附錄
Appendix

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) has to follow the six Data Protection Principles (DPPs). The DPPs represent the normative core of the PDPO and cover the entire life cycle of the handling 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 & 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 & 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，均高於服務承諾目標。在回覆電話查詢及確認收到書面查詢方面，所有個案均在兩個工作日內完成；在詳細回覆書面查詢方面，所有個案均在28個工作日內作出回覆。

在處理公眾投訴方面，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，私隱公署決定結束投訴的個案當中，99%的個案都能夠在180日內結案（服務指標為95%）。

至於處理法律協助計劃申請方面，所有個案均能夠在收到申請後兩個工作日內發出認收通知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 target performance. Replies to telephone enquiries and acknowledgements of written enquiries were all completed within two working days of receipt. All written enquiries that needed substantive replies were also responded to within 28 working days of receipt.

In handling public complaints, acknowledgement receipts were issued within two working days of receipt in 99% of the cases (our performance target is 98%). In situations where the PCPD decided to close a complaint case, 99% of the cases were closed within 180 days of receipt (our performance target is 95%).

As regards 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 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				
			2017	2018	2019	2020	2021
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%	100%	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%	99%	96%	99%	99%	99%
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%	100%	不適用[2] N/A[2]	100%
通知申請人申請結果 Inform the applicant of the outcome	申請人遞交法律協助申請的所有相關資料後三個月內 Within three months after the applicant has submitted all the relevant information for the application for legal assistance	90%	100%	83%	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3/2020號)

查閱資料要求 — 要求文件的目的是用以尋找資料使用者先前作出決定的依據 — 標的事宜與保障個人資料私隱無關 — 正確行使酌情權拒絕對投訴進行調查

Appeal Case Note (1)

(AAB Appeal No. 3 of 2020)

Data access request – requesting a document for the purpose of seeking evidence on the data user's prior decision – the subject matter was not related to the protection of personal data privacy – discretion not to further investigate the complaint duly exercised

聆訊委員會成員： **Coram:**	**彭耀鴻資深大律師(主席) Mr Robert PANG Yiu-hung, SC (Chairperson)** **容慧慈女士(委員) Ms Christine YUNG Wai-chi (Member)** **唐以恒先生(委員) Mr TONG Yee-hang (Member)**
裁決理由書日期： **Date of Decision:**	**2021年11月24日** **24 November 2021**

投訴內容

上訴人向某執法機構就一份調查報告提交兩次查閱資料要求，而有關報告的內容後來被發現為導致該執法機構決定檢控上訴人某些所干犯的罪行。上訴人指稱該執法機構未有於法定期限的40天內依從查閱資料要求，故向私隱專員作出投訴。

The Complaint

The Appellant lodged two data access requests (DARs) to a law enforcement agency (the Law Enforcement Agency) for access to an investigation report, which later transpired to have resulted in the Appellant's prosecution of certain offence(s). The Appellant alleged that the Law Enforcement Agency failed to comply with the DARs within the statutory timeframe of 40 days and hence made a complaint to the Privacy Commissioner.

私隱專員的決定

經審視相關的證據後，私隱專員認為在該執法機構逾時回覆查閱資料要求的事實上並沒有任何爭議。私隱專員拒絕繼續調查上訴人的投訴，其中一個依據是披露有關調查報告會透露該執法機構的行動，包括調查細節，同時該披露相當可能會損害調查及檢控罪行的工作，所以該執法機構可援引《私隱條例》第58(1)(a)條，拒絕依從有關的查閱資料要求。上訴人不滿私隱專員根據《私隱條例》第39(2)(d)條作出的決定，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) 就有關該執法機構逾時回覆查閱資料要求，委員會認為該執法機構已自願採取補救措施，故認同不必再作進一步調查。

The Privacy Commissioner's Decision

Upon examining the evidence available, it was not disputed that the Law Enforcement Agency delayed in responding to the DARs. One of the reasons why the Privacy Commissioner refused to further investigate into the Appellant's complaint was that the Law Enforcement Agency was entitled to invoke the exemption under section 58(1)(a) of the PDPO in refusing to comply with the DARs. The disclosure of the investigation report would reveal the action(s) taken by the Law Enforcement Agency, including the details of the investigation such that it would likely prejudice the investigation and prosecution of the crime concerned. Dissatisfied with the Privacy Commissioner's decision made pursuant to section 39(2)(d) of the PDPO, the Appellant lodged an appeal to the AAB.

The Appeal

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

(1) Regarding the allegation of a delay on the part of the Law Enforcement Agency, the AAB agreed that any further investigation of this issue was unnecessary as remedial actions had already been taken by the Law Enforcement Agency voluntarily.

(2) 委員會認為有證據顯示上訴人提出查閱資料要求的目的是尋找該執法機構在作出調查及／或檢控決定中的不當地方，而並非為了促進任何保障資料原則所賦予的權利，例如確定該執法機構所持有的個人資料的類別。委員會依仗*胡潔冰訴行政上訴委員會*[2007] 4 HKLRD 849一案的原則（即提出查閱資料要求的目的並非輔佐訴訟文件披露的權利或讓資料當事人以此作為途徑取得資料以作其他用途），認為上訴人藉查閱資料要求以收集該執法機構作出不當決定的證據，並非《私隱條例》下賦予資料當事人有關權利的目的。

委員會亦在判決中提出附帶意見，對《私隱條例》第58(1)(a)條的豁免在本案的適用性有所保留，認為私隱專員應查看有關調查報告，以考慮該執法機構是否有足夠理據援引《私隱條例》下相關的豁免條文。

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
黎國榮助理律師代表私隱專員

該執法機構（受到遭上訴所反對的決定所約束的人）缺席應訊

(2) Regarding the purpose for which the DARs were lodged, the AAB found evidence indicating that the Appellant's purpose for such requests was to fish for any irregularities in the then decision to investigate and / or prosecute, as opposed to furtherance of any of the relevant data protection principles, such as ascertaining the kinds of personal data held by the Law Enforcement Agency. The AAB applied the principle established in *Wu Kit Ping v Administrative Appeals Board* [2007] 4 HKLRD 849 (i.e. the purpose of lodging a DAR was not to supplement rights of discovery in legal proceedings or to enable a data subject to locate information for other purpose(s)) and opined that to look for evidence of perceived wrongdoing on the part of the Law Enforcement Agency was not a purpose for lodging a DAR as enshrined under the PDPO.

As *obiter dicta*, the AAB had reservations as to the applicability of the exemption under section 58(1)(a) of the PDPO and considered that the Privacy Commissioner should have examined the investigation report to consider whether there was sufficient justification for the Law Enforcement Agency to invoke the relevant exemption provision(s) under the PDPO.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Mr Alex LAI, Assistant Legal Counsel representing the Privacy Commissioner
The Law Enforcement Agency (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5/2020號)

查閱資料要求 — 要求查閱的資料受法律專業保密權的保障 — 要求的資料有可能披露投訴人士之身份 — 正確行使酌情權拒絕對投訴進行調查

Appeal Case Note (2)

(AAB Appeal No. 5 of 2020)

Data access request – the requested data was protected by legal professional privilege – the requested data might reveal the identity of the complainant – discretion not to further investigate the complaint duly exercised

聆訊委員會成員： **Coram:**	**廖玉玲女士，太平紳士(主席) Ms Elaine LIU Yuk-ling, JP (Chairperson)** **陳浩升先生(委員) Mr Ernest CHAN Ho-sing (Member)** **唐彩珍女士(委員) Ms TONG Choi-cheng (Member)**
裁決理由書日期： **Date of Decision:**	**2021年5月13日** **13 May 2021**

投訴內容

上訴人收到牙醫管理委員會(牙醫委員會)的信函通知，決定根據《牙醫註冊條例》取消上訴人的牙醫註冊。有關信函中亦提及牙醫委員會早前曾接獲有關向上訴人所作出的投訴(該投訴)，如上訴人其後申請復牌，牙醫委員會將跟進該投訴。

The Complaint

The Appellant was notified by the Dental Council of Hong Kong (Dental Council) of their decision to deregister the Appellant pursuant to the Dentists Registration Ordinance by a letter. It was also mentioned that the Dental Council had received a complaint against the Appellant (the Complaint), and if the Appellant intended to re-apply for a practising certificate, the Dental Council would follow up with the Complaint.

上訴人曾先後三次向牙醫委員會作出查閱資料要求，包括：(1)牙醫委員會就取消上訴人的牙醫註冊一事向法律顧問徵求的法律意見之複本；及(2)該投訴的詳情。由於牙醫委員會拒絕遵從上述查閱資料要求，故上訴人向私隱專員作出投訴。

The Appellant made a total of three DARs to the Dental Council, requesting, amongst other things, (1) a copy of the legal opinion rendered by its legal advisor regarding the decision to deregister the Appellant; and (2) the details of the Complaint. As the Dental Council refused to comply with the aforesaid DARs, the Appellant lodged a complaint to the Privacy Commissioner.

私隱專員的決定

The Privacy Commissioner's Decision

首先，私隱專員認為法律顧問向牙醫委員會提供的法律意見受到「法律專業保密權」的保障，故牙醫委員會可引用《私隱條例》第60條的豁免條文拒絕遵從有關查閱資料要求。

First, the Privacy Commissioner considered that the legal opinion rendered by the legal advisor of the Dental Council was subject to legal professional privilege. Hence, the Dental Council could have relied on the exemption under section 60 of the PDPO and refused to comply with the relevant DARs.

此外，私隱專員認同向上訴人提供該投訴的詳情，相當可能會直接或間接披露作出該投訴的人士之身份，有可能對調查該投訴構成損害，故牙醫委員會可引用《私隱條例》第58(1)(d)條的豁免，毋須向上訴人提供該投訴的詳情。

Further, the Privacy Commissioner agreed with the Dental Council that disclosing the details of the Complaint might have directly or indirectly revealed the identity of the Complainant, and may well have prejudiced the investigation against the Complaint. Therefore, the Dental Council was entitled to refuse to provide the Appellant with the details of the Complaint by relying on the exemption under section 58(1)(d) of the PDPO.

私隱專員認為個案沒有違反《私隱條例》的任何規定，故行使《私隱條例》第39(2)(d)條賦予的酌情權以拒絕對投訴進行調查。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

The Privacy Commissioner considered that there was no contravention of the requirements of the PDPO; and exercised the discretion under section 39(2)(d) of the PDPO not to carry out an investigation into the Appellant's complaint. Dissatisfied with the Privacy Commissioner's decision, the Appellant lodged an appeal to the AAB.

上訴

委員會確認私隱專員的決定，並基於下述理由駁回該上訴：

(1) 儘管委員會認同牙醫委員會所享有的法律專業保密權並不是絕對，但在考慮到法律顧問的角色及提供法律意見的相關情況，委員會認為有證據顯示所涉的法律意見應受法律專業保密權的保障。由於上訴人未能提出合理的相反證據，故所涉的法律意見可獲《私隱條例》第60條所豁免而毋須提供。

(2) 牙醫委員會進行紀律研訊的目的主要是針對牙醫的操守行為，而披露該投訴的詳情可能會直接或間接識辨作出該投訴的人士之身份，也可能會損害防止、排除或糾正（包括懲處）任何人所作的不合法或嚴重不當的行為、或不誠實的行為或舞弊行為，所以委員會認同該投訴的詳情屬於《私隱條例》第58(1)(d)條所涵蓋的豁免情況。

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
劉嘉儀律師代表私隱專員

牙醫委員會（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 AAB agreed that the legal professional privilege enjoyed by the Dental Council was not absolute. In considering the role of the legal advisor and the circumstances under which the legal opinion was provided, the AAB opined that the legal opinion obtained by the Dental Council was subject to legal professional privilege. In the absence of reasonable evidence to the contrary, the legal opinion concerned could be exempted from providing to the Appellant under section 60 of the PDPO.

(2) The aim of the disciplinary proceedings instituted by the Dental Council was targeted on misconduct of dentists. Disclosing the details of the Complaint might have not only directly or indirectly revealed the identity of the complainant, but also prejudiced the prevention, preclusion or remedying (including punitive action) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons. Hence, the AAB agreed that the details of the Complaint could be exempted under section 58(1)(d) of the PDPO.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Ms Lucia LAU, Legal Counsel representing the Privacy Commissioner
The Dental Council (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19/2020號)

查閱資料要求 — 提供的資料不完整 — 已在能力範圍內提供 — 沒有證據顯示資料使用者拖延提供資料 — 改正資料要求 — 把資料當事人的意見作附註 — 正確行使酌情權拒絕繼續調查投訴

Appeal Case Note (3)

(AAB Appeal No. 19 of 2020)

Data access request – data supplied not complete – data provided by data user in its best efforts – no evidence suggesting delay on the part of the data user in providing data – data correction request – discretion not to investigate the complaint duly exercised

聆訊委員會成員： **Coram:**	**廖玉玲女士，太平紳士(主席) Ms Elaine LIU Yuk-ling, JP (Chairperson)** **陳浩升先生(委員) Mr Ernest CHAN Ho-sing (Member)** **任文慧女士(委員) Ms Julienne JEN (Member)**
裁決理由書日期： **Date of Decision:**	**2021年11月9日** **9 November 2021**

投訴內容

上訴人分別向某執法機構提出查閱資料要求以查閱他早前報案的相關文件及紀錄；及提出改正資料要求以求刪除上述案件中該執法機構人員紀錄內的某些內容。該執法機構在收到該查閱要求的40日內向上訴人提供相關文件。由於上訴人認為該執法機構提供的資料不完整及未能閱覽獲提供的光碟，同時未有依從其改正資料要求，故向私隱專員作出投訴。

The Complaint

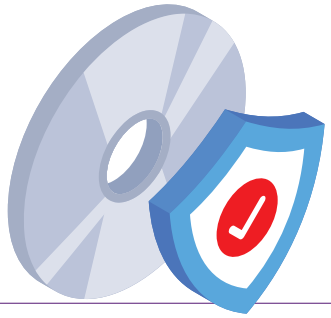
The Appellant submitted a DAR to a law enforcement agency (the Law Enforcement Agency) for obtaining documents and records relevant to a case which was reported by the Appellant earlier; and submitted a data correction request (DCR) requesting erasure of certain contents from the record of the officer of the Law Enforcement Agency respectively. Notwithstanding that the Law Enforcement Agency provided the requested documents within 40 days after receiving the DAR, the Appellant considered that the data supplied was not complete; the CD-Rom provided could not be read; and the DCR was not complied with. Hence, the Appellant complained to the Privacy Commissioner.

私隱專員的決定

就未有依從查閱資料要求的投訴，私隱專員認為，該執法機構已在其

The Privacy Commissioner's Decision

As regards the complaint against the failure of the Law Enforcement Agency in complying with the DAR,



能力範圍內向上訴人提供所要求的資料，並在得悉光碟未能閱覽後採取補救措施，包括提供第二隻光碟及應上訴人要求以紙張提供資料。

the Privacy Commissioner considered that the Law Enforcement Agency had made their best efforts to provide the Appellant with the data so requested. Further, upon being notified that the CD-Rom could not be read, it had already taken remedial measures, which included providing another CD-Rom and the relevant data in paper form in order to comply with the Appellant's request.

就未有依從改正資料要求的投訴，私隱專員認為，由於該要求並非遵照《私隱條例》第22(1)(a)條的規定提出，故同意該執法機構無需理會該要求。再者，由於有關該執法機構人員內的紀錄已被用作一宗相關的索償案之證物，故不適宜就其記錄的內容作出更改。

As regards the complaint against the failure of the Law Enforcement Agency in complying with the DCR, the Privacy Commissioner considered that the Law Enforcement Agency was not required to comply with such request as it was not made pursuant to section 22(1)(a) of the PDPO. Besides, the concerned record of the officer had been admitted as evidence in the relevant civil claim for damages, and it was not appropriate to change the contents.

就此，私隱專員引用《私隱條例》第39(2)(d)條賦予的酌情權，決定不繼續對上訴人的投訴進行調查。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

In view of the above, the Privacy Commissioner decided to exercise her discretion not to further investigate into the Appellant's complaint pursuant to section 39(2)(d) of the PDPO. Dissatisfied with the Privacy Commissioner's decision, the Appellant lodged an appeal with the AAB.

上訴

The Appeal

委員會確認私隱專員的決定，並基於下述理由駁回該上訴：

The AAB affirmed the Privacy Commissioner's decision, and dismissed the Appellant's appeal for the following reasons:

(1) 委員會認為該執法機構已在其能力範圍內遵從了上訴人的查閱資料要求，而上訴人未能提出充分證據證明該執法機構故意拖延提供其所要求查閱的資料，又或因延遲取得相關資料

(1) The AAB agreed that the Law Enforcement Agency had made their best efforts to comply with the DAR. The Appellant was unable to raise sufficient evidence to prove that the Law Enforcement Agency deliberately delayed the supply of data as per his request or he suffered from any actual harm

而對其構成任何實際傷害。委員會信納即使私隱專員繼續處理上訴人的投訴，亦不能為上訴人帶來任何實際的成效。

(2) 就改正資料要求的投訴，委員會認同私隱專員的決定指由於有關紀錄涉及該執法機構人員當時記下的內容，也曾作為呈堂證供，不應隨便刪除。同時，證據顯示該執法機構已在其紀錄中附註了上訴人的意見，故已遵從了改正資料要求的相關規定。

委員會亦在裁決理由書中提出附帶意見，認為上訴人要求的資料可能是為了查找上訴人與該執法機構間出現溝通問題之成因，而導致相關調查進展停滯不前。委員會同意查找溝通問題有別於個人資料私隱保障，故私隱專員可根據《私隱條例》第39(2)(ca)條，拒絕進行調查或終止調查。

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
廖雅欣助理律師代表私隱專員

該執法機構（受到遭上訴所反對的決定所約束的人）缺席應訊

due to the delay. The AAB accepted that even if the Privacy Commissioner had continued with her investigation, it would not have brought about any material result.

(2) Regarding the complaint concerning the DCR, the AAB agreed with the Privacy Commissioner's decision that the record constituted part of the contemporaneous record noted down by the officer of the Law Enforcement Agency, and had been admitted to the court as evidence such that its contents should not be revised. Meanwhile, as there was evidence indicating that the Law Enforcement Agency had made a note of the Appellant's opinion in its record, the relevant requirements of the DCR had been duly complied with.

As *obiter dicta* stated in the decision, the AAB opined that the Appellant's purpose of requesting the data was to look into the cause of the miscommunication between the Appellant and the Law Enforcement Agency, which subsequently led to the delay in investigation. The AAB agreed with the Privacy Commissioner's findings that to look into the miscommunication issues was different from that of protection of personal data privacy such that the Privacy Commissioner would be entitled to refuse to carry out or decide to terminate an investigation pursuant to section 39(2) (ca) of the PDPO.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Ms Joyce LIU, Assistant Legal Counsel representing the Privacy Commissioner
The Law Enforcement Agency (the Person bound by the decision appealed against) was absent

附錄三 Appendix 3

上訴個案簡述(四)

(行政上訴案件第21/2020號)

理賠師獲資料使用者委託作其代理人 — 在處理相關個人資料時不屬於第三者 — 資料使用者及理賠師使用相關個人資料作處理索償事宜之用屬合理 — 沒有證據顯示個人資料被使用或處理作其他不合法或不相關的目的 — 正確行使酌情權拒絕對投訴作進一步調查

Appeal Case Note (4)

(AAB Appeal No. 21 of 2020)

A loss adjuster was engaged by the data user as its agent – not a third party in processing relevant personal data – reasonable for the data user and loss adjuster to use personal data concerned for claims handling – no evidence that the personal data has been used or processed for other unlawful or unrelated purposes – discretion not to further investigate the complaint duly exercised

聆訊委員會成員： **Coram:**	**蔡源福資深大律師(主席) Mr CHUA Guan-hock, SC (Chairperson)** **錢丞海先生(委員) Mr CHIN Shing-hoi (Member)** **關蕙女士(委員) Miss Angelina Agnes KWAN (Member)**
裁決理由書日期： **Date of Decision:**	**2021年4月13日** **13 April 2021**

投訴內容

上訴人於一所超級市場內受傷。該超級市場的一名職員於一份顧客意外報告中記錄上訴人的個人資料，包括其姓名、電話號碼及年齡。該超級市場其後向代表它處理所有涉及人身傷害事件的理賠師提供該報告。上訴人向私隱專員投訴該超級市場：(1)沒有告知他有關收集其個人資料的目的；及(2)在未經其同意的情況下把載有其個人資料的該報告披露予該理賠師作和解談判之用。

The Complaint

The Appellant was injured in a supermarket (the Supermarket). A staff of the Supermarket recorded the Appellant's personal data, including his full name, telephone number and age, in a Customer Accident Report (the Report). The Report was subsequently provided to a loss adjuster, who acted on behalf of the Supermarket in handling all personal injuries incidents (the Loss Adjuster). The Appellant lodged a complaint to the Privacy Commissioner against the Supermarket for: (1) failing to inform him the purpose of collection of his personal data; and (2) disclosing the Report containing his personal particulars to the Loss Adjuster for settlement negotiations without his consent.

私隱專員的決定

經調查投訴後，私隱專員留意到該超級市場已經採取糾正措施及為受傷顧客制訂一份顧客資料表，當中列明：(1)個人資料應由個別人士自願提供；及(2)個人資料會被使用或轉移至其理賠師或保險公司作處理受傷事件之用。私隱專員亦認為該理賠師是該超級市場的代理人，代表它跟上訴人談判。

綜觀事件的所有情況，私隱專員引用《私隱條例》第39(2)(d)條賦予的酌情權終止調查。上訴人不滿私隱專員的決定，遂向委員會提出上訴。

上訴

委員會確認私隱專員的決定，並基於下述理由駁回上訴：

(1) 有關該超級市場是否有權在未有具體地告知上訴人的情況下委託該理賠師作為其代理人，委員會信納該超級市場為了處理有關個人或財產的實際或潛在損失，讓其理賠師或保險公司閱覽或處理上訴人的個人資料，以向該超級市場提供專業意見及協助，做法並不罕見。該理賠師在所有關鍵時刻均為該超級市場的代理人，並不屬於第三者。

The Privacy Commissioner's Decision

Upon investigation, the Privacy Commissioner noted that the Supermarket had taken remedial measures and devised a Customer Information Sheet for injured customers, which set out: (1) personal data should be provided on a voluntary basis; and (2) the personal data would be used or transferred to its loss adjusters and insurers for handling of the injury cases. The Privacy Commissioner also considered that the Loss Adjuster was acting as the agent on the Supermarket's behalf in negotiating with the Appellant.

Taking into account all circumstances of the case, the Privacy Commissioner exercised the discretion to terminate the investigation under section 39(2)(d) of the PDPO. Dissatisfied with the Privacy Commissioner's decision, the Appellant lodged an appeal to the AAB.

The Appeal

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

(1) Regarding whether the Supermarket was entitled to engage the services of the Loss Adjuster as its agent without specifically informing the Appellant, the AAB was satisfied that it was not uncommon for the Supermarket to allow its loss adjusters or insurers to have access to or process the Appellant's personal data in relation to actual or potential damages to persons or properties, with the aim of providing the Supermarket with professional advice and assistance. The Loss Adjuster was acting at all material times as the agent of the Supermarket and was not a third party.

(2) 就上訴人的個人資料被提供予該超級市場及／或該理賠師的目的而言，委員會採納一個常理性的方式作出考慮，並認為上訴人的個人資料被用作核對身份的目的，以確保任何補償金額會正確支付予相關人士。此外，本案亦無證據顯示上訴人在非自願的情況下提供其個人資料予該超級市場；或該超級市場及／或該理賠師使用該等個人資料作任何不合法或不相關的目的，而構成違反保障資料第1(1)原則的規定。

(3) 鑑於上述考慮及該超級市場已採取的糾正措施，委員會認同任何進一步的調查是不必要。委員會強調私隱專員有廣泛的酌情權可根據《私隱條例》第39(2)(d)條終止調查，而在本案中已合理地及公平地行使有關酌情權。

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

該超級市場（受到遭上訴所反對的決定所約束的人）缺席應訊

(2) Regarding the purposes for which the Appellant's personal data was provided to the Supermarket and / or the Loss Adjuster, the AAB adopted a common-sense approach and considered that the Appellant's personal data was used for the purposes of identity verification such that the compensation, if any, would be made to the correct person. There was also no evidence suggesting that the Appellant provided his personal data to the Supermarket on an involuntary basis; or that the Supermarket and / or the Loss Adjuster had used such personal data for any unlawful or unrelated purposes, which would otherwise constitute a contravention of the requirements of DPP 1(1).

(3) Given the aforesaid and the remedial measures taken by the Supermarket, the AAB accepted that any further investigation was unnecessary. The AAB emphasised that the Privacy Commissioner had a wide discretion to terminate an investigation under section 39(2)(d) of the PDPO, and such discretion had been exercised reasonably and fairly in this matter.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Ms Clemence WONG, Assistant Legal Counsel representing the Privacy Commissioner
The Supermarket (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

公共交通運輸公司職員被「起底」—《私隱條例》第64條—個人資料的披露

投訴內容

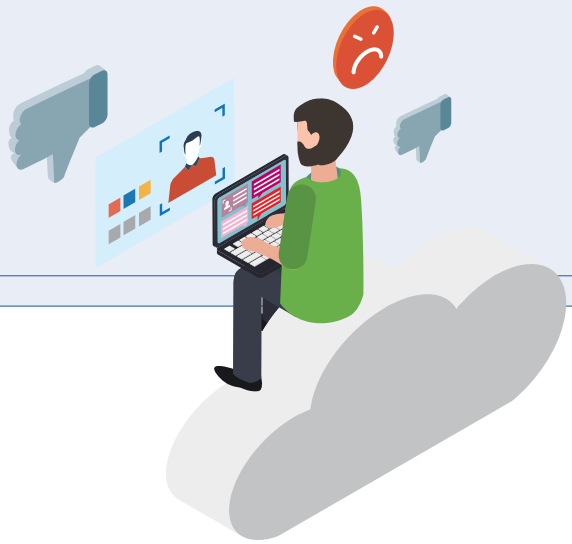
投訴人是某公共交通運輸公司的職員。2021年年初，投訴人發現有人在未得他的同意下，把他的姓名、相片，以及其他個人資料（包括他的職業、公司名稱及工作的車站）發放到社交媒體平台。發文者在帖文內以粗言穢語稱呼投訴人，指責他檢查車票，又呼籲網民去識別他。投訴人對他的個人資料在社交媒體平台被發布感到極度憂慮，遂向私隱公署求助。

Case 1

Staff of a public transport company was doxxed – section 64 of the PDPO – disclosure of personal data

The Complaint

The Complainant was a staff member of a public transport company. In early 2021, the Complainant found that his name, photo and other personal data (including his occupation, company name and the station where he worked) had been posted on a social media platform without his consent. The doxxer addressed the Complainant in foul language, blaming him for checking tickets, and incited other netizens to identify him. The Complainant was extremely distressed due to the disclosure of his personal data on the social media platform. He therefore sought assistance from the PCPD.



結果

在這個案中，不但投訴人的個人資料被披露，發文者更在網上呼籲網民識別投訴人。這無疑對投訴人的日常生活帶來不必要的威脅和滋擾。私隱公署要求有關社交媒體平台移除有關的「起底」帖文，並得到積極的回應。最終，相關涉事的帖文被移除，以減低對投訴人的傷害。

借鑑

近年個人資料被「武器化」，「起底」情況猖獗。雖然在接獲投訴時，「起底」並非刑事罪行，但是《私隱條例》於2021年10月經修訂後更能有效打擊「起底」行為。修例旨在將「起底」行為訂為刑事罪行、賦權私隱專員就「起底」及相關罪行進行刑事調查及檢控，以及賦予私隱專員法定權力要求停止披露「起底」訊息。市民在網上或社交媒體平台發布或轉載任何看來是「起底」的訊息前，都要三思。

Outcome

In this case, not only was the Complainant's personal data disclosed, the doxxer also incited netizens to identify the Complainant. This undoubtedly posed threats and harassment to the Complainant in his daily life. The PCPD requested the social media platform to remove the doxxing post concerned and received a positive response from the social media platform. The doxxing post was eventually removed to minimise damages to the Complainant.

Lessons Learnt

Doxxing activities have become rampant and personal data has been "weaponised" in recent years. Although at the time of the complaint, doxxing was not a criminal offence, the PDPO was amended in October 2021 to more effectively combat doxxing behaviour. The objectives of the amendments were to criminalise doxxing acts, empower the Privacy Commissioner to carry out criminal investigations and institute prosecutions in respect of doxxing and related offences, and confer on the Privacy Commissioner statutory powers to demand the cessation of disclosure of doxxing messages. Everyone should think twice before publishing or re-posting any message that appears to be related to a doxxing message on the Internet or social media platforms.

附錄四 Appendix 4

個案二

僱主張貼有職員個人資料的病毒檢測名單 — 保障資料第4原則 — 個人資料的保安

投訴內容

某機構為其員工(包括投訴人)安排了一連三天的2019冠狀病毒病的病毒檢測。在進行檢測首天，投訴人發現需要進行檢測的員工名單被張貼在員工診所門外，在場人士均可閱覽載於該名單上員工的姓名、完整身份證號碼、出生日期、電話號碼、職員編號等個人資料。現場有人對該名單作出拍攝。投訴人不滿其僱主沒有妥善保障員工的個人資料，遂向私隱公署作出投訴。

結果

該機構解釋，他們向其員工診所提供該名單，是讓該診所的護士為需要檢測的員工預先登記及預備所需物資，並作核對員工身份之用。為了協助員工識別其檢測的次序，護士在檢測當天將該名單張貼在該診所門外。該機構於事發翌日已即時要求診所的護士移除該名單，並提醒他們必須將該名單穩妥地保管。

經私隱公署介入後，該機構進一步向員工發出通告，要求員工刪除曾拍攝得有關該名單的照片，並提醒他們須遵從機構內部有關個人資料私隱的規定。此外，該機構亦承諾日後會要求各部門(包括其員工診

Case 2

An employer posted a list containing the personal data of staff who were to undergo virus testing – DPP 4 – security of personal data

The Complaint

An organisation arranged COVID-19 tests for its staff, including the Complainant, for three consecutive days. On the first day of testing, a list of the staff to be tested was posted outside the staff clinic, and the personal data of the staff on the list, including their names, full HKID Card numbers, dates of birth, phone numbers and staff numbers, were available for viewing by all the people present. The list was photographed by others at the scene. The Complainant was dissatisfied that his employer failed to properly protect the personal data of his staff and lodged a complaint with the PCPD.

Outcome

The organisation explained that the list was provided to the staff clinic so that the nurses of the clinic could pre-register the staff to be tested, prepare the necessary materials and verify the staff's identity. Aiming to assist the staff to ascertain the testing sequence, the nurses posted the list outside the clinic on the day of the test. On the day following the incident, the organisation immediately requested the nurses to remove and safeguard the list.

Upon PCPD's intervention, the organisation further issued a circular to its staff, requesting them to delete any photos of the list and reminding them to comply with the organisation's internal rules on personal data privacy. The organisation also undertook to require all departments (including its staff clinic) to exercise care when handling

所）必須將個人資料小心保管，並採取所有切實可行的步驟，確保個人資料受保障而不受未獲准許或意外的查閱、處理、刪除、喪失或使用所影響。另一方面，該機構表示日後在透過電郵發送含個人資料的檔案予其員工診所時，會將有關檔案加密，並會適當地將訊息標示為「機密」或「限閱文件」。

personal data and take all practicable steps to ensure the protection of personal data against unauthorised or accidental access, processing, erasure, loss or use. The organisation further indicated that the documents containing personal data would be encrypted and suitably marked as "Confidential" or "Restricted" when sending them to its staff clinic by email in future.

私隱公署亦就事件向該機構發出警告，要求他們日後務必敦促員工謹慎處理個人資料，定時提醒各部門在公開張貼任何文件前，須先小心審視當中是否載有個人資料，並仔細考慮及衡量展示有關資料的必要性及程度，以避免重蹈覆轍。

The PCPD also issued a warning to the organisation, requesting it to urge its staff to handle personal data with prudence and regularly remind its departments to carefully check, whether any documents contain personal data or not before posting them in public. The organisation was also requested to carefully consider and weigh the necessity and extent of displaying such data to avoid committing the same mistake.

借鑑

2019冠狀病毒病自爆發以來，已迅速升級為全球健康危機。在確保社區健康和安全的大前提下，僱主或會為員工安排定時作病毒檢測。迅速的防疫行動固然重要，但僱主亦不可忽視保障職員個人資料的重要性。在本案中，該護士的本意或是希望讓員工及早知悉檢測的先後次序而張貼該名單，卻未有審慎考慮該名單上載有敏感且不必要披露的個人資料。僱主應考慮採取披露最少個人資料而又達到同一目的的方法，以期在防疫和保障私隱方面取得適當的平衡。僱主應時刻小心謹慎妥善保障員工的個人資料，制定指引或措施、提供培訓或教育，提高職員對保障個人資料私隱的意識。

Lessons Learnt

COVID-19 has quickly escalated into a global health crisis following its outbreak. Employers may arrange regular virus testing for their staff to ensure the health and safety of the community. While prompt anti-epidemic measures are important, employers must not lose sight of the importance of protecting the personal data of their staff. In this case, the nurses' intention of posting the list might have been to keep the staff informed of the sequence of their respective tests in advance; nonetheless, they failed to consider that the list contained sensitive and excessive personal data. Employers should consider adopting an approach that minimises the disclosure of personal data while seeking to achieve their objective, so as to strike a proper balance between epidemic prevention and privacy protection. Employers should at all times exercise due care in safeguarding the personal data of their staff by formulating guidelines or measures, providing training or education, and raising staff awareness of personal data privacy protection.

附錄四 Appendix 4

個案三

電訊公司在客戶已報失身份證的情況下仍接納有人以該身份證申請服務 — 保障資料第4原則 — 個人資料的保安

投訴內容

投訴人曾被賊人盜取財物及身份證。他就此分別致電及到訪其電話服務供應商匯報有關事件，並着職員於電腦系統內記錄有關事宜，以免賊人假冒其身份。及後，一名人士（該名人士）到訪該電訊公司的分行，以投訴人被盜的身份證作身份證明，成功停用了投訴人的電話號碼並簽署了兩份新合約。同時，該名人士亦更改了投訴人收取該電訊公司帳單的電郵地址。

投訴人不滿該電訊公司就事件的處理，遂就此向警方報案及向私隱公署提出投訴。

結果

該電訊公司確認投訴人曾就被盜取身份證一事向他們作出通知。然而，事發時該電訊公司並無就客戶報失身份證方面訂立妥善的行事方式以作出記錄，故其分行職員在處理該名人士的服務申請時，並不知道投訴人身份證被盜的情況，僅按一般核對客人身份證明文件的程序（即要求客人出示身份證明文件正本及核對文件上的資料）處理該名人士提出的要求。

Case 3

A telecommunications company accepted a HKID Card that had been declared lost by a customer – DPP 4 – security of personal data

The Complaint

The Complainant had his belongings and HKID Card stolen. He then called and visited his telephone service provider to report the theft and asked its staff to record the theft in its computer system so that the thief could not assume his identity. Subsequently, a person (the Person) visited a branch of the telecommunications company and, using the HKID Card stolen from the Complainant as proof of identity, successfully deactivated the Complainant's telephone number and signed two new contracts. Meanwhile, the Person also changed the Complainant's email address from which the latter received his bills from the telecommunications company.

Dissatisfied with the handling of the case by the telecommunications company, the Complainant reported the incident to the Police and lodged a complaint with the PCPD.

Outcome

The telecommunications company confirmed that the Complainant had notified them of the theft of his HKID Card. However, at the time of the incident, the telecommunications company had not established proper practices to record the loss of a customer's HKID Card. As a result, its branch staff was not aware of the theft of the Complainant's HKID Card when processing the Person's application. The staff conducted the normal procedure of checking the customer's proof of identity (i.e. asking the customer to produce the original identity document and checking the information on the document) to process the Person's request.

因應本個案，該電訊公司就客戶報失身份證方面實施一系列的措施，包括要求報失身份證的客戶出示臨時身份證或其他身份證明文件予職員核對身份，並填妥一份「遺失身份證文件聲明書」。職員便會於電腦系統中標明不可再接納該報失的身份證作為該客戶的身份證明文件。另一方面，如職員遇上曾經報失身份證的客戶提出申請或更改服務，職員必須核對該客戶提供的身份證的簽發日期，以確保該身份證是在報失日期後發出的；如職員對該客戶的身份有懷疑，則必須要求該客戶出示其他身份證明文件。該電訊公司並規定所有這類個案必須經主管審批才可作進一步處理。

私隱公署就事件向該電訊公司發出警告，要求他們必須敦促職員嚴格遵循有關保障客戶個人資料方面的政策（包括就客戶報失身份證方面所實施的上述措施），加強對職員的培訓，並提醒他們須以謹慎的態度處理客戶的個人資料，以符合《私隱條例》的相關規定。

借鑑

今時今日，身份盜用個案屢見不鮮，資料使用者如何有效地保障客戶個人資料，面臨前所未有的挑戰。面對層出不窮的犯案手法，資料使用者必須訂立妥善的核實身份機制，才可避免不法分子有機可乘。在本個案中，若該電訊公司在案發時已備有妥善機制就客戶報失身份證的情況作出記錄及核證，便能有效識辨懷疑個案，亦可把握機會將賊人繩之於法。

In response to this case, the telecommunications company implemented a series of measures to deal with the loss of a customer's HKID Card. They included requiring the customer who reported the loss of his HKID Card to present his recognisance form or other identity documents to its staff for verification of identity and to complete a "Declaration of Loss of HKID Card". The staff would then suitably make a remark in the computer system, noting that the lost HKID Card could no longer be accepted as the customer's identity proof. On the other hand, when a customer wished to apply for or change a service, and that customer had previously reported a loss of his HKID Card, its staff must check and ensure that the HKID Card presented was issued after the date of the report. When in doubt about the identity of the customer, the staff must request other identity documents from the customer. The telecommunications company also required that all such cases must be approved by a supervisor before it could be proceeded with.

The PCPD issued a warning to the telecommunications company regarding the incident. It was required to urge its staff to strictly follow its policies on the protection of customers' personal data (including the above measures in relation to the reporting of loss of customers' HKID Cards). It was also required to strengthen the training for its staff and remind its staff to handle customers' personal data with prudence in order to comply with the relevant requirements of the PDPO.

Lessons Learnt

With identity theft being a common occurrence nowadays, data users are faced with an unprecedented challenge to effectively protect their customers' personal data. In the face of the multifariousness of crimes, it is important for data users to formulate proper identity verification mechanisms to avoid loopholes which unscrupulous individuals may exploit. In this case, if the telecommunications company had a proper recording and verification mechanism in place, it would have been able to effectively identify the suspected case. The telecommunications company would then have had the opportunity to bring the thief to justice.

附錄四 Appendix 4

個案四

物業管理公司職員使用環保紙張時披露業戶的個人資料 — 保障資料第4原則 — 個人資料的保安

投訴內容

投訴人為某物業管理公司旗下屋苑的住戶。某日，投訴人發現有數十張「油漆未乾」的告示懸掛或張貼於屋苑內行人通道的兩旁。投訴人注意到該些告示背面，載有該公司與業戶之間的通訊電郵。而其中一張告示背後，是投訴人曾向該公司發送的投訴電郵列印本。該列印本清楚顯示了投訴人的英文姓名、電郵地址及投訴內容。投訴人遂向私隱公署投訴該公司。

結果

該公司表示，根據其既定指引，環保紙只供內部使用。是次事件乃基於個別員工的人為疏忽所致，而公司已對有關員工作出口頭訓示及嚴正警告。該公司亦因應事件而修訂使用環保紙的指引，規定職員日後一律不可使用涉及個人資料的書信或文件作環保紙張，否則會受到紀律處分。

Case 4

Staff of a property management company disclosed the personal data of residents when using recycled paper – DPP 4 – security of personal data

The Complaint

The Complainant was a resident of an estate managed by a property management company. One day, the Complainant found dozens of notices displaying the words "Wet Paint" hung or posted on both sides of the pedestrian walkway in the estate. The Complainant noticed that on the back of these notices were email exchanges between residents and the company. In particular, a printout of a complaint email from the Complainant to the company was on the back of one of the notices. It clearly showed her English name, email address and the content of the complaint. The Complainant thus lodged a complaint against the company with the PCPD.

Outcome

The company said that according to its established guidelines, recycled paper was for internal use only. The incident was caused by human negligence on the part of individual staff members, who were given verbal reprimands and warnings. In the light of the incident, the company revised its guidelines on the use of recycled paper, requiring its staff to stop using documents or correspondences involving personal data as recycled paper in future, failing which they would be subject to disciplinary action.

私隱公署認為該公司未有採取所有切實可行的步驟，去確保員工對個人資料的保安風險有一定程度的意識或敏感度，故該公司因未能妥善保障所持有的個人資料而違反了保障資料第4原則的規定。私隱公署警告該公司，必須就銷毀或棄置載有個人資料文件制訂周詳的內部政策及指引，以便員工遵循（例如載有個人資料但不需保留的文件須適時銷毀、要求員工定期檢查回收箱內的紙張是否包括載有個人資料的文件）。同時，該公司亦應派員進行有效的監察及與員工溝通，以確保員工知悉並依從其內部政策及指引行事。

The PCPD considered that the company had failed to take all practicable steps to ensure a degree of awareness of or sensitivity to the security risks associated with personal data among staff. The company therefore failed to properly protect the personal data held by it in contravention of DPP 4. The PCPD warned the company that it needed to formulate a comprehensive internal policy and guidelines on the destruction or disposal of documents containing personal data for its staff to follow (e.g. destroying in a timely manner the documents that contain personal data but need not be retained; and requiring staff to regularly check whether the paper in recycling bins include documents containing personal data). The company should also assign designated staff to effectively monitor and communicate with other staff to ensure that they are aware of and follow its internal policy and guidelines.

借鑑

雖然該公司已有指引訂明環保紙只供內部使用，但是次事件仍然發生。另外，不論是負責列印「油漆未乾」告示，或是負責張貼該些告示的職員，均沒有發現該些告示背後載有個人資料。由此可見，該公司職員對保障個人資料私隱的意識不足。該公司應汲取是次事件的經驗，明白到制訂相關政策固然是當務之急，但採取措施讓員工了解並遵從有關政策亦是刻不容緩。該公司亦應提供全面的培訓予員工，以提高員工對保障個人資料私隱的意識。

Lessons Learnt

The incident occurred despite the company's guidelines stipulating that recycled paper was for internal use only. Moreover, neither the staff responsible for printing the "Wet Paint" notices nor the staff responsible for posting the notices had come to realise that there was personal data printed on the back of the notices, proving a lack of awareness of personal data privacy protection among staff. The company should learn from this experience that it is pivotal not only to formulate the relevant policy, but also to adopt measures to enhance the awareness of such policy and foster a strong sense of compliance among staff. The company should also provide comprehensive training to its staff to strengthen their appreciation for personal data privacy protection.

附錄四 Appendix 4

個案五

食肆對顧客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

為應對2019冠狀病毒病疫情，政府實施進入食肆規定，規定食肆負責人須確保顧客在進入食肆前利用手提電話流動應用程式「安心出行」掃瞄場所二維碼，或登記其姓名、聯絡電話及到訪食肆的日期及時間，並要求餐廳保留書面或電子紀錄31天。該進入食肆規定於2021年2月18日實施後，私隱公署接獲投訴指有食肆沒有妥善處理顧客登記資料，因而就此對14宗投訴展開調查。

結果

私隱公署的調查結果顯示：11間食肆使用共用的登記表格或登記簿、一間食肆沒有設置表格收集箱、一間食肆沒有保持表格收集箱時刻蓋好，以及一間食肆使用尚未剪開的共用表格。以上情況均顯示該些食肆對登記的個人資料所採取的保安措施不足，以致有關資料可被未獲准許或意外的查閱或使用，違反《私隱條例》保障資料第4(1)原則的規定。

Case 5

Restaurants took inadequate security measures to protect customers' information – DPP 4 – security of personal data

The Complaint

In response to the COVID-19 pandemic, the Government imposed the Restaurant Entry Requirement whereby the responsible persons of restaurants had to ensure that customers either scanned the venue's QR code with the "LeaveHomeSafe" mobile app or registered their names, contact numbers, and dates and times of their visits before entering the restaurants, and for restaurants to keep such written or electronic records for 31 days. Since the implementation of the Restaurant Entry Requirement on 18 February 2021, the PCPD had received complaints about the failure of restaurants to properly handle the registered data of customers, and as a result, launched investigations into 14 complaints.

Outcome

The PCPD's findings revealed that: 11 restaurants used common registration forms or books; one restaurant did not set up any collection box for the forms; one restaurant failed to cover the collection box at all times; and one restaurant used uncut sheets of paper as common forms. The above practices exposed the registered personal data to unauthorised or accidental access or use, and contravened DPP 4(1) of the PDPO as regards the security of personal data.

涉事的14間食肆其後已採取相應的補救措施，包括以獨立表格取代共用的登記表格或登記簿、設置以不透明物料造成的表格收集箱供顧客使用、以及要求店員必須確保表格收集箱時刻蓋好。然而，考慮到防範於未然，私隱公署向所有涉事食肆發出執行通知，要求涉事食肆採取適當及切實可行的措施，以保障顧客的登記資料，並指明涉事食肆須採取的步驟防止違反再發生。有關步驟包括制定書面政策及指引予其職員，並透過定期傳閱指引文件及提供培訓，以提升職員對保障個人資料私隱的意識。

The 14 restaurants subsequently took remedial action, including replacing common registration forms or books with individual registration forms, setting up a form-collection box made of opaque materials for customers' use, and requesting its staff to cover the collection box at all times. Nevertheless, in order to prevent recurrence of similar incidents in future, the PCPD issued Enforcement Notices to the restaurants in question to request them to implement appropriate and practicable measures to protect the registration data of customers and specified the steps that ought to be taken by the restaurants for preventing recurrence of the contravention. These measures included providing a written policy and guidance to their staff, as well as circulating the guidance regularly and providing training to staff to raise their awareness of personal data privacy protection.

借鑑

不論食肆的業務規模、營業模式或資源多寡，食肆在收集、持有、處理和使用個人資料方面都有責任遵守《私隱條例》的規定。在實施防疫措施上，食肆須為店員提供適當培訓及指引，提高他們對保障個人資料私隱的意識。有效的保障個人資料私隱的措施亦有助提升食肆的商譽及競爭優勢，帶來更多潛在商機。

另一方面，為保障個人資料，市民應注意向不同食肆提供個人資料所帶來的私隱風險。

Lessons Learnt

Regardless of the scale of business, mode of operation and availability of resources, all restaurants have the responsibility to comply with the requirements of the PDPO in the collection, holding, processing and use of personal data. When it comes to implementing anti-epidemic measures, restaurants should raise their staff's awareness of personal data privacy protection through appropriate training and guidance. With effective measures in place to protect personal data privacy, restaurants are set to enhance their goodwill, competitive edge and potential business opportunities.

On the other hand, to safeguard their personal data, members of the public should be mindful of the privacy risks inherent in providing personal data to restaurants.

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

地產代理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

An estate agent 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：	**九龍城裁判法院**
Court:	**Kowloon City Magistrates' Court**
審理裁判官：	**莊靜慧暫委裁判官**
Coram:	**Ms CHONG Ching-wai, Erica, Deputy Magistrate**
裁決日期：	**2021年9月7日**
Date of Decision:	**7 September 2021**

投訴內容

投訴人透過一間地產代理公司購買物業，並向該公司提供了他的姓名及電話號碼。投訴人其後向該公司提出拒收直銷訊息要求，並獲對方確認已將他的個人資料加入該公司的拒收名單，不會再致電聯絡投訴人作直接促銷。然而，投訴人稍後收到該公司的一名地產代理的來電，查詢投訴人是否有意放售物業。

The Complaint

The Complainant provided his full name and mobile phone number to an estate agency when he purchased a property. He subsequently made an opt-out request to the agency and received a confirmation from the agency that his personal data had already been included in its opt-out list and no further direct marketing calls would be made to him. However, the Complainant later received a direct marketing call from an estate agent of the agency asking him if he wished to sell his property.

結果

該名地產代理被控沒有依從資料當事人的拒收直銷訊息要求，而繼續使用其個人資料作直接促銷（違反《私隱條例》第35G(3)條）。經審訊後該名地產代理被裁定罪名成立，被判罰款港幣15,000元。

借鑑

公司職員在致電客戶進行促銷前，應該先核對公司所備存的「拒收直銷訊息的客人名單」。若個別職員沒有核對拒收名單而以電話聯絡名單中的客戶作出直接促銷，有關職員便可能須負上刑事責任。

根據《私隱條例》第35G(3)條，資料使用者如收到客戶有關停止使用其個人資料作直接促銷的要求，須在不向該客戶收費的情況下，依從其要求。違反有關規定屬刑事罪行，一經定罪，最高刑罰是罰款港幣500,000元及監禁三年。

Outcome

The estate agent was charged with 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 estate agent was convicted after trial and fined HK$15,000.

Lessons Learnt

Before calling a customer for direct marketing purposes, a staff member of a company should check the opt-out list maintained by the company. An individual staff member who has failed to check the opt-out list and called the customers on the list for direct marketing may have committed a criminal offence.

Pursuant to section 35G(3) of the PDPO, a data user who receives a customer's request to cease using his personal data in direct marketing must comply with the request without a charge. Failing to comply with the requirement is a criminal offence, and is punishable by a fine up to HK$500,000 and imprisonment of up to 3 years.

附錄五 Appendix 5

個案二

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

Case 2

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：	**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：	**2021年9月7日**
Date of Decision:	**7 September 2021**

投訴內容

投訴人是一間電訊公司的客戶，並曾向該公司提出拒收直接促銷訊息的要求。不過，該公司在致電通知投訴人合約即將到期的同時，向他推廣新的服務計劃。

The Complaint

The Complainant was a customer of a telecommunications company. He made an opt-out request to the company to not receive its direct marketing messages. However, a representative of the telecommunications company made a phone call to the Complainant, informing him of the expiry of his service contract and at the same time promoting to him a new service plan.

結果

該公司被控沒有依從資料當事人拒收直銷訊息的要求，而繼續使用其個人資料作直接促銷，違反《私隱條例》第35G(3)條。該公司承認上述控罪，被判罰款港幣8,000元。

借鑑

儘管商戶致電提醒客戶合約快將期滿是出於好意，但如果商戶職員打算於電話對話中，進一步向客戶推銷續約服務或新合約服務，職員應先核實有關客戶是否已同意商戶使用其個人資料作直接促銷或曾否提出拒收直銷訊息要求。

Outcome

The telecommunications company was charged with 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 telecommunications company pleaded guilty to the charge and was fined HK$8,000.

Lessons Learnt

A business organisation may out of goodwill make phone calls to customers to remind them of the expiry of their service contracts. However, if the staff member intends to further promote contract renewal services or new contract services to the customers during the phone calls, he should check beforehand whether the customers have already consented to the use of their personal data for direct marketing purposes or whether they have made opt-out requests.

附錄五 Appendix 5

個案三

Case 3

一名人士在使用客戶的個人資料作直接促銷前沒有採取指明的行動通知客戶及取得其同意，以及沒有告知客戶他有拒收直接促銷訊息的權利 —《私隱條例》第35C及35F條

An individual used a customer's personal data in direct marketing without taking specified actions to notify the customer and obtain his consent, and failed to notify the customer of his opt-out right – sections 35C and 35F of the PDPO

法院：	**粉嶺裁判法院**
Court:	**Fanling Magistrates' Court**
審理裁判官：	**吳重儀裁判官**
Coram:	**Ms NG Chung-yee, Debbie, Magistrate**
裁決日期：	**2021年8月26日**
Date of Decision:	**26 August 2021**

投訴內容

投訴人在數年前曾就家居維修事宜與多間公司聯絡，Y女士是其中一間公司的代表。有一天，投訴人收到Y女士一則透過即時通訊軟件發出關乎投資置業的直接促銷訊息，並表示可安排車輛接送參觀物業。

The Complaint

A few years ago, the Complainant made contact with several companies to enquire about home repair services, and Ms Y was a representative of one of the companies. One day, the Complainant received a direct marketing message via an instant massaging app from Ms Y regarding property investment and was informed that she could arrange transportation for viewing the properties.

結果

Y女士承認違反兩項《私隱條例》的罪名，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。

第一項控罪指Y女士在使用投訴人的個人資料作直接促銷前，未有採

Outcome

Ms Y pleaded guilty to two charges under the PDPO and was fined HK$4,000 in total (HK$2,000 in respect of each charge).

The first charge related to the offence of using the personal data of the Complainant in direct marketing

取指明行動通知投訴人及取得其同意，違反了《私隱條例》第35C條。

without taking specified actions to notify the customer and obtain his consent, in contravention of section 35C of the PDPO.

第二項控罪指Y女士在首次使用投訴人的個人資料作直接促銷時，未有告知投訴人有權要求她在不向其收費的情況下，停止使用他的個人資料作直接促銷，違反了《私隱條例》第35F條。

The second charge related to the offence of failing to inform the Complainant, when using his personal data in direct marketing for the first time, of his right to request not to use his personal data in direct marketing without charge, in contravention of section 35F of the PDPO.

借鑑

資料使用者（不論個人或機構代表）在使用個人資料進行直接促銷前，必須採取《私隱條例》第35C條下所述明的指明行動。條文的指明行動包括告知資料當事人：資料使用者不得在取得他的同意前，使用其個人資料作直接促銷；資料使用者擬使用作直接促銷的個人資料的類別；擬就甚麼類別的促銷標的使用其個人資料進行直接促銷；及提供回應是否同意的途徑等資訊。

Lessons Learnt

Before using a data subject's personal data in direct marketing, a data user (whether an individual or a representative of an organisation) must take the specified actions under section 35C of the PDPO. The specified actions include notifying the data subject: that the data user may not use his personal data for direct marketing unless he has received the data subject's consent; of the kinds of personal data that the data user intends to use for direct marketing; of the classes of marketing subjects in relation to which the personal data of the data subject is to be used; and of a response channel through which the data subject can communicate his consent.

此外，《私隱條例》第35F條亦訂明，資料使用者在首次使用資料當事人的個人資料作直銷時，仍須告知該資料當事人他有權要求資料使用者，在不向其收費的情況下，停止在直銷中使用有關資料。

Pursuant to section 35F of the PDPO, the data user must also, when using the data subject's personal data in direct marketing for the first time, notify the data subject of his right to request the data user to cease to so use the data, without charge to the data subject.

違反上述每項規定屬刑事罪行，一經定罪，最高刑罰是罰款港幣500,000元及監禁三年。

Failure to comply with each of the above requirements is a criminal offence, and is punishable by a fine up to HK$500,000 and imprisonment of up to 3 years.

附錄五 Appendix 5

個案四

一名記者在未經資料使用者的同意下刊登屬於一位知名人士兒子的出生登記紀錄內記項的核證副本的詳細資料——《私隱條例》第64(1)條

Case 4

A reporter published the details of a certified copy of an entry in the birth register pertaining to a celebrity's son without the consent from the data user – section 64(1) of the PDPO

法院：	**西九龍裁判法院**
Court:	**West Kowloon Magistrate's Court**
審理裁判官：	**徐綺薇主任裁判官**
Coram:	**Ms Ivy CHUI Yee-mei, Principal Magistrate**
裁決日期：	**2021年6月15日**
Date of Decision:	**15 June 2021**

投訴內容

投訴人是一位香港知名人士。一名雜誌社的記者於入境事務處取得該知名人士兒子根據生死登記條例規定而備存的出生登記紀錄內一項記項(俗稱「出世紙」)的核證副本，並在未經資料使用者(即入境事務處)的同意下，於雜誌上刊登有關該位知名人士兒子出生紀錄的詳細資料。

The Complaint

The Complainant was a celebrity in Hong Kong and a reporter gained access to a certified copy of an entry in the birth register kept under the Births and Deaths Registration Ordinance (commonly known as "birth certificate") pertaining to the Complainant's son from the Immigration Department and published the details of the birth entry concerned in a magazine without the consent from the data user (i.e. the Immigration Department in the present context).

結果

兩間雜誌社及總編輯分別承認披露未經資料使用者同意而取得的個人資料控罪，各被判處罰款港幣40,000元。而該名雜誌記者則獲撤銷控罪，以港幣2,000元簽保守行為12個月。

借鑑

此為首宗以違反《私隱條例》第64(1)條起訴被告人「起底」行為的案件。任何人士干犯《私隱條例》第64(1)條所訂罪行，一經定罪，最高可判罰款港幣1,000,000元及監禁五年。

Outcome

Two magazine companies and the chief editor pleaded guilty to the charge of disclosing personal data of a data subject which was obtained from a data user without the data user's consent, and they were fined HK$40,000 each. The charge against the reporter was dropped and the court imposed a 12-month bind over on him for HK$2,000.

Lessons Learnt

This was the first doxxing case in which the defendants were convicted for contravention of the offence under section 64(1) of the PDPO. A person who commits an offence under section 64(1) is liable on conviction to a maximum fine of HK$1,000,000 and to imprisonment for 5 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

醫療中心的客戶個人資料管理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

一間醫療中心向私隱公署通報，指其載有病人檔案的客戶個人資料系統被勒索軟件攻擊，導致約115,000名病人的個人資料，包括姓名、性別、出生日期、香港身份證號碼、聯絡號碼及地址、電郵地址、職業、家族歷史及病人緊急聯絡人的資料外洩。

是次事故源於該醫療中心使用過時的操作系統及軟件，導致其系統容易遭受攻擊。

Case 1

Unauthorised access to a clinical centre's customer personal data system – DPP 4 – security of personal data

Background

A clinical centre reported to the PCPD that its customer personal data system containing patient files had suffered a ransomware attack. As a result, about 115,000 records of patients' personal data containing names, gender, dates of birth, HKID Card numbers, contact numbers and addresses, email addresses, occupations, family history and emergency contact information were leaked.

The incident was caused by the use of outdated operating systems and software, which had left its system vulnerable to attackers.

補救措施

在收到該醫療中心的通報後，私隱公署展開了循規審查，並向該醫療中心提供以遵從《私隱條例》相關規定的建議。該醫療中心為其系統進行保安漏洞掃瞄、更新相關的軟件及操作系統，以及每週定期為有關系統進行檢查，以確保所有安裝的軟件均是最新版本。與此同時，該醫療中心承諾每年聘請獨立網絡安全公司為其系統進行保安審計。

借鑑

資料使用者使用過時的軟件及操作系統可引致嚴重的安全漏洞。醫療機構持有大量屬敏感性質的病人資料，因此應採取切實可行的措施，確保其系統沒有安裝過時或不受技術支援的軟件，以減低遭受網絡攻擊的風險。醫療機構應定期進行漏洞掃瞄以識辨系統內潛在的保安漏洞，及適時進行修補。

Remedial Measures

Upon receiving the notification from the clinical centre, the PCPD initiated a compliance check and provided recommendations to the clinical centre to ensure compliance with the provisions of the PDPO. The clinical centre conducted a vulnerability scan on its systems, updated the relevant software and operating systems, and scheduled a weekly system update exercise to ensure that all software installed was up to date. It also agreed to engage an external cybersecurity company to conduct a security audit on its systems on an annual basis.

Lessons Learnt

The use of outdated software and operating systems could expose a data user to severe security vulnerabilities. Healthcare organisations possess a huge amount of patients' sensitive data and should therefore take reasonably practicable measures to ensure their systems are free from outdated or unsupported software to minimise the risk of exposure to cyberattacks. Healthcare organisations should perform periodic vulnerability scanning exercises to detect possible security vulnerabilities and take timely action to remediate them.

附錄六 Appendix 6

個案二

在一間醫院內進行未經授權的拍照 — 保障資料第4原則 — 個人資料的保安

背景

一間醫院向私隱公署通報，指一名隸屬一所大學的研究員在該醫院的一間病房巡房及在手術室觀摩手術期間拍照，並透過即時通訊軟件與他人分享照片，儘管病房及手術室的牆上均貼有「不准拍照」的標示。其中一張照片顯示了七名病人的姓名、香港身份證號碼、性別、年齡及手術細節的簡要。

該研究員表示沒有意識到分享照片的行為會無意中洩露病人的個人資料。

補救措施

在收到有關醫院的通報後，私隱公署展開了循規審查，並向該醫院提供以遵從《私隱條例》相關規定的建議。醫院要求校方提醒其員工在進入醫院臨床區域時須遵守醫院的指引。該大學頒布了一套新的指

Case 2

Unauthorised photo-taking in a hospital – DPP 4 – security of personal data

Background

A hospital reported to the PCPD that a research staff from a university had attended a ward and an operating theatre for surgery observations. Even though "No photo taking" signs were posted on the walls of the ward and the operating theatre, the staff took photos and shared them with others via an instant messaging app. One of the photos showed the names, HKID Card numbers, gender, age and brief operation details of seven patients.

The research staff stated that he was not aware that his act of photo sharing had inadvertently disclosed patients' personal data.

Remedial Measures

Upon receiving the notification from the hospital, the PCPD initiated a compliance check and provided recommendations to the hospital to ensure compliance with the provisions of the PDPO. The hospital requested the university to remind its staff members to observe the guidelines of the hospital when they entered the clinical

引，以妥善處理病人的個人資料和敏感信息。這套新指引明確禁止員工在任何病房或手術室拍照，並禁止透過社交媒體平台或即時通訊軟件分享包含病人資料的照片或文字訊息。

areas of the hospital. The university promulgated a new set of guidelines for the proper handling of patients' personal data and sensitive information. It explicitly prohibited photo taking at any wards or operating theatres as well as uploading and sharing of photos or text messages containing patient data through social media platforms or instant messaging app.

借鑑

病人資料屬敏感的個人資料，應受到高度保護。為此，處理病人資料的機構應制定清晰的資料保障指引，並可加入與有關機構營運相關的實際示例，以更清晰地說明可能違反資料保障指引的情況。此外，機構應提供足夠員工培訓，以向他們灌輸資料保障的思維，並提醒他們須適當考慮有關妥善處理病人資料的既定協議。

Lessons Learnt

Patient's data are sensitive personal data which should be afforded a high degree of protection. To this end, organisations handling patients' data should formulate clear data protection guidelines, in which practical examples relevant to their operations could be included to better illustrate what may constitute violations of the guidelines. Adequate staff training should be provided to instil a data protection mindset in staff and remind them to give due consideration to the established protocols on the proper handling of patients' personal data.

附錄六 Appendix 6

個案三

於在家工作安排中遺失手提電腦 — 保障資料第4原則 — 個人資料的保安

背景

一個政府部門向私隱公署通報，表示一名員工在公共交通工具上，遺失了一部由該部門提供予員工用作在家工作的手提電腦。該電腦載有該員工的下屬的工作評核的草擬報告，當中涉及的個人資料包括姓名、職級及委任日期、薪金點、職責及初步工作評語。該員工沒有在工作評核階段完結後適時從該手提電腦中刪除上述工作評核的草擬報告。

Case 3

Loss of notebook computer under work-from-home arrangements – DPP 4 – security of personal data

Background

A government department reported to the PCPD that a staff member had lost an official notebook computer, which was provided to the staff member under work-from-home (WFH) arrangements, on public transport. The computer contained draft staff appraisal reports including their names, ranks and dates of appointment, salary points, duties and preliminary assessments. The staff member had failed to delete the draft appraisal reports upon completion of the appraisal period.

補救措施

在收到有關政府部門的通報後，私隱公署展開了循規審查。私隱公署發現，由於該手提電腦內的資料已被加密保護，當中的個人資料受到未獲准許或意外的查閱的風險較低。雖則如此，該部門已提醒所有員工，需要小心處理公務使用的便攜式儲存裝置。

該部門修訂工作指引，提醒員工不應將機密資料永久儲存於手提電腦內，並應適時刪除不再需要的機密資料。

借鑑

自2019冠狀病毒病大流行肆虐開始，不少機構需要實行在家工作安排，以減少社區的人流及社交接觸。雖然大部分機構已訂立政策，要求員工加密儲存於手提電腦內的電子檔案，但機構難以確保員工適時刪除已不需使用而載有個人資料的文件。為加強保障個人資料，機構應考慮要求員工透過虛擬私人網絡(VPN)處理工作文件，而非直接將有關文件儲存於便攜式儲存裝置內。

Remedial Measures

Upon receiving the notification from the government department, the PCPD initiated a compliance check. The PCPD found that while the personal data contained in the notebook computer had been encrypted to reduce the risk of unauthorised or accidental access to the data, the department reminded staff to take extra care in handling official portable devices.

The department revised its guidelines reminding staff members that notebook computers should not be used as permanent storage of restricted information, and such information should be deleted when it was no longer necessary.

Lessons Learnt

In view of the severity of the COVID-19 pandemic situation, many organisations have adopted WFH arrangements to reduce the flow of people and social contacts in the community. It is noted that most organisations have policies in place to require their staff members to encrypt electronic records in notebook computers. However, it is difficult to ensure staff members deleted obsolete documents containing personal data in notebook computers. To further enhance the protection of personal data, organisations should consider requesting their staff members to access work files through a virtual private network (VPN) connection instead of storing work files locally.


PCPD
H K
PDPO
DOXXING