開其私隱政策聲明及相關指引以述明學校在收集及使用個人資料方面的政策及實務；及

- 該學校確認將繼續致力保障其收集所得的個人資料以保護資料當事人的私隱，例如安排教職員參與有關保障個人資料的培訓。

考慮到該學校所採取的補救措施，私隱專員公署向該學校發出警告信，要求該學校日後在處理個人資料時須嚴格遵守相關規定，包括但不限於《私隱條例》下的保障資料原則。

Upon the intervention of the PCPD, the School has taken the following remedial actions:

- Revised the Forms by adding the PICS and including the requisite information on (i) the purpose of collection of the data; (ii) whether it is obligatory or voluntary for individuals to supply their data, and the consequences for failure to comply; and (iii) the rights to request access to and correction of the data, as well as the contact details of the individual designated to handle the data access and correction requests;

- Removed the relevant students' photos from the School's website, and issued a notice with a reply slip to obtain parental consent for using students' photographic images and works on the School's website and its publications;

- A Privacy Policy Statement and relevant guidelines in relation to the policies and practices of the collection and use of personal data are available on the School's website; and

- The School confirmed that it would continue to make every effort to safeguard personal data collected in order to protect the privacy of the data subjects, including arranging personal data protection training for staff members.

Taking into account the remedial actions of the School, the PCPD issued a warning letter to the School requesting it to strictly comply with the relevant requirements, including but not limited to observing the DPPs under the PDPO, when handling personal data in the future.

## 借鑑

由於學校在日常運作中可能需要頻繁地收集和使用學生及其家長的個人資料，因此在處理這些個人資料時應時刻保持謹慎，並重視資料當事人的個人資料私隱權利。具體而言，學校應透過提供收集個人資料聲明或等同文件以述明其收集個人資料的目的。此外，學校亦應在其網站上提供其私隱政策及實務，以便各持份者查閱。

本個案突顯了該學校缺乏尊重個人資料私隱的意識及忽略其重要性。作為學生的照顧者，學校理應致力保護兒童私隱。就此，學校應主動並定期審視其日常運作（包括在更新學校網站時）對私隱的潛在影響。當學校因新目的而上載學生照片至其網站時，應在發布前先取得有關人士的同意。

## Lessons Learnt

As schools may frequently collect and use the personal data of students and parents in their day-to-day operation, they should be cautious in the handling of that personal data and put sufficient weight on the data subjects' personal data privacy rights. In particular, schools should specify the collection purposes of the personal data by way of providing a PICS or its equivalent. Moreover, their privacy policies and practices should also be made readily available on their websites so they can be easily accessed by the parties concerned.

The matters in this case demonstrated the School's lack of awareness of the importance of respecting personal data privacy. As the carer of their students, schools should endeavour to protect children's privacy. In this regard, schools should take initiatives to conduct regular reviews of any potential privacy impact of their daily working procedures, including the updating of their websites. Whenever students' photos are uploaded for a purpose different from that for which they were collected, consent from the relevant persons should be sought beforehand.

# 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 Case 1

### 電訊公司沒有依從客戶的拒收直銷訊息要求，繼續使用其個人資料作直接促銷 — 《私隱條例》第35G條

### A telecommunications company failed to comply with the opt-out request from a customer to cease using his personal data in direct marketing – section 35G 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：** | **2024年2月20日** |
| **Date of Decision:** | **20 February 2024** |

**投訴內容**

投訴人是一間電訊公司的客戶，並曾向該公司提供他的個人資料。投訴人其後透過電郵向該公司作出拒收直銷訊息的要求，並獲該公司書面確認收悉有關要求。然而，投訴人其後仍先後兩次分別收到該公司推廣其服務的來電及電郵。

**The Complaint**

The complainant was a customer of a telecommunications company who had provided his personal data to the company. Subsequently, the complainant made a request to the company by email to opt out of direct marketing. Receipt of the same was acknowledged by the company in writing. However, the complainant later, on two occasions, received a call and an email respectively from the company promoting its services.

## 結果

該公司被票控兩項違反《私隱條例》第35G(3)條罪行，沒有依從資料當事人的要求繼續使用其個人資料作直接促銷。該公司承認傳票控罪，每張傳票分別被判罰款港幣2,000元，合共港幣4,000元。

## 借鑑

市民對保障其個人資料私隱的意識日漸提升，機構更需尊重客戶對其個人資料使用於直接促銷的意願。為避免類似情況再次發生，機構應定期更新拒收直銷訊息名單，並加強員工在依從客戶拒收直銷訊息要求的培訓，確保他們對《私隱條例》下有關直接促銷的規定有充分的認知。資料使用者一旦違反《私隱條例》第35G條的規定，即屬違法，一經定罪，可處罰款港幣50萬元及監禁三年。

## Outcome

The company was summoned for two offences of failing to comply with the request from a data subject to cease using his personal data in direct marketing, contrary to section 35G(3) of the PDPO. The company pleaded guilty to the offences and was fined HK$2,000 for each summons, totalling HK$4,000.

## Lessons Learnt

As the public becomes more aware of the need to protect the privacy of their personal data, organisations need to respect their customers' choices about the use of their personal data in direct marketing. To prevent recurrence of similar cases, organisations should regularly update opt-out lists and strengthen the training of staff on complying with customers' opt-out requests to ensure that they are fully aware of the requirements relating to direct marketing under the PDPO. A data user who contravenes the requirements of section 35G under the PDPO commits an offence and is liable on conviction to a fine of HK$500,000 and to imprisonment for three years.

# 附錄五
# APPENDIX 5

## 個案二

## 兩人發生金錢糾紛，第三者知情後在網上將當中一人「起底」—《私隱條例》第64(3A)條

## Case 2

## After learning about a monetary dispute between two individuals, a third party doxxed one of them online – section 64(3A) of the PDPO

| | |
|---|---|
| **法院：** | **沙田裁判法院** |
| **Court:** | **Shatin Magistrates' Court** |
| **審理裁判官：** | **陳慧敏署理主任裁判官** |
| **Coram:** | **Ms CHAN Wai-mun, Acting Principal Magistrate** |
| **裁決日期：** | **2024年1月12日** |
| **Date of Decision:** | **12 January 2024** |

### 投訴內容

投訴人於2020年曾經與另一名人士發生金錢糾紛。及至2022年9月及12月，被告在社交媒體平台上發布了兩條載有投訴人個人資料的訊息，要求投訴人還款。投訴人被披露的個人資料包括英文姓名、手提電話號碼、相片及香港身份證副本，從中可以看到投訴人的中文姓名、英文姓名、香港身份證號碼、出生日期、性別，以及事主的照片等。

### The Complaint

In 2020, the complainant had a monetary dispute with a third party. Subsequently, the defendant posted two messages containing the complainant's personal data on a social media platform, one in September and one in December 2022, demanding repayment of the outstanding loan from the complainant. The personal data disclosed included the complainant's English name, mobile phone number, his photos and a copy of the complainant's HKID Card, which showed particulars of his Chinese name, English name, HKID Card number, date of birth, gender and a photo of him, etc.

### 結果

於2024年1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，法院判處被告監禁兩個月，緩刑兩年。

### Outcome

The defendant was convicted of two charges of contravening section 64(3A) of the PDPO, "disclosing personal data without data subject's consent", in January 2024 upon his guilty plea. The Court sentenced the defendant to two months' imprisonment, suspended for two years.

### 借鑑

身份證載有敏感的個人資料，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 up to HK$1,000,000 and imprisonment up to five years.

# 附錄五
# APPENDIX 5

## 個案三

## 女子在互聯網上披露鄰居夫婦的個人資料 —《私隱條例》第64(3A)條

## Case 3

## A female disclosed personal data of her neighbours on the Internet – section 64(3A) of the PDPO

| | |
|---|---|
| **法院：** | **西九龍裁判法院** |
| **Court:** | **West Kowloon Magistrates' Court** |
| **審理裁判官：** | **蘇文隆主任裁判官** |
| **Coram:** | **Mr SO Man-lung, Don, Principal Magistrate** |
| **裁決日期：** | **2024年3月8日** |
| **Date of Decision:** | **8 March 2024** |

### 投訴內容

兩名投訴人是夫婦，被告是他們的鄰居，兩戶素有積怨。2022年3月，兩名投訴人與被告發生爭執，期間被告以手提電話錄影兩名投訴人。翌日至2022年5月期間，被告在一個社交媒體平台的兩個公開群組先後發布了四條包含兩名投訴人個人資料的帖文，該些帖文附有上述的錄影片段，並對兩名投訴人作出負面的評論和指控。

### The Complaint

The two complainants were a married couple, and the defendant was their neighbour. The relationship between two households had been tense because of previous grudges. In March 2022, a dispute arose between the defendant and the complainants, during which the defendant took a video of the complainants with her mobile phone. On the date following the dispute and until May 2022, four messages containing the personal data of the complainants, each with the said video attached, were posted in two open discussion groups on a social media platform, alongside some negative comments and allegations against the complainants.

**結果**

於2024年3月，被告在認罪下被裁定干犯四項《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，法院判處被告監禁兩星期，緩刑三年，並罰款港幣500元。

**借鑑**

「起底」並非解決衝突的適當途徑，也不是有效的方法。這種行為可能導致嚴重的法律後果，違例者一經定罪，可被處即時監禁。

**Outcome**

The defendant was convicted of four charges of contravening section 64(3A) of the PDPO, "disclosing personal data without consent", in March 2024 upon her guilty plea. The Court sentenced the defendant to two weeks' imprisonment, suspended for three years, and a fine of HK$500.

**Lessons Learnt**

Doxxing is neither an appropriate nor effective avenue for resolving conflicts. Such behaviour can also lead to serious legal repercussions, and offenders can be liable on conviction to immediate imprisonment.

# 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

### 即時通訊軟件帳戶遭騎劫 — 保障資料第4原則 — 個人資料的保安

### Case 1

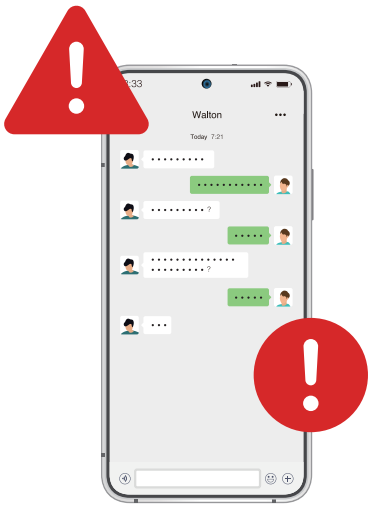
### Instant messaging account hijacking – DPP 4 – security of personal data

**背景**

私隱專員公署在本報告年度接獲23宗有關社福機構及學校的資料外洩事故通報，表示用作與服務使用者、學生及／或學生家長通訊的即時通訊軟件帳戶遭騎劫，騙徒繼而盜用有關即時通訊軟件帳戶假冒受害機構，向通訊錄的聯絡人發送訊息企圖騙取金錢。有關事件涉及近2,600名服務使用者、學生、學生家長及／或職員的姓名及手提電話號碼等個人資料。

**Background**

The PCPD received 23 data breach notifications from social welfare organisations and schools during this reporting year, reporting that their accounts on an instant messaging application, which was used for communication with service users, students and/or parents of students, had been hijacked. The fraudsters then impersonated the organisations and used the hijacked accounts to send messages to the contacts in the address books, attempting to swindle them. The incidents involved the personal data of nearly 2,600 individuals and the affected data included names and mobile phone numbers of service users, students, parents of students and/or staff members.



### 補救措施

私隱專員公署對涉事的社福機構及學校展開了循規審查，並向他們提供遵從《私隱條例》規定的建議。就此，該等社福機構及學校都加強了即時通訊軟件帳戶的保安措施，例如啟用帳戶的雙重認證功能、定期檢查已連結的裝置及登出不再使用或不明的裝置連結，並制訂指引向員工述明安全使用即時通訊軟件的注意事項，包括小心留意網頁連結，不要誤按虛假的即時通訊軟件網頁版，及切勿向他人透露任何密碼或驗證碼等。

### 借鑑

機構如使用即時通訊軟件與通訊錄的聯絡人溝通，應採取足夠的安全措施保障有關帳戶的安全，包括啟用雙重認證功能，定期更新軟件並留意官方發出的安全資訊，並就此制定合適的政策供員工依循。機構亦應就安全使用有關軟件向員工提供合適的培訓，並定期監察他們使用有關帳戶的情況，確保他們符合相關政策的規定。

### Remedial Measures

The PCPD initiated compliance checks against those social welfare organisations and schools and provided recommendations to them to ensure compliance with the provisions of the PDPO. In light of the incident, the social welfare organisations and schools enhanced the security measures of their instant messaging accounts. This included enabling two-factor authentication on the accounts, regularly checking linked devices in account settings and logging out of any devices that are no longer in use or are unknown to the users. Additionally, guidelines on precautions for using the instant messaging accounts were formulated for their staff members. These guidelines emphasised paying close attention to web links, avoiding clicking fake web versions of the instant messaging applications and not disclosing passwords or verification numbers to others.

### Lessons Learnt

If organisations are to use instant messaging applications to communicate with individuals in their contact lists, they should implement sufficient security measures to safeguard the security of the relevant accounts, including enabling two-factor authentication, regularly updating software, paying attention to official security information and formulating appropriate policies for staff members to follow. Organisations should provide appropriate training to staff members regarding the safe usage of the applications and regularly monitor their usage to ensure their compliance with the relevant policies.

# 附錄六
# APPENDIX 6

## 個案二

### 一名中學教師沒有適當地設定內部檔案的存取權限 — 保障資料第4原則 — 個人資料的保安

**背景**

一間中學向私隱專員公署通報，指一名教師在離職前將文件連同117名學生的個人資料製成雲端範本供內部使用。然而，該名教師沒有適當地設定有關檔案的存取權限，以致未經准許查閱的學生有機會查看該些檔案，當中載有117名學生的姓名、性別、就讀小學名稱、成績、跨境生和有特殊學習需要的學生標示及分班結果。

**補救措施**

在收到有關中學的通報後，私隱專員公署展開了循規審查，並向該中學提供遵從《私隱條例》規定的建議。該中學停止了所有用戶建立或使用雲端的範本功能，並制定守則述明教職員透過雲端分享檔案時需注意的事項，例如確保在分享檔案之前設定存取權限等。

## Case 2

### A secondary school teacher failed to properly configure access rights to an internal file – DPP 4 – security of personal data

**Background**

A secondary school reported to the PCPD that a departing teacher had customised a template on a cloud drive that included documents and personal data of 117 students, for internal use. However, the teacher failed to properly configure the access rights to the file, allowing unauthorised students to access the file. The file contained names, genders, names of primary school attended, academic results, indicators for cross-boundary students and students with special educational needs and class allocation results of the 117 students.

**Remedial Measures**

Upon receiving the notification from the secondary school, the PCPD initiated a compliance check and provided recommendations to the secondary school to ensure compliance with the provisions of the PDPO. The secondary school disabled the functions of creating and using custom templates on the cloud drive for all user accounts and formulated a code stipulating precautions when sharing files through cloud drives, such as ensuring that access rights are set before sharing the file, etc.

**借鑑**

學校使用資訊系統以處理學生個人資料實屬普遍，學校應制訂清晰而有效的資訊科技政策及程序，羅列教職員在使用資訊系統及軟件時應如何保障個人資料的安全，並採取措施確保負責處理學生個人資料的教職員遵從有關規定行事，減低出現人為錯誤的風險。

**Lessons Learnt**

It is common for schools to use information systems to process personal data of students. Therefore, schools should formulate clear and effective information technology policies that outline how to safeguard the security of personal data when using the information systems and applications. Schools should also devise measures to ensure staff members' compliance with relevant policies to mitigate the risks of human error.

# 附錄六
# APPENDIX 6

## 個案三

### 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**

一間社區中心及一個政府部門分別向私隱專員公署通報，該政府部門委託該社區中心舉辦一個義工計劃，而該社區中心的一名員工在未獲授權的情況下，將計劃參加者的個人資料儲存至一枚可攜式儲存裝置，而該員工在與公事無關的情況下攜帶該裝置到一公共場所並於該處遺失了該裝置。該裝置載有225名人士的個人資料，包括50名計劃參加者的個人資料，以及該中心的服務使用者及自僱人士的紀錄。

**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。該社區中心採取了各項措施防止類似事件再次發生，包括提醒員工將載有個人資料的文件攜離中心的審批機制以及有關保障資料的守則及工作指引；要求員工如須使用可攜式儲存裝置儲存個人資料或機密文件，必須使用該社區中心提供及已進行加密處理的可攜式儲存裝置；以及委託第三方專業顧問對其資訊系統及運作程序進行私隱影響評估及審計。

## Case 3

### Loss of a portable storage device containing personal data – DPP 4 – security of personal data

**Background**

A community centre and a government department respectively reported to the PCPD that the government department had entrusted the community centre to organise a volunteer programme, and that a staff member of the community centre stored the personal data of the programme participants on a portable storage device without authorisation and carried it to a public place in non-official circumstances. The device was lost while being carried and it contained the personal data of 225 individuals, including 50 programme participants, as well as records of the service users and self-employed persons of the community centre.

**Remedial Measures**

Upon receiving the notification, the PCPD initiated a compliance check. The community centre implemented various measures to prevent recurrence of similar incidents. The measures included reminding all staff members about the approval mechanism for taking documents containing personal data outside the centre, as well as the data protection codes and guidelines; requiring staff members to use encrypted portable storage devices, provided by the community centre, for storing personal data and confidential documents; and engaging third-party professional consultants to conduct privacy impact assessments and audits for its information system and operating procedures.

而該政府部門亦提醒其委託的其他承辦商有關保障個人資料的要求及其重要性，為承辦商或機構制定處理個人資料的指引，並於與承辦商或合作機構簽訂的服務合約中加入與《私隱條例》相關的條款，以確保承辦商或合作機構符合有關規定。

The government department reminded other engaged contractors about the requirements and significance of personal data protection, formulated guidelines for contractors or organisations regarding the processing of personal data and incorporated provisions of the PDPO into its contracts with contractors or organisations to ensure compliance.

**借鑑**

便攜式儲存裝置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。不過，當機構使用便攜式儲存裝置時，由於可以簡單且快速地複製和轉移大量個人資料至機構系統以外的地方（而普遍來說機構系統較為安全），因而增加了資料保安事故的風險。機構應在切實可行範圍內避免使用便攜式儲存裝置來存儲個人資料。如有必要使用便攜式儲存裝置，應制訂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。

**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 because large amounts of personal data can be easily and quickly copied and transferred outside of corporate systems, which are generally better secured. 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 use and whereabouts, as well as erase data in portable storage devices securely after each use.

另一方面，機構委託第三方處理個人資料時，應以合約規範或其他方法，防止轉移予第三方作處理的個人資料在未獲准許的或意外的情況下被查閱、處理、刪除、喪失或使用。

On the other hand, if organisations entrust 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 data transferred to the data processor for processing.

# 附錄六
# APPENDIX 6

## 個案四

### 一個專業團體的電郵系統遭未獲授權查閱 — 保障資料第4原則 — 個人資料的保安

**背景**

一個專業團體向私隱專員公署通報，表示一名員工點擊釣魚電郵內的連結，並在連結中的釣魚登入頁面輸入電郵帳戶的登入憑證，令黑客成功盜用其帳戶，並向大約2,700人發送釣魚電郵，導致再多兩個員工的電郵帳戶被盜用，黑客其後利用盜用的帳戶查閱載有17,517人的電郵地址的文件。

## Case 4

### Unauthorised access to a professional association's email system – DPP 4 – security of personal data

**Background**

A professional association reported to the PCPD that a staff member clicked on an embedded link in a phishing email and entered his login credentials on a phishing login page. As a result, the account was compromised and used to send phishing emails to around 2,700 individuals, which led to two other email accounts of staff members being compromised. The compromised accounts were then used to access documents that contained the email addresses of 17,517 individuals.

### 補救措施

收到該團體的通報後，私隱專員公署展開循規審查。該團體向私隱專員公署表示，已因應事件啟用基於網域的訊息驗證、報告和一致性功能，以阻止任何未經授權的電子郵件進入工作人員的收件匣。此外，該團體已為所有帳戶重設密碼及採用雙重認證，亦採用地理位置檢查以阻止使用來自已知涉及黑客活動國家的IP位址的登入。該團體承諾對所有員工進行加強網絡安全意識的培訓。

### 借鑑

員工成為網絡釣魚攻擊的受害者可能會對機構造成嚴重後果。為了防止此類攻擊，機構應讓員工了解網絡釣魚相關的風險，並提供有關如何識別和避免網絡釣魚的定期培訓。此外，機構應在電郵系統中實施完備的偵測和過濾系統來加強保安措施。同時，機構應實施多重認證功能和定期更改密碼，以降低機構被未經授權存取資料的風險。

### Remedial Measures

Upon receipt of the notification from the association, the PCPD initiated a compliance check. The association informed the PCPD that, in light of the incident, it had enabled the domain-based message authentication, reporting and conformance function, preventing unauthorised emails from reaching staff members' inboxes. Furthermore, the association had reset the passwords of all user accounts and implemented two-factor authentication. Additionally, the association implemented a geo-location check, blocking logins from IP addresses associated with countries that were commonly known for hackers. The association also undertook to conduct security awareness training for all staff members.

### Lessons Learnt

Phishing attacks can have severe consequences for organisations when staff members fall victim to them. To prevent such attacks, it is crucial to educate staff members about the risks associated with phishing emails and provide regular training on how to identify and avoid them. Moreover, organisations should enhance their security measures by implementing robust detection and filtering systems in their email systems. Meanwhile, organisations should implement multi-factor authentication and regular password updates to mitigate the risk of unauthorised access.