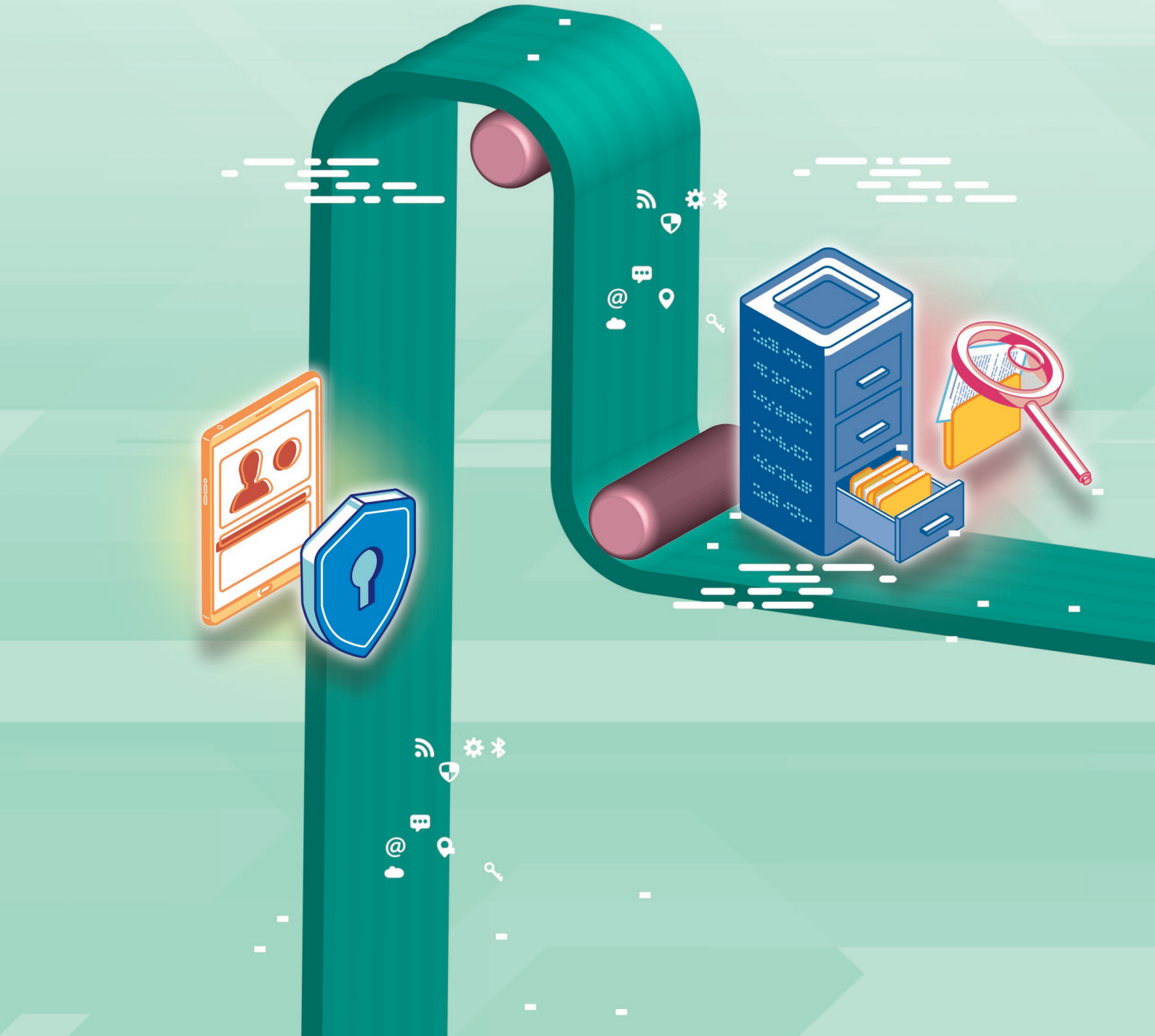
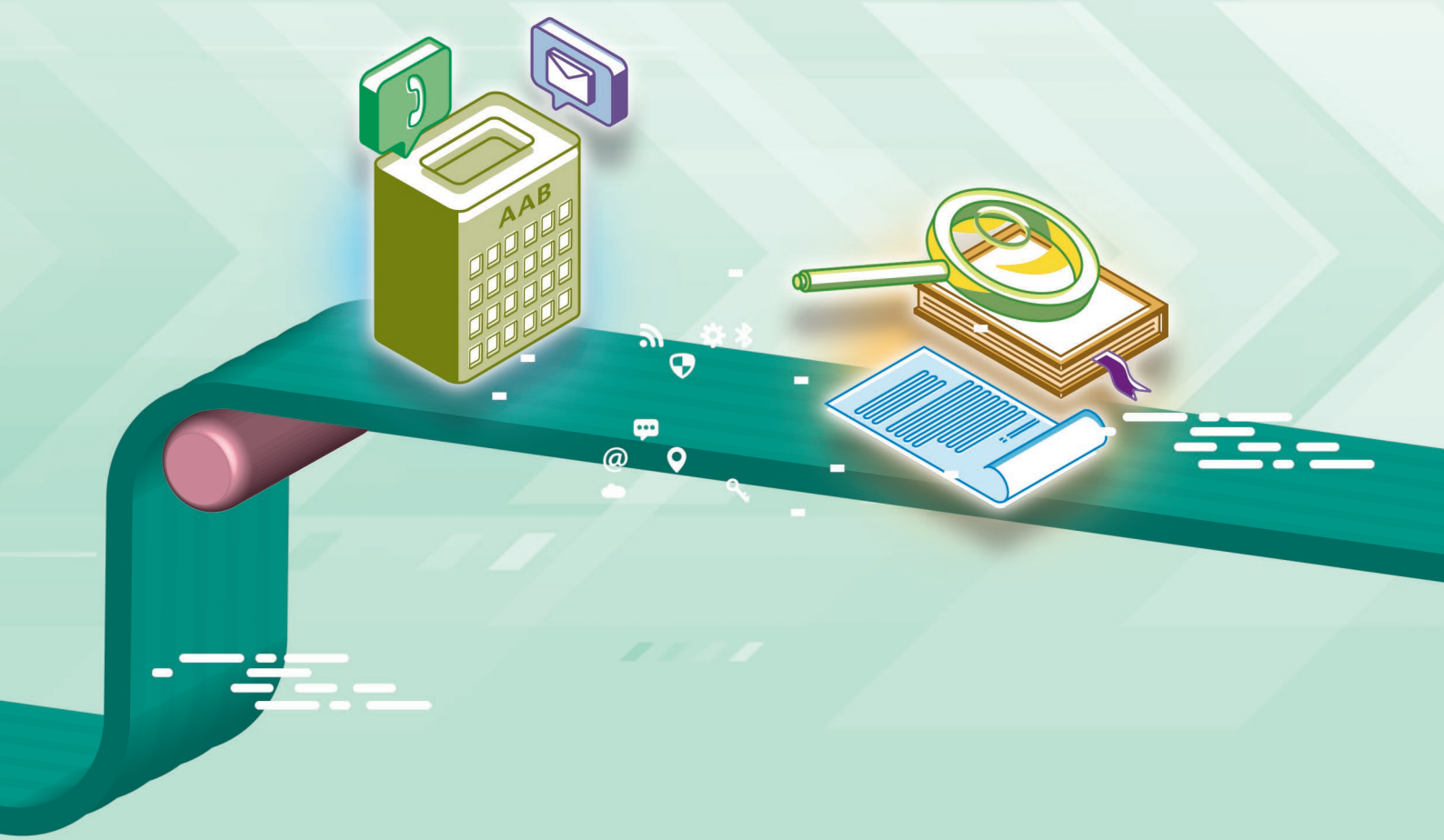
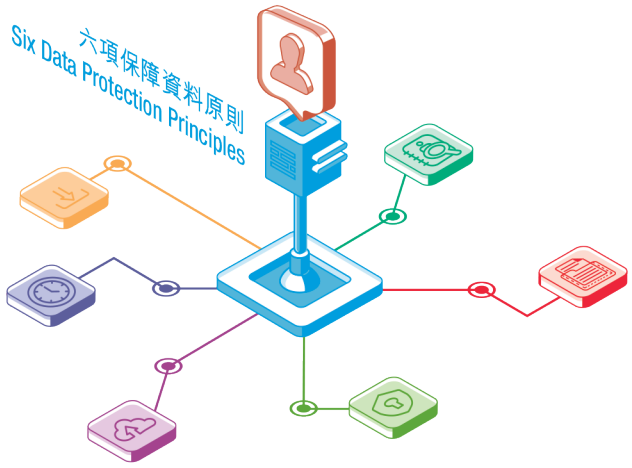
附錄
Appendix





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 is not kept for a period longer than is necessary to fulfill 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，均達致服務承諾的目標。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個工作日內完成。

至於公眾投訴個案，在收到投訴後兩個工作日內發出認收通知的比率為99%，高於服務承諾目標不少於98%。此外，私隱公署決定結束投訴個案當中，99%的個案都能夠在180日內結案，亦高於服務承諾目標不少於95%。

至於法律協助計劃申請，私隱公署於2020年沒有收到任何申請。有關通知申請人申請結果，承接2019年遞交的申請個案均在申請人遞交所有相關資料後三個月內完成通知。

Performance Pledge

In the reporting year, the PCPD met its performance target in the handling of public enquiries, complaints and applications for legal assistance. 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.

On public complaints, acknowledgement receipts were issued within two working days of receipt in 99% of the cases. In situations where the PCPD decided to close a complaint case, 99% were closed within 180 days of receipt. The performance in both categories exceeded the target performance of 98% and 95% respectively.

As regards applications for legal assistance, none was received in 2020. For applications submitted in 2019 and processed in 2020, all applicants were informed of the outcome of applications for legal assistance within three months of submission of all relevant information.

服務標準 Service Standard		服務標準（個案達到服務標準的百分比）Target Performance (% of cases meeting standard)	服務表現 Actual Performance				
			2016-17	2017-18	2018-19	2019-20	2020-21
處理公眾查詢 Handling public enquiries							
回覆電話查詢 Return a telephone enquiry	接獲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	接獲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	接獲查詢後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	接獲投訴後兩個工作日內 Within two working days of receipt	98%	99%	100%	100%	99%	99%
結束投訴個案 Close a complaint	接獲投訴後180日內 Within 180 days of receipt[1]	95%	96%	99%	96%	99%	99%
處理法律協助計劃申請 Handling applications for legal assistance							
確認收到申請 Acknowledge receipt of an application	接獲申請後兩個工作日內 Within two working days of receipt	99%	100%	100%	100%	100%	不適用 N/A[2]
通知申請人申請結果 Inform the applicant of the outcome	接獲所有相關資料後三個月內 Within three months after the applicant has submitted all relevant information for the application	90%	100%	100%	83%	100%	100%

1. 私隱公署按《私隱條例》第 37 條準則接納投訴後開始計算。
2. 於 2020 年沒有收到申請。

1. The counting starts on the date on which a complaint is formally accepted as a complaint under section 37 of the PDPO.
2. No application was received in 2020.

附錄三
Appendix 3

上訴個案簡述一

（行政上訴委員會上訴案件 第2/2017 號）

改正資料要求 — 個人信貸資料 —《私隱條例》第39(2)(d)條 — 採取糾正措施 — 進一步調查不能合理地預計可帶來更滿意的結果 — 並非保存於上訴人檔案內的個人資料並不構成上訴人的個人資料 — 保障資料第2原則：個人資料的準確性及保留期間

聆訊委員會成員：許偉強資深大律師（主席）
劉貴顯先生（委員）
唐彩珍女士（委員）
裁決理由書日期：2020年4月28日

投訴內容

上訴人接連收到由一所銀行（下稱「甲銀行」）及一間追收欠賬公司郵寄至其住址（下稱「該住址」）的信件，內容均是向他追收欠賬。上訴人稱該等信件與另一名人士（下稱「戊女士」）的賬戶有關，跟他本人沒有任何關係。上訴人其後得知該住址是由一信貸資料機構（下稱「該信貸資料機構」）提供予甲銀行。

上訴人首先向甲銀行及追收欠賬公司作出投訴，但被要求直接聯絡該信貸資料機構以更正相關資料。上訴人隨後向該信貸資料機構提出改正資料要求，要求它把該住址從戊女士的紀錄中移除（下稱「相關住址紀錄」）。不過，該信貸資料機構表示，相關資料是由另一銀行（下稱「乙銀行」）提供，並在當時已獲確認相關住址紀錄屬戊女士的「正確地址」，因此拒絕依從上訴人的改正資料要求。

上訴人亦認為該信貸資料機構未有採取所有切實可行的步驟以確保個人資料的準確性，違反保障資料第2原則的規定。

私隱專員的決定

私隱專員調查後決定行使《私隱條例》第39(2)(d)條的酌情權，不對上訴人的投訴作進一步調查，其理由如下：

Appeal Case Note (1)

(AAB Appeal No. 2 of 2017)

Data correction request – consumer credit data – section 39(2)(d) of the PDPO – remedial measures taken – further investigation cannot reasonably be expected to bring about a more satisfactory result – the personal data not maintained in the Appellant's profile did not constitute his personal data – DPP 2: accuracy and duration of retention of personal data

Coram: Mr Richard KHAW Wei-kiang, S.C. (Chairman)
Mr Kenneth LAU Kwai-hin (Member)
Ms TONG Choi-cheng (Member)
Date of Decision: 28 April 2020

The Complaint

The Appellant received various letters from a bank (Bank A) and a debt collection company posted to his residential address (the Address), and the contents of which were related to collection of debts from him. The Appellant claimed that such letters were related to the bank account of another individual (Ms E) and were in no way associated with him. The Appellant subsequently noted that the Address was provided to Bank A by a credit reference agency (the Credit Reference Agency).

The Appellant first complained to Bank A and the debt collection company but was asked to contact the Credit Reference Agency directly to rectify the relevant information. The Appellant subsequently made a data correction request to the Credit Reference Agency and requested to have the Address removed from Ms E's record (the Relevant Address Record). Nonetheless, the Credit Reference Agency stated that the relevant information was previously provided by another bank (Bank B) whereby the Relevant Address Record was confirmed to be Ms E's "correct address" at the material time. The Credit Reference Agency thus refused to comply with the Appellant's data correction request.

The Appellant also considered that the Credit Reference Agency failed to take all practicable steps in ensuring the accuracy of the personal data, thereby contravening the requirements of DPP 2.

The Privacy Commissioner's Decision

Upon investigation, the Privacy Commissioner decided to exercise discretion not to further investigate into the Appellant's complaint under section 39(2)(d) of the PDPO for the following reasons:

上訴個案簡述 Appeal Case Note 1

1）該信貸資料機構在收集相關住址紀錄時並非在彙編有關上訴人的資料；及

2）相關住址紀錄經已從該信貸資料機構及乙銀行的資料庫中移除。換言之，有關資料準確性的爭議已獲解決。

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以《私隱條例》第39(2)(d)條作為不進一步處理投訴的理據，原因是該信貸資料機構及乙銀行已採取糾正措施，把相關住址紀錄從它們的資料庫中移除。此外，委員會亦認同私隱專員所指由於上訴人最初作出投訴的主要事項，即該信貸資料機構保存不準確的資料已獲處理，故任何進一步的調查亦不會帶來更滿意的結果。

即使上述觀點已足以駁回上訴人提出的論據，但為完整起見，委員會進一步考慮上訴人的上訴理由，而該等理據均被駁回如下：

1）甲銀行及乙銀行最初都是以資料使用者的身份收集相關住址記錄，不論是由戊女士或該信貸資料機構所收集。因此，戊女士才是資料當事人，而相關住址記錄並不構成上訴人的個人資料。

2）由於相關住址記錄並不構成上訴人的個人資料，上訴人向該信貸資料機構作出的投訴並不能成立。

行政上訴委員會的決定

上訴被駁回。

上訴人親身應訊
吳鎧楓高級律師（署理）代表私隱專員

環聯資訊有限公司法律及合規部高級顧問Craig Choy律師代表環聯資訊有限公司（受約束人）

1) The Credit Reference Agency was not compiling information about the Appellant when it collected the Relevant Address Record; and

2) The Relevant Address Record had been removed from the databases of the Credit Reference Agency and Bank B. In other words, the issues relating to the accuracy of personal data had been resolved.

Dissatisfied with the Privacy Commissioner's decision, the Appellant lodged an appeal to the AAB.

The Appeal

The AAB affirmed the Privacy Commissioner's decision not to pursue the complaint any further under section 39(2)(d) of the PDPO as remedial measures had already been taken by the Credit Reference Agency and Bank B in removing the Relevant Address Record from their databases. Further, the AAB agreed with the Privacy Commissioner that the subject matter of the Appellant's complaint, i.e., the maintaining of inaccurate personal data by the Credit Reference Agency had already been dealt with, and hence any further investigation would not bring about a more satisfactory result.

Although the above views were sufficient to refute the arguments advanced by the Appellant, for the sake of completeness, the AAB further considered the Appellant's grounds of appeal, which were all rejected by the AAB as follows:

1) Bank A and Bank B obtained the Relevant Address Record as data users in the first place, whether it was collected directly from Ms E or the Credit Reference Agency. Hence, Ms E was the data subject and the Relevant Address Record did not constitute the Appellant's personal data.

2) Given that the Relevant Address Record did not constitute the Appellant's personal data, his complaint against the Credit Reference Agency could not be substantiated.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Mr Dennis NG, Senior Legal Counsel (Acting) representing the Privacy Commissioner
Mr Craig Choy, Senior Consultant of Legal & Compliance Department for TransUnion Limited (the Person bound by the decision)

附錄三
Appendix 3

上訴個案簡述二

（行政上訴委員會上訴案件 第18/2020號）

投訴涉及個人的聲譽及身分於信函內被錯誤描述 — 主要標的事宜不關乎保障個人資料私隱 — 採取糾正措施 — 正確行使酌情權拒絕對投訴進行調查 — 進一步調查不能合理地預計可帶來更滿意的結果 — 保障資料第3原則：個人資料的使用

聆訊委員會成員：沈士文先生（主席）
何思鏞女士（委員）
劉佩芝女士（委員）
裁決理由書日期：2021年2月4日

投訴內容

上訴人曾受僱於某機構（下稱「該機構」），並擔任該機構的工會（下稱「該工會」）主席。該工會接獲一封匿名信，內附數頁屬於該機構一名前僱員的醫療報告（下稱「該報告」）。上訴人以該工會主席的身分與該機構會面，把該報告轉交予該機構。

該機構嘗試追查該報告外洩的源頭但不果。及後，上訴人得悉該機構曾去信另一名前僱員謝女士查詢（下稱「該信函」），而該信函提及是上訴人將該報告交予該機構。上訴人認為該信函內容作出錯誤描述，因他當時是以該工會主席身分而非個人身分收到該報告，並將該報告轉交該機構。再者，上訴人認為該信函的內容導致謝女士誤會上訴人把此事向該機構作出舉報，因而向謝女士「洩露」了他的身份及「損毀」了他的聲譽，故向私隱專員作出投訴。

私隱專員的決定

首先，私隱專員認為沒有證據可證明上訴人的個人聲譽受損，而聲譽本身並不構成《私隱條例》下定義的「個人資料」。此外，私隱專員也沒有發現任何證據指該機構是

Appeal Case Note (2)

(AAB Appeal No. 18 of 2020)

Complaint related to an individual's reputation and wrongful description of his personal capacity in a letter – primary subject matter did not relate to protection of personal data privacy – remedial measures taken – discretion not to investigate the complaint duly exercised – further investigation cannot reasonably be expected to bring about a more satisfactory result – DPP 3: use of personal data

Coram: Mr Erik Ignatius Shum Sze-man (Chairman)
Ms Mindy Ho Sze-may (Member)
Miss Julia Lau Pui-g (Member)
Date of Decision: 4 February 2021

The Complaint

The Appellant was previously employed by an organisation (the Organisation) and acted as the Chairman of a staff union of the Organisation (the Union). The Union received an anonymous letter containing copies of a few pages of the medical reports belonging to a former employee of the Organisation (the Reports). In his capacity as the Chairman of the Union, the Appellant met with the Organisation and passed the Reports to the same.

The Organisation tried to look into the source of the leakage of the Reports but to no avail. The Appellant subsequently noticed that the Organisation had sent a letter to Ms Tse, another former employee of the Organisation, for enquiry (the Letter). The Letter stated that it was the Appellant who passed the Reports to the Organisation. The Appellant contended that the Letter was factually incorrect as he had received the Reports and had given them to the Organisation in his capacity as the Chairman of the Union and not in his personal capacity. Further, the Appellant considered that the content of the Letter caused Ms Tse to misunderstand that he reported the matter to the Organisation, which "leaked" his identity to Ms Tse and "degraded" his reputation. The Appellant therefore lodged a complaint to the Privacy Commissioner.

The Privacy Commissioner's Decision

First, the Privacy Commissioner could not find any evidence indicating that there was any damage caused to the Appellant's reputation, and reputation itself did not constitute "personal data" as defined under the PDPO. Further, given that there was no

上訴個案簡述 Appeal Case Note 2

外洩該報告的源頭，故私隱專員行使《私隱條例》第 39(2)(ca) 及 39(2)(d) 條賦予的酌情權，拒絕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。

上訴

委員會確認私隱專員的決定，並認同：

1）從沒有任何證據指出該報告外洩是由該機構的不當做法引致。無論如何，該機構已採取一系列糾正措施，包括委聘獨立顧問檢討及加強訊息管理系統、按建議採取措施加強資料保安，並向僱員提供培訓，以提升他們對個人資料私隱的意識。該機構亦確認日後如有類似情況，在引述資料來源時，只會透露消息人士的職務身分，而不會指名道姓。

2）此外，即使假設私隱專員繼續調查投訴並證實上訴人的指控成立，有鑑於該機構已作出上述的糾正措施，私隱專員的調查亦不能帶來任何其他實質的結果。在這個情況下，私隱專員無須按照上訴人的要求發出執行通知。

3）上訴人的投訴主要涉及其聲譽和身分被錯誤描述，而不是投訴其姓名或其他個人資料於該信函中（又或於其他情況下）被披露。上訴人的投訴標的與保障其個人資料私隱無關。

行政上訴委員會的決定

上訴被駁回。

上訴人親身應訊
吳鎧楓高級律師（署理）代表私隱專員

陳樂信資深大律師代表中華電力有限公司（受約束人）

evidence indicating that the said leakage was caused by the Organisation, the Privacy Commissioner exercised the discretion under sections 39(2)(ca) and 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.

The Appeal

The AAB confirmed the Privacy Commissioner's decision and agreed that:

1) There was no evidence indicating that the leakage of the Reports was caused by any malpractice on the part of the Organisation. In any event, the Organisation had taken a series of remedial measures, including engaging an independent consultant to review and strengthen its data management system, implementing measures as recommended to enhance data security, and providing training to its employees to enhance their awareness of personal data privacy. The Organisation also confirmed that if a similar situation arose in future, it would only disclose the source of the information with reference to the informant's capacity instead of identifying the informant by name.

2) Further, even assuming that the Privacy Commissioner continued to investigate into the complaint and found the Appellant's complaint substantiated, in view of the aforesaid remedial measures taken by the Organisation, the Privacy Commissioner's investigation could not bring about any other concrete results. In this context, there was no need for the Privacy Commissioner to issue an Enforcement Notice as requested by the Appellant.

3) The Appellant's complaint was primarily related to his reputation and the wrongful description of his capacity, as opposed to divulging of his name or any other personal data in the Letter (or under any other circumstances). The subject of the Appellant's complaint was not related to protection of his personal data privacy.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Mr Dennis NG, Senior Legal Counsel (Acting) representing the Privacy Commissioner
Mr Abraham Chan, S.C. representing CLP Power Hong Kong Limited (the Person bound by the decision)

附錄三
Appendix 3

上訴個案簡述三

（行政上訴委員會上訴案件 第 23/2020 號）

未經上訴人同意使用電子健康紀錄於其他目的 — 採取糾正措施 — 正確行使酌情權拒絕對投訴進行調查 — 進一步調查不能合理地預計可帶來更滿意的結果 — 要求的濟助超出《私隱條例》涵蓋的範圍 — 保障資料第3原則：個人資料的使用

聆訊委員會成員：沈士文先生（主席）
郭岳忠先生（委員）
陳溢謙先生（委員）
裁決理由書日期：2021年3月16日

投訴內容

上訴人到醫療中心向一名醫生（下稱「甲先生」）求診。上訴人因不滿甲先生處方的藥物，遂向醫務委員會（下稱「醫委會」）作出投訴。醫委會認為沒有足夠證據顯示事件有任何失當行為，故駁回該投訴。

上訴人其後收到短訊通知，知悉甲先生曾查閱上訴人在電子健康紀錄互通系統（下稱「醫健通」）內的電子健康紀錄。因此，上訴人聲稱甲先生侵犯其私隱，向醫委會作出第二項投訴，而案件經上訴人同意後轉介至私隱專員作跟進。上訴人要求甲先生向他作出賠償及公開道歉。

私隱專員的決定

私隱專員經初步查詢後發現，甲先生查閱上訴人的電子健康紀錄，並非正在為上訴人作出治療，而是為了回顧病歷以回應醫委會的查詢，故甲先生查閱及使用上訴人的健康紀錄的目的與當初收集目的並不一致，違反保障資料第3原則。

私隱專員因此向甲先生發出書面警告，而甲先生承諾以後當查閱病人的醫健通電子健康紀錄時，務必嚴守「有需要知道」的原

Appeal Case Note (3)

(AAB Appeal No. 23 of 2020)

Use of electronic health record for other purpose without the Appellant's consent – remedial measures taken – discretion not to investigate the complaint duly exercised – further investigation cannot reasonably be expected to bring about a more satisfactory result – relief sought beyond the purview under the PDPO – DPP 3: use of personal data

Coram: Mr Erik Ignatius Shum Sze-man (Chairman)
Mr Dick Kwok Ngok-chung (Member)
Mr Eugene Chan Yat-him (Member)
Date of Decision: 16 March 2021

The Complaint

The Appellant consulted a doctor (Mr A) of a medical centre. The Appellant was dissatisfied with the medicine prescribed to him by Mr A and hence lodged a complaint to the Medical Council of Hong Kong (the Medical Council). The complaint was dismissed by the Medical Council on the ground that there was insufficient evidence as proof of any misconduct.

The Appellant subsequently received an SMS which stated that Mr A had accessed his electronic health record in the Electronic Health Record Sharing System (eHRSS). As a result, the Appellant lodged a second complaint to the Medical Council for an alleged violation of his privacy by Mr A. The case was referred to the Privacy Commissioner for follow-up upon the Appellant's consent. The Appellant demanded Mr A for compensation and an open apology.

The Privacy Commissioner's Decision

Upon preliminary enquiry, the Privacy Commissioner found that when Mr A accessed the Appellant's electronic health record, he was not providing medical treatment to the Appellant but to refresh his memory to handle the enquiry from the Medical Council. In this connection, the purpose of Mr A's access and use of the Appellant's health records at the material time was inconsistent with the original purpose for which the data was collected, thereby contravening DPP3.

Hence, the Privacy Commissioner issued a written warning to Mr A. In response, Mr A undertook that he would abide by the principle of "need-to-know" when he accessed any patient's electronic health

上訴個案簡述 Appeal Case Note 3

則(下稱「該承諾」),並確認自事件發生後不曾查閱上訴人的醫健通電子健康紀錄。

鑑於甲先生已就書面警告採取糾正措施,私隱專員認為並無必要就個案進行調查,故把個案轉介予電子健康紀錄統籌處(下稱「醫健通統籌處」),並行使《私隱條例》第39(2)(d)條的酌情權,決定不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。

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) 是次事件是單一事件,沒有證據顯示甲先生進一步違反該承諾。鑑於私隱專員已向甲先生發出書面警告及將個案轉介予醫健通統籌處,加上甲先生已採取糾正措施,委員會認同私隱專員不作進一步調查的決定。

2) 證據顯示上訴人的主要投訴是針對甲先生對待上訴人的方式及處方的藥物,卻沒有令上訴人蒙受實質或重大損害。倘上訴人欲要求甲先生作出賠償,他可根據《私隱條例》第66條提出相關的法律程序,但他沒有這樣做。上訴人希望藉向私隱專員作出投訴以獲得濟助,即要求甲先生作出賠償及公開道歉,其要求明顯已超出《私隱條例》涵蓋的範圍。

行政上訴委員會的決定

上訴被駁回。

上訴人親身應訊
吳凱欣助理律師代表私隱專員

吳漢輝大律師受肯尼狄律師行延聘代表甲先生(受約束人)

record in eHRSS in future (the Undertaking), and confirmed that he had not accessed the Appellant's electronic health record in eHRSS since then.

Given that Mr A had taken remedial measures in response to the written warning, the Privacy Commissioner considered that any investigation into the case was unnecessary and referred the case to the Electronic Health Record Office (eHR Office). The Privacy Commissioner also 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.

The Appeal

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

1) It was a one-off incident and there was no evidence suggesting that Mr A had further breached the Undertaking. Given that the Privacy Commissioner had already issued a written warning to Mr A and referred the case to the eHR Office, coupled with the remedial measures taken, the AAB affirmed the Privacy Commissioner's decision not to conduct further investigation.

2) There was evidence indicating that the Appellant's major complaint was about the manner in which he was treated by Mr A and the medicines so prescribed; there was however no actual or substantial damage caused upon the Appellant. If the Appellant wished to seek compensation from Mr A, he could commence legal proceedings under section 66 of the PDPO. However, he did not decide to do so. The intended relief sought by the Appellant in lodging a complaint to the Privacy Commissioner, i.e., compensation and an open apology from Mr A, was clearly outside the purview of the PDPO.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Ms Annabel Ng, Assistant Legal Counsel representing the Privacy Commissioner
Mr Eddie Ng, Barrister instructed by Messrs Kennedys for Mr A (the Person bound by the decision)

附錄三
Appendix 3

上訴個案簡述四

（行政上訴委員會上訴案件 第 28/2020 號）

查閱資料要求 — 未能闡明所要求的個人資料 — 要求文件以作上訴人的紀律聆訊用途 — 正確行使酌情權拒絕對投訴作進一步調查 — 保障資料第6原則：查閱個人資料

聆訊委員會成員：沈士文先生（主席）
陳溢謙先生（委員）
劉詠蔪工程師（委員）
裁決理由書日期：2021年2月19日

投訴內容

上訴人曾向其僱主（下稱「該僱主」）提交查閱資料要求，以索取該僱主對他作出紀律聆訊的所有相關調查報告、文件及信函（下稱「第一項查閱要求」）。該僱主就上訴人的第一項查閱要求已向其提供所要求的文件。

上訴人其後向該僱主提出另一項查閱要求，索取與上述紀律聆訊程序指引中五個不同段落相關的文件、紀錄或材料（下稱「第二項查閱要求」）。該僱主及後要求上訴人闡明於第二項查閱要求中所指的個人資料，惟上訴人逐字重覆第二項查閱要求的內容，未有進一步闡明確實所需查閱的個人資料。

由於該僱主沒有遵從上訴人提出的第二項查閱要求，故上訴人向私隱專員作出投訴。

私隱專員的決定

第一項查閱要求沒有任何爭議。關於第二項查閱要求，私隱專員認同當中所要求的文件之描述並不清晰。由於上訴人沒有回覆該僱主合理地提出的澄清要求，故應視之為從未提出有效的查閱資料要求。換言之，該僱主無需遵從上訴人所提出的第二項查閱要求。

Appeal Case Note (4)

(AAB Appeal No. 28 of 2020)

Data access request – failure to provide clarification of the personal data requested – requesting document for the purpose of the Appellant's disciplinary proceedings – discretion not to further investigate the complaint duly exercised – DPP 6: access to personal data

Coram: Mr Erik Ignatius Shum Sze-man (Chairman)
Mr Eugene Chan Yat-him (Member)
Ir Lau Wing-yan (Member)
Date of Decision: 19 February 2021

The Complaint

The Appellant previously made a data access request to his employer (the Employer) for all relevant investigation reports, documents, and correspondence associated with the disciplinary proceedings instituted by the Employer against him (1st DAR). The Employer provided the Appellant with documents in response to the 1st DAR.

The Appellant subsequently made another data access request (2nd DAR) to the Employer requesting all relevant documents, records or materials with reference made to five different paragraphs of the Employer's procedural guidelines for the aforesaid disciplinary proceedings. The Employer subsequently requested the Appellant to clarify the personal data as requested in the 2nd DAR, but the Appellant replied by making a verbatim reproduction of the 2nd DAR without providing any further clarification.

As the Employer did not comply with the 2nd DAR, the Appellant lodged a complaint to the Privacy Commissioner.

The Privacy Commissioner's Decision

There was no dispute in relation to the 1st DAR. With regard to the 2nd DAR, the Privacy Commissioner agreed that the description of the requested documents was unclear. Given that the Appellant did not respond to the Employer's reasonable request for clarification, there was no valid data access request in this instance. In other words, the Employer was not required to comply with the 2nd DAR.

上訴個案簡述 Appeal Case Note 4

另外，私隱專員有理由相信上訴人作出第二項查閱要求，似乎並非為了釐清該僱主持有其個人資料的種類，而是為了與個人資料私隱無關的其他目的。

根據*胡潔冰訴上訴委員會* [2007] 4 HKLRD 849一案中所確立的原則，查閱資料要求的目的並非用以輔助任何進行訴訟程序中文件披露的權利，或以便資料當事人尋求資料以作其他用途。私隱專員認為有關原則同樣適用於上訴人正面臨的紀律聆訊當中。就此，私隱專員引用《私隱條例》第39(2)(ca)及39(2)(d)條賦予的酌情權，拒絕對上訴人的投訴作進一步調查。

上訴人不滿私隱專員的決定，遂向委員會提出上訴。

上訴

委員會確認私隱專員的決定，並基於下述理由駁回上訴人的上訴：

1）第二項查閱要求過於含糊及籠統，因而並非有效的查閱資料要求，該僱主無需遵從上訴人的要求。在上述要求的敘述中，上訴人只引述該僱主的紀律聆訊程序指引當中的某些段落，但上訴人未有指明所需文件的性質及種類，藉此讓該僱主可遵從有關查閱要求。

2）《私隱條例》的目的並非讓資料當事人以此作為查閱文件或資料以作其他用途的途徑，尤其是當訴訟及紀律聆訊的文件披露是由其他法律原則及程序所規管。儘管本案件涉及紀律聆訊而非訴訟程序，私隱專員已正確地把*胡潔冰*一案中的原則應用於相關紀律聆訊。

行政上訴委員會的決定

上訴被駁回。

上訴人親身應訊
黃寶漫助理律師代表私隱專員

政府律師方穎琪代表消防處處長（受約束人）

Besides, there were reasons for the Privacy Commissioner to believe that the 2nd DAR did not appear to be made for the purpose of ascertaining the kinds of personal data held by the Employer, but was made for other purposes irrelevant to personal data privacy.

According to the principles established in *Wu Kit Ping v Administrative Appeals Board* [2007] 4 HKLRD 849, the purpose of lodging a data access request is not to supplement rights of discovery in legal proceedings or to enable a data subject to locate information for other purposes. The Privacy Commissioner considered that such principles should equally apply to the disciplinary proceedings that the Appellant was facing. Hence, the Privacy Commissioner exercised the discretion under sections 39(2)(ca) and 39(2)(d) of the PDPO not to carry out any further investigation into the Appellant's complaint.

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) The 2nd DAR was far too vague and general, and hence was not a valid data access request with which the Employer had to comply. The description of the said request was only related to certain references to the paragraphs in the Employer's procedural guidelines for disciplinary proceedings, but the Appellant failed to specify the nature and type of documents requested therein to enable the Employer to comply with the 2nd DAR.

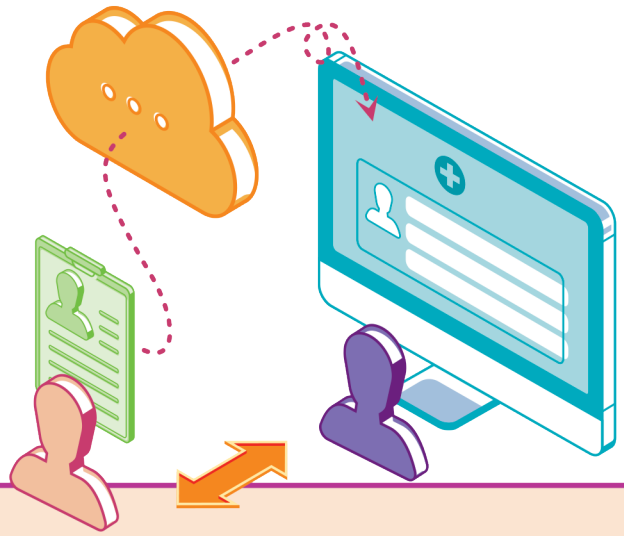
2) It is not the legislative intent of the PDPO to facilitate data subjects to gain access to documents or information for other purposes, especially when discovery of documents in litigation and disciplinary proceedings is governed by other legal principles and procedures. Though the disciplinary proceedings in the present case were not legal proceedings, the Privacy Commissioner had duly applied the same principle in the *Wu Kit Ping* case in respect of such disciplinary proceedings.

The AAB's Decision

The appeal was dismissed.

The Appellant appeared in person
Ms Clemence Wong, Assistant Legal Counsel representing the Privacy Commissioner
Ms Agnes Fong, Government Counsel representing Director of Fire Services (the Person bound by the decision)

附錄四
Appendix 4



投訴個案選錄，以作借鑑

個案一

為非醫療目的取覽病人電子健康紀錄 — 保障資料第3原則 — 個人資料的使用

投訴內容

投訴人曾同意讓一名醫生在電子健康紀錄互通系統中上載及取覽其健康紀錄。在唯一一次求診後，投訴人向香港醫務委員會（醫委會）投訴該醫生。在醫委會處理投訴人的個案期間，投訴人收到電子健康紀錄統籌處的短訊，得知該醫生在互通系統中查閱投訴人的電子健康紀錄。投訴人不滿該醫生並非為治療的目的查閱其健康紀錄，遂向私隱公署投訴該醫生。

結果

《私隱條例》的保障資料第3原則訂明，資料使用者如未得資料當事人的訂明同意，他的個人資料只可使用（包括披露或轉移）於當初收集資料時擬使用的目的或與此目的直接有關的目的上。私隱公署認為，該醫生在未有另行取得投訴人同意下，在互通系統中取覽投訴人的電子健康紀錄作治療以外的目的，違反了保障資料第3原則的規定。

Summaries of Selected Complaint Cases – Lesson Learnt

Case 1

Accessing a patient's electronic health record for non-medical purposes – DPP 3 – use of personal data

The Complaint

The Complainant gave consent to a doctor (Doctor) to upload his health record to the Electronic Health Record Sharing System (Sharing System) and access the said data. After the first and only visit, the Complainant made a complaint against the Doctor to the Medical Council of Hong Kong (Medical Council). While the Medical Council was handling the Complainant's case, the Complainant received a text message from the Electronic Health Record Office, informing him that the Doctor had accessed his electronic health record in the Sharing System. The Complainant was dissatisfied that the Doctor had accessed his health record for purposes not related to treatment and thus lodged a complaint against the Doctor with the PCPD.

Outcome

DPP 3 of the PDPO provides that without the prescribed consent of the data subject, his personal data may only be used (including disclosure or transfer) for the purpose for which the data was originally collected or for purposes directly related to that purpose. The PCPD was of the view that the Doctor was in contravention of DPP 3 by accessing the Complainant's electronic health record in the Sharing System for a purpose other than providing treatment to the Complainant and without obtaining separate consent from the Complainant.

投訴個案選錄 • 以作借鑑
Summaries of Selected Complaint Cases – Lesson Learnt

1

私隱公署介入後，該醫生承諾日後只會在向病人提供治療時，按「有需要知道」原則取覽互通系統中的健康紀錄。

其後私隱公署亦向該醫生發出警告，要求他確保本案的違規事件不會重演。此外，私隱公署亦將個案轉介予管理互通系統的電子健康紀錄統籌處作跟進。

借鑑

醫護人員應以此案為鑑，務必以審慎態度配合專業判斷，評估取覽病人電子健康紀錄的需要。不當使用互通系統內的病人資料不但會違反《私隱條例》保障資料第3原則的規定，亦可能不符合電子健康紀錄統籌處就使用互通系統所訂立的實務守則。

Upon the PCPD's intervention, the Doctor undertook to access electronic health records in the Sharing System only for the purpose of providing treatment to patients and on a "need-to-know" basis.

Regarding the incident, the PCPD issued a warning to the Doctor, requesting him to ensure that the non-compliance in this case would not be repeated. In addition, the PCPD referred the case to the Electronic Health Record Office, which manages the Sharing System, for follow-up actions.

Lesson Learnt

Healthcare providers should exercise prudence and professional judgment before assessing patients' data in the Sharing System. Inappropriate use of the patients' data in the Sharing System not only contravenes DPP 3 of the PDPO, but may also violate the Code of Practice for using the Sharing System .

附錄四
Appendix 4

個案二

旅行社向第三者披露客戶的付款資料 — 保障資料第3原則 — 個人資料的使用

投訴內容

一間旅行社的常客A小姐介紹投訴人在該旅行社購買機票。投訴人其後未有支付餘款，而該旅行社亦無法與投訴人取得聯繫。就此，該旅行社向A小姐發電郵詢問投訴人的地址，並向A小姐披露了投訴人逾期付款的詳情。投訴人認為該旅行社不應向A小姐披露其付款資料，目的為向他施加壓力以追收欠款。就此，投訴人向私隱公署作出投訴。

結果

私隱公署認為，縱使該旅行社因無法聯絡投訴人而向介紹人詢問投訴人的聯絡地址，該旅行社亦無必要向介紹人透露投訴人逾期付款的詳情。

私隱公署介入後，該旅行社承諾日後在類似情況下，不會向第三者披露非必要的客戶資料。

私隱公署已向該旅行社發出警告，要求該旅行社定期提醒員工《私隱條例》的相關規定，並採取適當措施確保員工遵守。

Case 2

Disclosure of a customer's payment information to a third party by a travel agency – DPP 3 – use of personal data

The Complaint

Miss A, a regular customer of a travel agency, recommended the Complainant to purchase a flight ticket from that travel agency. The Complainant failed to pay the balance and the agency was unable to get in touch with the Complainant. The travel agency then sent an email to Miss A, asking for the address of the Complainant but the email disclosed the details of the Complainant's overdue payment. The Complainant considered that the travel agency should not have disclosed his payment information to Miss A and the purpose of such disclosure was to exert pressure on him. Hence, the Complainant made a complaint with the PCPD.

Outcome

The PCPD found that even though the travel agency was unable to reach the Complainant and had to ask his referee for his contact address, it was unnecessary for the travel agency to disclose details of the overdue payment to the referee.

After the PCPD's intervention, the travel agency undertook not to disclose unnecessary information of customers to third parties in similar circumstances.

Regarding the incident, the PCPD issued a warning to the travel agency, requesting it to regularly remind its staff members of the relevant requirements under the PDPO and implement measures to ensure compliance.

投訴個案選錄 • 以作借鑑
Summaries of Selected Complaint Case – Lesson Learnt

2

借鑑

根據保障資料第3原則，客戶的個人資料只能用於與當初收集目的相同或直接相關的目的。

客戶的財務資料（例如拖欠付款）通常被視為敏感資料，應格外小心處理。除非有實質需要，否則不應向第三者披露此等資料。如果需要接觸介紹人以尋找客戶，只應按目的而向介紹人提供恰好足夠的資訊。向介紹人披露過量的客戶個人資料（例如付款的詳細資料），便可能違反保障資料第3原則的規定。

Lesson Learnt

DPP 3 requires that personal data shall only be used for a purpose that is the same as or directly related to the original collection purpose.

The financial status of a customer, such as default in payment, is commonly considered sensitive data. Such data should be handled with extra care and only be disclosed to a third party when there is a genuine need. If a referee is contacted to locate a customer, only the minimum data for identification should be shared. Excessive disclosure of personal data (e.g. payment details) to a referee may contravene the requirements under DPP 3.

附錄四
Appendix 4

個案三

醫院沒有預先通知醫生而收集巡房時間及診治病人數目 — 保障資料第1原則 — 個人資料的收集

投訴內容

投訴人在一間公營醫院任職醫生。投訴人不滿該醫院的管理層在沒有預先通知他的情況下，收集其巡房的時間及診治病人數目等數據。

結果

該醫院的管理層解釋，因應臨床服務模式轉變，遂收集醫院內多名醫生的診症時間和診治病人數目等數據，作計算不同類別病人的服務成本之用。

在私隱公署介入後，負責監察該醫院行政工作的機構承諾修訂內部指引，確保指引涵蓋員工入職後收集個人資料的情況，並清楚說明收集個人資料的目的和用途。此外，該機構已向全體員工發出電郵，提醒員工在收集個人資料之前，必須明確地告知同事有關收集資料的目的。

私隱公署亦就事件向該機構發出警告，要求密切監察員工遵守上述內部指引。

Case 3

A hospital collected the time spent by a doctor on wards rounds and the number of patients he attended to, without prior notification – DPP 1 – collection of personal data

The Complaint

The Complainant was a doctor at a public hospital. He was dissatisfied that the hospital management collected statistical data concerning him, such as the time he spent on ward rounds and the number of patients he attended to, without any prior notification.

Outcome

The hospital management explained that, due to changes in clinical service model, it collected data including doctors' consultation time and number of patients attended to for calculating the service cost for different types of patients.

After the PCPD's intervention, the organisation managing the hospital promised to amend its internal guidelines to ensure that they covered the situations in which the employees' personal data were collected, and clearly stated the purpose and use of such collection. Moreover, the organisation sent emails to its employees, reminding them to inform colleagues of the purpose of collection before collecting the personal data from them.

Regarding the incident, the PCPD issued a warning to the organisation, requesting it to closely monitor its employees' compliance with the said guidelines.

投訴個案選錄 • 以作借鑑
Summaries of Selected Complaint Cases – Lesson Learnt

3

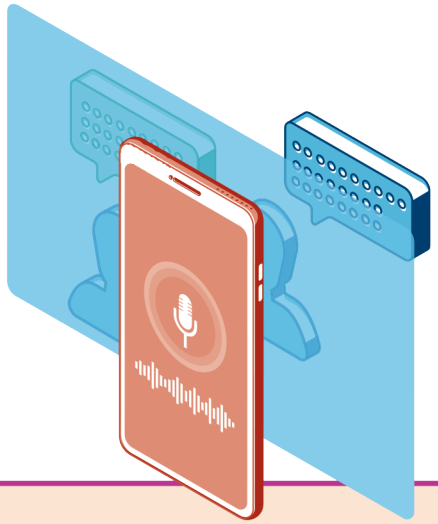
借鑑

該醫院管理層在本案中收集數據的行為出於行政及統計需要，與其管理醫院的職能直接有關。然而，管理層在收集數據前，未有告知醫生收集資料的目的等詳情。當醫生知悉在不知情下被收集數據，難免會猜測管理層的用意，或憂慮數據可能被用作工作表現評估，舉動損害了醫生對管理層的信任。私隱公署欣悉該機構迅速作出上述改善措施，提高收集個人資料安排的透明度，減少僱員的猜疑，重建互信。

Lesson Learnt

The hospital management collected data for administrative and statistical purposes, which were directly related to its function of managing the hospital. However, the management collected the data without informing the doctors of the collection purposes. Hence, when the doctors learnt that the management had collected such data without prior notification, inevitably they speculated or were worried that the data was used to evaluate their work performance. Trust was hence damaged. The PCPD was pleased that the organisation had promptly taken the above remedial actions, and improved the transparency of personal data collection to avoid suspicion and rebuild trust with its employees.

附錄四
Appendix 4



個案四

上司以不公平手法把與下屬對話的內容錄音 — 保障資料第1原則 — 個人資料的收集

投訴內容

投訴人是某公營機構的職員，其部門主管先後兩次跟投訴人討論其工作表現。其後，投訴人得知兩次會議均被錄音。投訴人不滿主管偷錄會議，遂向私隱公署作出投訴。

結果

兩次會議的討論內容均圍繞投訴人的工作表現，故會議錄音屬投訴人的個人資料，但私隱公署認為在相關會議進行錄音並非不合法。然而，主管沒有在會議前將錄音安排告知投訴人，則屬不公平收集投訴人的個人資料，違反保障資料第1(2)原則。此外，主管也沒有在會議進行錄音時或之前告知投訴人收集其個人資料的目的，亦違反了保障資料第1(3)原則。

Case 4

Unfair audio-recording of conversations with a subordinate by a supervisor – DPP 1 – collection of personal data

The Complaint

The Complainant was an employee of a public organisation. His supervisor met with him twice to discuss his work performance. After the meetings, the Complainant learned that the meetings were audio-recorded and was dissatisfied with his supervisor's covert actions. He thus lodged a complaint to the PCPD.

Outcome

The Complainant's work performance was the subject of discussion of the meetings. The audio-record of the meetings therefore constituted the Complainant's personal data. The PCPD considered that the act of audio-recording the meetings was not unlawful. However, the supervisor failed to inform the Complainant of the audio-recording arrangement prior to the meetings. This amounted to unfair collection of the Complainant's personal data and was in breach of DPP 1(2). In addition, the supervisor also failed to inform the Complainant of the purpose of collection of his personal data on or before he started to audio-record the meetings, hence violating DPP 1(3).

投訴個案選錄 • 以作借鑑
Summaries of Selected Complaint Cases – Lesson Learnt

4

因應私隱公署的意見及為防止同類事件再次發生，該機構制定了書面指引，所有人員以錄音方式收集個人資料時，在錄音進行之時須向在場人士明確說明正在錄音。該機構亦提醒該主管日後必須根據上述指引行事，並將是次事件納入員工培訓教材。

私隱公署亦就事件向該機構發出警告，要求它定時審核相關措施，並密切監察其員工有否嚴緊遵從上述指引行事。

借鑑

在資料當事人不知情下偷錄對話，可被當事人視為不受歡迎或侵擾個人資料私隱的行為。雖然《私隱條例》沒有要求資料使用者在收集個人資料前取得資料當事人的同意，但資料使用者必須以公平及合法的方法收集個人資料。為避免爭端，錄音者在進行錄音前，應告知資料當事人對話會被錄音及錄音之目的。

In response to the PCPD's advice and to prevent the recurrence of similar incidents, the organisation established written guidelines, instructing all staff collecting personal data by means of audio-recording to make it clear to those present at the time of recording that recording would be made. It also reminded the supervisor that he must follow the said guidelines in future and included this incident in its employee training materials.

Regarding the incident, the PCPD had issued a warning to the organisation, requesting it to review the relevant measures regularly and to closely monitor its employees' compliance with the said guidelines.

Lesson Learnt

Surreptitiously recording a conversation without the knowledge of the data subject may be considered by the data subject as unwelcome or even intrusive to personal data privacy. Although the PDPO does not require a data user to obtain the data subject's consent before collecting his personal data, the data user must collect personal data in a fair and lawful manner. To avoid disputes, before audio-recording, the recording party should inform the data subject that the subsequent conversation will be recorded and the purpose of the recording.

附錄五
Appendix 5

檢控個案選錄

個案 1

電訊公司被控在未獲投訴人同意下使用其個人資料作直接促銷，亦沒有依從投訴人的拒收直銷訊息要求—《私隱條例》第 35E 及 35G 條

投訴內容

投訴人於2014年9月開始使用一間電訊公司的寬頻服務，並於2016年11月向該公司提出拒收直接促銷資訊的要求。然而，投訴人卻於2018年3月及7月期間，合共收到三次該公司推廣新服務計劃的來電。

結果

該公司被控違反六項《私隱條例》的罪行，包括三項在未獲資料當事人同意下，將該名資料當事人的個人資料使用於直接促銷（違反《私隱條例》第35E(1)條），及三項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）。

該公司承認上述六項控罪，每項控罪分別被判罰款港幣2,000元，共被判罰款港幣12,000元。

Summaries of Selected Conviction Cases

Case 1

Using personal data in direct marketing without consent and failing to comply with opt-out request – sections 35E and 35G of the PDPO

The Complaint

The Complainant subscribed to a telecommunications company's broadband service in September 2014 and opted out of receiving its direct marketing messages in November 2016. However, in March and July 2018, he subsequently received a total of three direct marketing calls from the telecommunications company promoting a new service plan.

Outcome

The telecommunications company faced six charges under the PDPO, including three charges of failing to obtain the Complainant's consent for using his personal data in direct marketing (contrary to section 35E(1) of the PDPO) and three charges of failing to comply with the requirement from a data subject to cease to use his personal data in direct marketing (contrary to section 35G(3) of the PDPO).

The telecommunications company pleaded guilty to the six charges and was fined HK$12,000 in total (HK$2,000 in respect of each charge).

檢控個案選錄
Summaries of Selected Conviction Cases

1

借鑒

市民日漸提升保障個人資料私隱的意識，機構更須尊重客戶對其個人資料使用於直接促銷的意願。這有助機構建立顧客的信心及提升直銷行業的專業性和成效，對機構和消費者來說可謂雙贏。另一方面，違反《私隱條例》下有關直接促銷的規定可構成罪行，每項控罪可處最高罰款港幣50萬元及監禁3年。

Lesson Learnt

In view of the rising public awareness of the importance of protecting personal data privacy, organisations should respect their customers' preferences on the use of their personal data in direct marketing. This is conducive to building customer trust, enhancing the professionalism of the industry, and increasing the effectiveness of direct marketing, thus leading to a win-win outcome for both companies and consumers. Failure to comply with the requirements under the PDPO in relation to direct marketing is an offence, which could lead to a fine of up to HK$500,000 and imprisonment of up to 3 years.

附錄五
Appendix 5

個案 2

電訊公司職員未獲公司同意而披露由公司取得的客戶個人資料 —《私隱條例》第 64(2) 條

投訴內容

一名電訊公司的技術員，從公司電腦系統中取得一名警務人員家屬的個人資料（包括電話號碼、英文名字、中文名字及香港身份證號碼），並將有關資料提供予社交平台的「起底」群組。上述資料其後於社交平台被公開發布，導致該名警務人員及其家屬蒙受心理傷害。

結果

該技術員被裁定四項罪行罪名成立，包括三項「目的在於使其本人或他人不誠實地獲益而取用電腦」及一項「披露未經資料使用者同意而取得個人資料而導致當事人蒙受心理傷害」罪，後者屬《私隱條例》第 64(2) 條下的罪行。

就違反《私隱條例》第 64(2) 條，該技術員被判處 18 個月監禁，連同其他定罪合共監禁 24 個月。

Case 2

An employee of a telecommunications company obtained and disclosed a customer's personal data without the company's consent – section 64(2) of the PDPO

The Complaint

A technician who worked for a telecommunications company obtained the personal data (including phone number, English name, Chinese name and HKID Card number) of one family member of a police officer from the company's computer system. The technician then provided the personal data to a "doxxing channel" on a social media platform. The personal data of the family member was publicised on the platform, causing psychological harm to the police officer and his family members.

Outcome

The technician was convicted of four offences, including three counts of "access to computer with criminal or dishonest intent with a view to dishonest gain for himself or another" and one count of "causing psychological harm to a data subject by disclosing personal data obtained without the data user's consent". The latter is an offence under section 64(2) of the PDPO.

The technician was sentenced to imprisonment for 18 months for an offence under section 64(2) of the PDPO. Together with other convictions, he was sentenced to imprisonment for 24 months.

檢控個案選錄
Summaries of Selected Conviction Cases

2

借鑒

「起底」是指透過網上搜尋器、社交平台、討論區、公共登記冊、匿名報料等方式，搜集目標人士或其相關人士（如家屬、親友等）的個人資料，並發布在互聯網、社交媒體及其他公眾平台等（如公眾地方）。

「起底」對受害人影響深遠，對當事人及家屬所造成的心理傷害不容忽視。事實上，絕大部份「起底」活動的目的只為對受害人施加心理壓力。「起底」不但不道德，「起底」人士亦可能需要承受嚴重的法律後果。《私隱條例》第64(2) 條訂明，任何人披露未經資料使用者同意而取自該資料使用者的某資料當事人的個人資料，而該項披露導致該資料當事人蒙受心理傷害，即屬違法。該罪行的最高刑罰是罰款港幣100萬元及監禁5年。

Lesson Learnt

Doxxing refers to the gathering of the personal data of target person(s) or related person(s) (such as family members, relatives or friends) through online search engines, social platforms, discussion forums, public registers, anonymous reports, etc., and disclosure of the personal data on the Internet, social media and other open platforms (such as public places).

The impact of doxxing on victims is far-reaching and the psychological damage caused to the victims and their families cannot be ignored. In fact, the vast majority of doxxing acts are intended to exert psychological pressure on the victims. Doxxing is not only immoral. The doxxer may also have to bear serious legal consequences. According to section 64(2) of the PDPO, it is an offence to disclose personal data of a data subject without the data user's consent and if the disclosure causes psychological harm to the data subject. The maximum penalty of the offence is a fine of HK$1,000,000 and imprisonment for 5 years.

附錄五
Appendix 5

個案 3

護士未獲得診所同意而披露由診所取得的病人個人資料 —《私隱條例》第 64(2) 條

投訴內容

一名在診所任職的護士，將載有一名求診警員的個人資料（包括姓名、香港身份證號碼、出生日期和電話號碼）的電腦螢幕截圖，連同貶義評論，上載至社交媒體帳戶，導致該名警員蒙受心理傷害。

結果

該名護士被控兩項罪行，分別為「目的在於使其本人或他人不誠實地獲益而取用電腦」及「披露未經資料使用者同意而取得個人資料而導致當事人蒙受心理傷害」，後者屬《私隱條例》第 64(2) 條下的罪行。

該名護士承認上述兩項控罪，共被判 240 小時社會服務令。

Case 3

A nurse obtained and disclosed a patient's personal data without the clinic's consent – section 64(2) of the PDPO

The Complaint

A nurse who worked for a clinic captured a screenshot containing the personal data (including name, HKID Card number, date of birth and phone number) of a police officer from the clinic's computer system. She then uploaded the screenshot together with some derogatory comments to her social media account. The disclosure of the personal data had caused psychological harm to the police officer.

Outcome

The nurse faced two charges, including "access to computer with criminal or dishonest intent with a view to dishonest gain for himself or another" and "causing psychological harm to a data subject by disclosing personal data obtained without the data user's consent". The latter is an offence under section 64(2) of the PDPO.

The nurse pleaded guilty to the two charges above and was sentenced to a 240-hour community service order.

檢控個案選錄
Summaries of Selected Conviction Cases

3

借鑒

該名護士乘工作之便，針對受害人的職業，將他的個人資料發布到社交媒體，令受害人承受被滋擾的風險及重大心理困擾。現今社交媒體及即時通訊軟件使用廣泛，資料傳播得又快又遠，影響極大。「起底」者要承擔嚴重法律後果，網絡世界亦非法外之地，故此所有社交媒體用戶必須謹記守法。

Lesson Learnt

The nurse took advantage of her job and posted the victim's personal data on social media, targeting his occupation and exposing him to risks of harassment and significant psychological distress. Social media and instant messaging software are widely used nowadays. Once a photo is uploaded, it would not be possible to control how quickly or widely it gets spread. The impact on the victim could be extremely serious and far-reaching. Given the serious legal consequences, all social media users should bear in mind that the cyberworld is not beyond the law.

附錄六
Appendix 6

循規行動個案選錄，以作借鑑

個案 1

國際連鎖服裝公司的客戶個人資料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

一間國際連鎖服裝公司向私隱公署通報，指其載有電子商務客戶及忠誠計劃會員的客戶個人資料系統被勒索軟件攻擊，導致資料外洩事故，涉及約 200,000 客戶紀錄，包括姓名、電話號碼、電郵地址、性別及年齡組別。

該公司聘請獨立顧問就該事故作出調查。調查結果顯示該公司未能發現一個已為人知可被攻擊的漏洞，讓攻擊者成功透過該漏洞，使用有效憑證資料登入客戶個人資料系統，於該公司的網絡安裝勒索軟件。

Summaries of Selected Compliance Cases – Lesson Learnt

Case 1

Unauthorised access to an international fashion chain's customer personal data system – DPP 4 – security of personal data

Background

An international fashion company reported to the PCPD that its customer personal data system for e-commerce customers and loyalty programme members suffered a ransomware attack. As a result, about 200,000 customer records containing names, telephone numbers, email addresses, genders and age ranges were compromised.

The company engaged an independent consultant for investigation, which revealed that the company had failed to identify a known exploitable vulnerability. The attacker successfully logged into the customer personal data system with valid credentials and installed ransomware in the company's network.

循規行動個案選錄 • 以作借鑑個案
Summaries of Selected Compliance Cases – Lesson Learnt

1

補救措施

該公司採取了下述的補救措施：

（i） 通知受該事故影響的所有客戶；
（ii）掃描系統尋找出所有已識辨的漏洞並作出修補；
（iii）加強監控系統的保安偵測及保護措施；
（iv）登入系統採用多重身份認證；及
（v）設定資料的保存期限，每年刪除過時的資料。

借鑑

資料使用者應定期檢視及監察其網絡的保安措施，並適時進行測試及安裝相關系統的保安修補。資料使用者亦應把個人資料的保存期限，設定為不長於為完成收集個人資料目的之所需時間。保存期限越短，保安風險亦會越低。

Remedial Measures

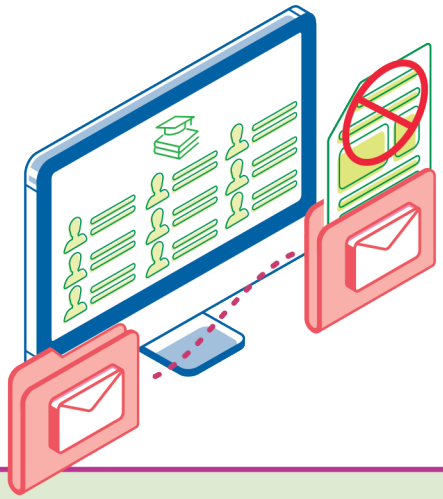
The company took the following remedial measures:

(i) Notified all affected customers;
(ii) Scanned the system for all identified vulnerabilities and applied patches;
(iii) Strengthened the detection and protection measures of its monitoring system;
(iv) Enforced multi-factor authentication at login; and
(v) Defined retention periods and erased obsolete data on an annual basis.

Lesson Learnt

Data users should regularly review and monitor security of their networks and test and apply security patches in a timely manner. Data users should also limit the retention period of personal data, which should not be longer than necessary for the fulfilment of the collection purpose. The shorter the retention period, the lower the security risks.

附錄六
Appendix 6



個案2

大學在電郵意外披露學生的個人資料 — 保障資料第4原則 — 個人資料的保安

背景

一所大學學院的員工以密件副本方式發送電郵，通知學院的部份非本地學生有關大學的隔離安排。但當該員工在一份載有所有學生的總表中選取非本地學生的電郵地址時，意外地在電郵中夾附了該總表。

該總表載有約2,500名有關學院學生的姓名、出生日期、國籍、電郵地址、通訊地址及聯絡電話號碼。因此，該些個人資料被不必要地披露予該電郵的所有收件者。涉事大學向私隱公署通報上述事故。

Case 2

Inadvertent disclosure of students' personal data via email by a university – DPP 4 – security of personal data

Background

A faculty staff member intended to email the faculty's non-local students about the university's quarantine arrangements. However, when retrieving the email addresses of the non-local students from the faculty's master list of students, the staff member mistakenly attached the master list in the email.

The master list contained names, dates of birth, nationalities, email addresses, correspondence addresses and contact numbers of about 2,500 students of the faculty. As a result, the personal data was unnecessarily disclosed to the recipients of the email concerned. The university reported the incident to the PCPD.

循規行動個案選錄 • 以作借鑑個案
Summaries of Selected Compliance Cases – Lesson Learnt

2

補救措施

該大學現要求所有寄給部門以外並載有個人資料的電郵，必須在發送前由另一位員工檢查。此外，載有學生個人資料的工作檔案（例如涉事的總表）必須加密保護。

借鑑

大學持有大量學生個人資料，因此應採取切實可行的措施，以確保負責處理學生個人資料的員工接受培訓，員工應遵從有關個人資料私隱方面的政策，並審慎實行。大學應建立相關程序，確保員工遵從這些政策。

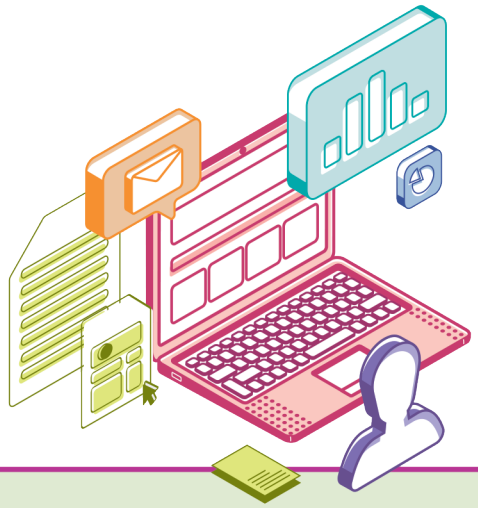
Remedial Measures

The university now requires all outbound emails containing personal data be checked by another staff member before they are sent. Besides, work files containing personal data, for example, the master list, must be encrypted.

Lesson Learnt

Universities possess a large volume of students' personal data and should therefore take reasonably practicable measures to ensure that staff handling such data are properly trained. Staff should observe relevant personal data privacy policies and exercise due diligence in applying those policies. Universities should establish procedures to ensure staff's compliance with those policies.

附錄六
Appendix 6



個案3

遺失載有工作檔案的手提電腦 — 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，指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在家工作的手提電腦。該手提電腦載有約400名該部門員工的個人資料，包括姓名、電郵地址、職位及員工號碼，而有關資料已被加密保護。

補救措施

由於該手提電腦內的資料已被加密保護，相關個人資料受未獲准許或意外查閱的風險較低。不過，該部門已提醒所有員工，需小心保護於該部門的便攜裝置內儲存的個人資料。

此外，該部門已要求所有員工在家工作時，應盡量透過虛擬私人網絡讀取工作檔案，以替代儲存工作檔案於手提電腦內。

Case 3

Loss of notebook computer containing work files – DPP 4 – security of personal data

Background

A government department reported to the PCPD that a staff member lost an official notebook computer on public transport. The computer, provided to the staff member for work-from-home (WFH) arrangement, contained encrypted personal data (names, email addresses, posts, and staff numbers) of about 400 staff members of the department.

Remedial Measures

While encryption lowered the risk of unauthorised access to the personal data, the department reminded staff to take extra care in handling official portable devices.

Besides, the department requested staff to access work files through VPN connection instead of storing work files locally when practicable.

循規行動個案選錄 • 以作借鑑個案
Summaries of Selected Compliance Cases – Lesson Learnt

3

借鑑

自2019冠狀病毒病出現，機構採取在家工作安排，令個人資料較以往有更大機會遭外洩。2020年11月，私隱專員就在家工作安排發出三份「在家工作安排下的個人資料保障」系列的實用指引，為機構、僱員及視像會議軟件使用者提供實務建議，以加強資料保安及個人資料保障。

機構在檢討在家工作安排的政策時，可參考上述的實用指引。一般來說，機構應當：

- 為在家工作安排下的資料處理（包括個人資料）制定清晰的政策；
- 採取所有合理切實可行的步驟確保資料安全，特別是當涉及使用資訊及通訊科技，或將資料和文件轉移予僱員在家工作；
- 為在家工作的僱員提供足夠培訓及支援；及
- 確保為僱員提供的電子裝置內的資料安全。

Lesson Learnt

The outbreak of COVID-19 compelled organisations to adopt WFH arrangement, making personal data more susceptible to breach. In November 2020, the Privacy Commissioner issued three "Protecting Personal Data under Work-from-Home Arrangements" Guidance Notes. They provided practical advice for organisations, employees and users of video conferencing software to enhance data security and personal data protection.

Organisations may make reference to these Guidance Notes when reviewing their WFH policies. Generally speaking, organisations should:

- Set out clear policies on the handling of data (including personal data) in WFH arrangements;
- Take all reasonably practicable steps to ensure the security of data, in particular when information and communication technology is adopted, or when employees possess source or copies of data and documents to work from home;
- Provide sufficient training and support to employees; and
- Ensure the security of the data stored in the electronic devices provided to employees.

附錄六
Appendix 6

個案 4

流動應用程式傳送未受加密的個人資料 — 保障資料第 4 原則 — 個人資料的保安

背景

在監察個人資料風險時，私隱公署或會檢視個別資料使用者涉及大規模收集和使用個人資料的行動。

在 2020 年下半年，私隱公署就本地研發及營運並涉及收集個人資料的流動應用程式，進行保安測試，以檢視有關公司是否符合保障資料第 4 原則的要求。

私隱公署發現 14 個流動應用程式沒有使用足夠加密以保障傳送的個人資料。攻擊者可能就此干擾數據傳送，暗中竊取資料或修改傳送路徑。

Case 4

Unencrypted personal data transmitted in mobile applications – DPP 4 – security of personal data

Background

In monitoring personal data risks, the PCPD may inspect the activities of a data user involving large-scale collection and use of personal data.

In the second half of 2020, the PCPD conducted security testing to determine whether the mobile applications (apps) developed or operated by local enterprises which involved the collection of customers' personal data complied with DPP 4.

The PCPD found that 14 apps did not use adequate encryption to securely transmit personal data. As such, attackers could secretly eavesdrop or modify the transmission data.

循規行動個案選錄 • 以作借鑑個案
Summaries of Selected Compliance Cases – Lesson Learnt

4

補救措施

所有有關機構接納私隱公署的建議更新相關應用程式，採用加密工具保障所傳送的個人資料。

借鑑

網上活動和交易方便了我們的生活，但同時亦為個人資料私隱帶來不能忽視的風險。假如流動應用程式未有採用嚴謹保安措施，保護所收集的個人資料，有關資料可能會落入黑客手中。

機構必定要保護及尊重客戶的個人資料，才能贏得信任，從而在市場上保持競爭力。機構應定期檢視及更新其流動應用程式，以確保個人資料受保障。

Remedial Measures

All enterprises concerned took the PCPD's advice and implemented adequate encryption in their apps to protect personal data transmission.

Lesson Learnt

Online activities and transactions are convenient but carry non-negligible risks to personal data privacy. Personal data collected by different apps may end up in the hands of hackers if such data is not protected by stringent security measures.

Organisations must protect and respect personal data to garner the trust of their customers to remain competitive. Organisations should regularly review and update their apps to ensure security of personal data.


PCPD
HK
pcpd