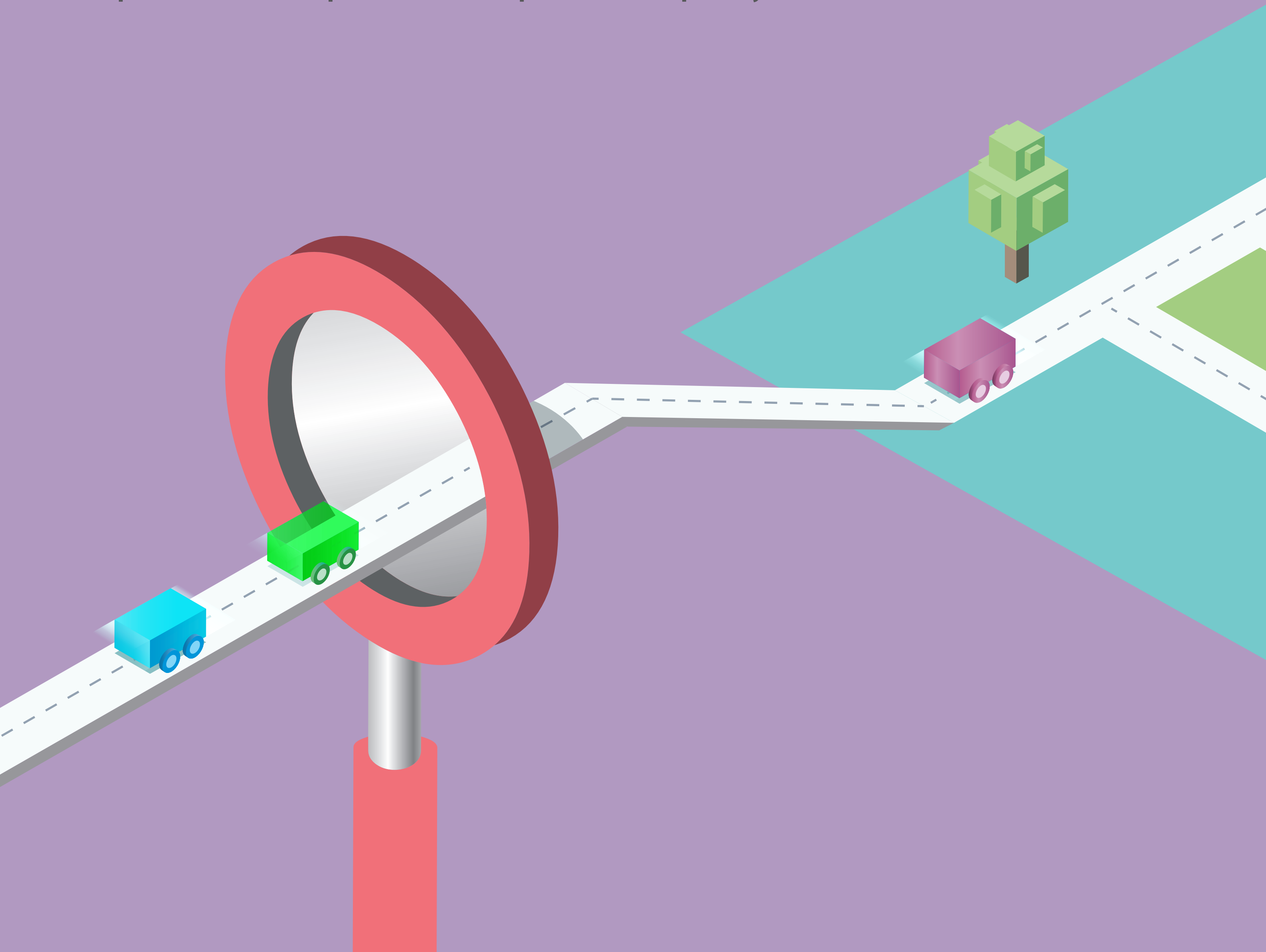
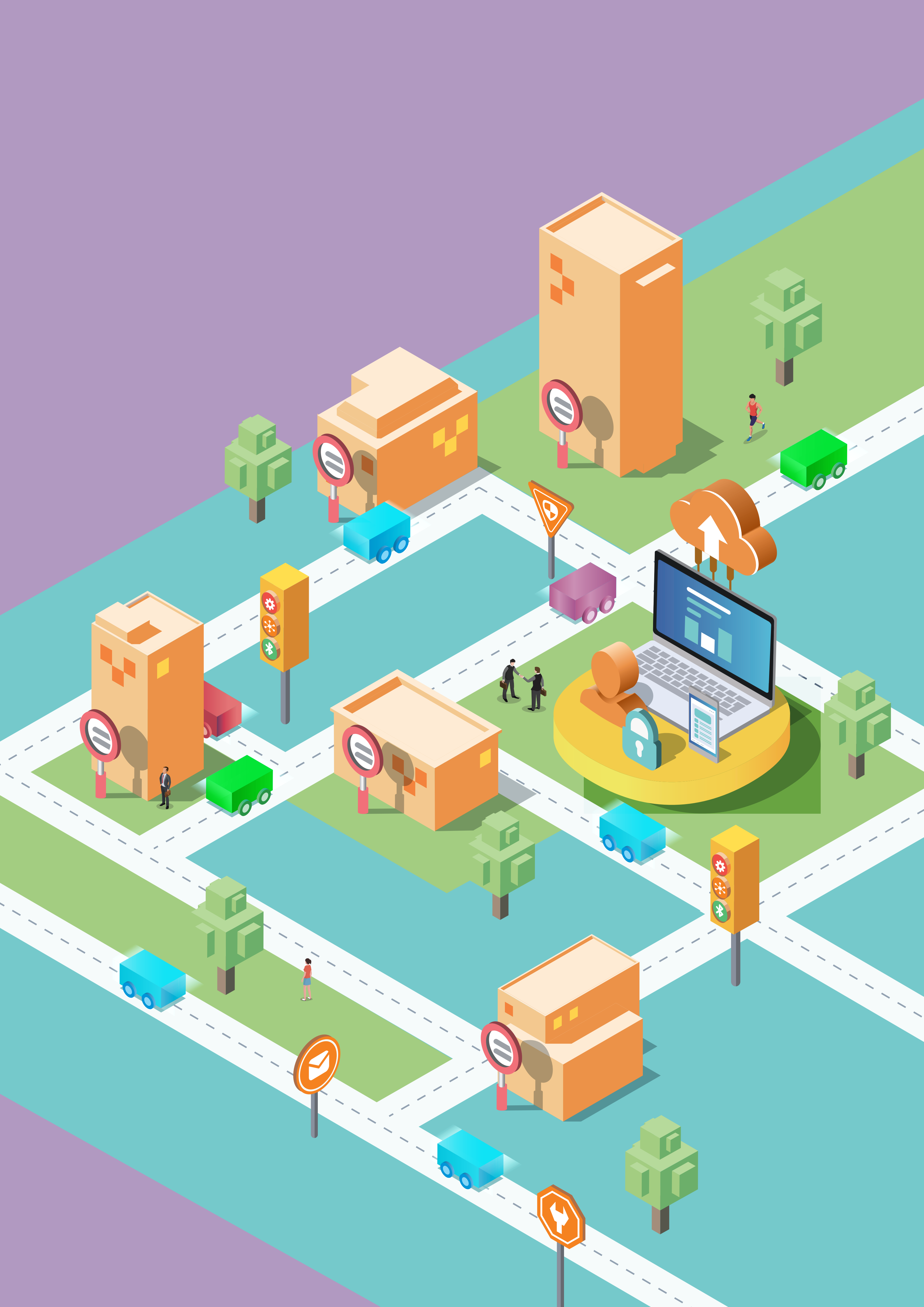
MONITORING COMPLIANCE EMBRACING CHALLENGES
監督符規 擁抱挑戰

公署監察和推動資料使用者要循規以符合《私隱條例》的規定。隨著資訊科技急速發展而衍生的私隱風險，公署鼓勵和支援機構採取合乎道德的措施保障個人資料， 並尊重消費者的個人資料私隱。

The PCPD monitors and promotes compliance with the provisions of the Ordinance. In view of the privacy risks brought about by the rapid advancement in information and communications technology, we encourage and facilitate organisations to adopt ethical measures to ensure personal data protection and respect consumers' personal data privacy.





循規行動

當有足夠理由相信有機構的行事方式與《私隱條例》規定不相符時，私隱專員會展開循規審查或調查。在完成循規審查或調查後，私隱專員會書面告知有關機構，指出與《私隱條例》規定不符或不足之處，並促請有關機構採取適當的補救措施，糾正可能違規的情況和採取預防措施。

在報告年度內，私隱專員共進行了307次循規審查，較2017/18年度的272次上升13%。在報告年度內亦主動進行四次循規調查，較2017/18年度的一次上升三倍。

下文重點介紹在年內進行的部分循規行動。

循規調查

未獲授權取覽或查閱一間航空公司約940萬名乘客個人資料

一間航空公司在2018年10月24日代表其本身及其附屬公司（統稱「該航空公司」）就有關其發現約有940萬名乘客的個人資料曾被未獲授權而取覽或查閱一事，向公署作出資料外洩事故通報。該航空公司於2018年3月13日首次在系統中發現可疑活動跡象，因而發現事件。

受影響的資料當事人均屬該航空公司的乘客，當中包括兩個計劃的會員及註冊用戶，來自超過260個國家／法域／地區。涉及的個人資料主要包括受影響乘客的姓名、航班編號及日期、稱謂、電郵地址、會員號碼、地址及電話號碼等。由於事件涉及大量本地及海外人士的敏感個人資料，私隱專員於2018年11月5日就事件展開調查。

COMPLIANCE ACTIONS

The Privacy Commissioner conducts compliance checks or investigations into practices that he has sufficient grounds to consider to be inconsistent with the requirements under the Ordinance. Upon completion of a compliance check or investigation, the Privacy Commissioner alerts an organisation in writing, pointing out the inconsistency or deficiency, and advising the organisation, if necessary, to take remedial actions to correct any breaches and prevent further breaches.

During the reporting year, the Privacy Commissioner carried out 307 compliance checks and four compliance investigations, as compared with 272 compliance checks and one compliance investigation in 2017/18, representing 13% and three-fold increases respectively.

Below are the highlights of some of the compliance actions conducted during the year.

COMPLIANCE INVESTIGATION

Unauthorised access to personal data of approximately 9.4 million passengers of an airline company

On 24 October 2018, an airline company on behalf of itself and its group entities (collectively referred to as Airline) gave a data breach notification to the PCPD in relation to its discovery of unauthorised access to personal data of approximately 9.4 million passengers of the Airline. The incident was discovered when the Airline first detected suspicious activity on its network on 13 March 2018.

The data subjects affected were the Airline's passengers including members of two programmes and registered users from over 260 countries/jurisdictions/locations. The personal data involved consisted mainly of the affected passengers' name, flight number and date, title, email address, membership number, address, phone number, etc. In light of the voluminous and sensitive personal data of local and foreign citizens involved, the Privacy Commissioner initiated an investigation on 5 November 2018.

調查結果

調查發現該航空公司的資料保安，資料保留及資料外洩事故通報的做法存有下列問題：

資料保安

- 未能識辨一個廣為人知及可被加以利用的保安漏洞，亦未能識辨利用該漏洞的行為，同時沒有採取合理地切實可行的步驟在建立一個連接互聯網的伺服器（該伺服器）時進行適當的部署；
- 只為該伺服器每年進行一次漏洞掃描，就有效保障其資訊系統以面對不斷變化的數碼威脅的做法屬流於表面及過份鬆懈；
- 沒有採取合理地切實可行的步驟，避免該伺服器的管理員控制台埠曝露於互聯網，因此導致為攻擊者開啟一個入口；
- 未有對涉及存取其資訊系統內個人資料的所有遙距使用者實施有效的多重身份認證；
- 在沒有採取有效的保安管控措施下，為了方便遷移數據中心而建立未經加密的數據庫備份檔案，因而導致受影響乘客的個人資料曝露予攻擊者；
- 未有建立有效的個人資料庫存以涵蓋所有載有個人資料的系統；及
- 對風險的警覺性低，在2017年的保安事故發生後沒有採取合理地切實可行的步驟，以減低資訊系統被植入惡意軟件及被入侵的風險。

Result of investigation

The investigation revealed the following issues in relation to the data security, data retention and data breach notification practices of the Airline:

Data Security

- Failure to identify the commonly known exploitable vulnerability and the exploitation, and failure to take reasonably practicable steps to accord due deployment of an Internet-facing server;
- Vulnerability scanning exercise for the Internet-facing server at a yearly interval being too lax in the context of effectively protecting its information systems against evolving digital threats;
- Failure to take reasonably practicable steps not to expose the administrator console port of the Internet-facing server to the Internet, as a result of which a gateway for attackers was opened;
- Failure to apply effective multi-factor authentication to all remote access users for accessing its IT system involving personal data;
- Producing unencrypted database backup files to facilitate migration of data centre without adopting effective security controls, thus exposing the personal data of the affected passengers to attackers;
- Failure to have an effective personal data inventory to cover all systems containing personal data; and
- Risk alertness being low and failure to take reasonably practicable steps to reduce the risk of malware infections and intrusions to its IT system after the earlier security incident in 2017.

資料保留

- 沒有採取所有合理地切實可行的步驟，確保受影響乘客的香港身份證號碼的保留時間不超過達致已廢除的核實身份的目的。

資料外洩事故通報

目前《私隱條例》沒有規定資料使用者須向私隱專員及資料當事人通報資料外洩事故，亦沒有規定資料使用者須在指定時間內作出通報。因此，私隱專員認為該航空公司沒有違反《私隱條例》的規定。不過，該航空公司當初應能在2018年3月發現可疑活動時立即通知受影響乘客，並建議他們提前採取適當的步驟，以符合他們的合理期望。

鑑於本案所揭露的事實及所有相關情況，私隱專員認為該航空公司在漏洞管理、採用有效的技術保安措施，以及資料管治方面，沒有採取所有合理地切實可行的步驟，以保障受影響乘客的個人資料免受未獲授權的取覽或查閱，違反了保障資料第4(1)原則(資料保安原則)，及沒有採取所有合理地切實可行的步驟，確保受影響乘客的香港身份證號碼的保留時間不超過達致已廢除的核實身份的目的，違反了保障資料第2(2)原則(資料刪除原則)。

Data Retention

- Failure to take all reasonably practicable steps to ensure that the Hong Kong Identity Card numbers of the affected passengers were not kept longer than was necessary for the fulfilment of the defunct verification purpose for which the data was used.

Data Breach Notification

There being no statutory requirements under the Ordinance for a data breach notification, whether to the Privacy Commissioner or the affected passengers, and whether within a particular period of time or otherwise, the Privacy Commissioner found no contravention of the Ordinance in this connection. Nevertheless, the Airline could have notified the affected passengers of the suspicious activity once detected back in March 2018 and advised them of the appropriate steps to take earlier to meet their legitimate expectation.

In light of the facts revealed and in all the circumstances of the case, the Privacy Commissioner found that the Airline contravened Data Protection Principle 4(1) (Data Security Principle) of Schedule 1 to the Ordinance by failing to protect the affected passengers' personal data against unauthorised access in terms of vulnerability management, adoption of effective technical security measures and data governance, and Data Protection Principle 2(2) (Data Erasure) by failing to take all reasonably practicable steps to ensure that the Hong Kong Identity Card numbers of the affected passengers were not kept longer than was necessary for the fulfilment of the purpose.

執行通知

私隱專員向該航空公司送達執行通知，指示該航空公司：

- 聘請獨立的資料保安專家徹底檢修載有個人資料的系統；
- 為所有會存取載有個人資料的資訊系統的遙距使用者實施有效的多重身份認證，並承諾定期檢視遙距存取的權限；
- 定期在伺服器及／或應用程式層面進行有效的漏洞掃描；
- 聘請獨立的資料保安專家定期對其網絡的保安進行檢視／測試；
- 制定清晰的資料保留政策，訂明每個系統內的乘客資料的保留期限，即不超過將其保存以貫徹該資料被使用於的目的，並承諾實施有效措施以確保政策獲有效執行；及
- 從所有系統徹底銷毀從一個會員計劃所收集的所有不必要的香港身份證號碼。

借鑒

雖然個人資料不像其他動產（例如鈔票）或不動產般屬有形的資產，但那亦不足以免除企業沒有妥善地保護資料及沒有在達致有關目的而不再需要該資料時徹底銷毀資料的責任。顧客（資料當事人）及監管機構合理地期望企業能擁有一個完備、有效及可行、能適切企業的規模與需要、並可全面實施的私隱循規政策和計劃，以落實法例要求。

Enforcement notice

The Privacy Commissioner served an Enforcement Notice to direct the Airline to:

- engage an independent data security expert to overhaul the systems containing personal data;
- implement effective multi-factor authentication to all remote users for accessing its IT system involving personal data and undertake to conduct regular review of remote access privileges;
- conduct effective vulnerability scans at server and application levels;
- engage an independent data security expert to conduct reviews/tests of the security of the Airline’s network;
- devise a clear data retention policy to specify the retention period(s) of passengers’ data, which is no longer than is necessary for the fulfilment of the purpose, and undertake to implement effective measures to ensure effective execution; and
- completely obliterate all unnecessary Hong Kong Identity Card numbers collected from one of its membership programmes from all systems.

Lesson learnt

The fact that personal data is less tangible than other personalty (e.g. bank notes) or realty does not absolve businesses of their failures to keep it safely and to obliterate it when it is no longer necessary for the fulfilment of the purpose for which the data is or is to be used. To give effect to the legal requirements, there is an expectation of comprehensive, effective and evidenced privacy compliance policies and programmes being put in place, relevant and scalable for the businesses concerned, as well as demonstrable internally and externally. This legitimate expectation comes from both the customers, who are the data subjects, and the regulators.

循規調查

電訊商載有38萬名客戶及服務申請者個人資料的客戶資料庫遭入侵事件

2018年4月16日，一間電訊商發現一個已停用的資料庫遭未經授權入侵，導致近38萬名客戶及服務申請者的個人資料外洩。儲存在涉事資料庫內的個人資料包括姓名、電郵地址、通訊地址、電話號碼、身份證號碼和選擇以信用卡付款的人士的信用卡資料(例如持卡人姓名、信用卡號碼和到期日)。由於涉及大量及敏感的個人資料，私隱專員就事件展開調查[1]。

調查結果

事發時，該電訊商將客戶資料儲存在三個資料庫內。遭黑客入侵的資料庫是一個已停用的資料庫，儲存截至2012年的客戶和服務申請者的個人資料。調查發現：

- 涉事資料庫本應在2012年完成系統遷移後被刪除，卻因人為疏忽而被保留下來，並繼續連接內部網絡，該電訊商遺忘了涉事資料庫的存在；

- 該電訊商在系統遷移後沒有作全面及審慎的檢查，以致未有適時刪除涉事資料庫；

[1] 調查報告於2019年2月21日發表。

COMPLIANCE INVESTIGATION

Intrusion into a telecommunications company's customer database containing personal data of 380,000 customers and service applicants

On 16 April 2018, a telecommunications company uncovered unauthorised access to its inactive customer database, which caused leakage of personal data of nearly 380,000 customers and service applicants. The types of personal data contained in the database in question included name, email address, correspondence address, telephone number, Hong Kong Identity Card number and credit card information such as the name of cardholder, credit card number and date of expiry (if the customers opted for credit card payment). In light of the voluminous and sensitive personal data involved, the Privacy Commissioner initiated an investigation[1].

Result of investigation

At the time of the incident, the telecommunications company stored customers' data in three databases. The database in question was inactive, containing personal data of customers and service applicants as of 2012. The investigation found that:

- The database in question should have been deleted after a system migration in 2012, but was nevertheless retained and remained connected to internal network owing to human oversight. Its existence escaped the memory and attention of the telecommunications company;

- The telecommunications company failed to conduct a comprehensive and prudent review after system migration, leading to the failure to delete the database in question;

[1] The investigation report was published on 21 February 2019.

- 該電訊商在事發前沒有仔細考量舊客戶個人資料的保留期限和制定資料保留的內部指引，以及保留舊客戶的資料時間過長；

- 涉事資料庫的保安措施不足，沒有更新修補程式及將資料作加密處理；及

- 該電訊商未能充分掌握其資訊科技設備和保安措施的實施情況。

基於調查中所得和該電訊商所承認的事實，以及本個案的所有情況，私隱專員認為該電訊商(i)沒有採取所有切實可行的步驟刪除已不再需要的資料庫，加上保留舊客戶的個人資料時間過長，因而違反《私隱條例》第26條（資料刪除）和《私隱條例》附表1的保障資料第2(2)原則（資料保留）；和(ii)沒有採取所有切實可行的步驟以確保涉事資料庫內的個人資料受保障而不受未獲准許的查閱，因而違反《私隱條例》附表1的保障資料第4(1)原則（資料保安）。

- The telecommunications company failed to give due consideration to the retention period of former customers' personal data or provide relevant internal guidance. It also retained, for an excessive period of time, data of former customers;

- The safeguards for the database in question had been insufficient. No updating of security patches or encryption was carried out with that database; and

- The telecommunications company failed to exercise control over its IT and security facilities.

In light of the facts revealed and admitted by the telecommunications company in the investigation, and in all the circumstances of the case, the Privacy Commissioner found that the telecommunications company contravened (i) section 26 of the Ordinance (Data Erasure) and Data Protection Principle 2(2) of Schedule 1 to the Ordinance (Data Retention) by failing to take all practicable steps to erase personal data stored in the database in question, where it was no longer needed, and retained personal data of former customers for an excessive period of time, and (ii) Data Protection Principle 4(1) (Data Security Principle) by failing to take all practicable steps to ensure that personal data held in the database in question was protected against unauthorised access.

執行通知

私隱專員向該電訊商送達執行通知，並指令其：

- 制定清晰的程序，訂明系統遷移後刪除不再需要的資料庫內的個人資料的步驟、時限和監察措施；
- 制定清晰的資料保留政策，訂明客戶及服務申請者個人資料的保留期限，不得超過將其保存以貫徹該資料被使用於或會被使用於的目的所需的時間；
- 制定清晰的資料保安政策，訂明定期檢視用戶權限及遠程接達服務的保安措施；
- 實施有效的措施，確保有關員工知悉和執行上述項目所訂的政策及程序；及
- 根據上述所訂的資料保留政策，刪除所有超過保留期限的客戶及服務申請者的個人資料。

借鑑

此個案源於黑客入侵一間電訊商的網絡及從一個已停用的資料庫中下載客戶資料。如該電訊商在系統遷移後已適時妥善刪除資料庫，事件對客戶造成的損害本可避免。公署自 2014 年起提倡私隱管理系統，其中一項系統管理措施是個人資料庫存。按時更新的個人資料庫存可讓機構清楚了解所持有的個人資料種類、儲存資料的地點及保留期限等。私隱專員因此建議機構（尤其是儲存大量個人資料的機構）慎重檢視資料庫存和保留期限，以免成為黑客入侵的受害者。

Enforcement notice

The Privacy Commissioner served an enforcement notice on the telecommunications company directing it to:

- devise clear procedures to specify the steps, time limits and monitoring measures for deleting personal data in obsolete database(s) after system migration;
- devise a clear data retention policy to specify the retention period(s) of personal data of customers and service applicants, which is no longer than is necessary for the fulfillment of the purpose;
- devise a clear data security policy to cover regular review of user privileges and security controls of remote access service;
- implement effective measures to ensure that the policies and procedures would be expressly informed to relevant staff members and effectively executed; and
- erase all the personal data of customers and service applicants which is retained longer than the retention period(s) as specified in the data retention policy devised.

Lesson learnt

This case originated from a hacking incident where a hacker infiltrated a telecommunications company's network and downloaded customers' data from a database that was no longer in use. Damage to customers could have been avoided if the database had been deleted by the company after system migration in a considered and timely manner. An updated personal data inventory, which is one of the programme controls of privacy management programme advocated by the Privacy Commissioner since 2014, will provide an organisation with a clearer picture of the kinds of personal data it holds, the location of data storage, the respective retention period, etc. The Privacy Commissioner recommends organisations, particularly those storing an enormous amount of personal data, to critically review their data inventories and retention periods, to prevent from falling prey to cyberattacks.

循規審查

商場會員計劃及網上推廣活動的個人資料收集

為了解香港商場營運商收集個人資料的情況，同時因應公眾對網上推廣活動收集個人資料的行為的關注，公署於2018年共巡視100 間商場和審視300 個要求提供個人資料以換取優惠的網頁，並對有設立會員計劃的41 間商場及表面看來有過度收集個人資料的19 間網頁營運商，展開循規審查[1]。

商場會員計劃

公署向商場展開的循規審查結果顯示，31個會員計劃（佔巡視期間發現的52個會員計劃[2]之中的60%）收集個人資料（包括聯絡方法、敏感個人資料和個人及家庭狀況相關的資料）時抱有「寧濫勿缺」的心態，有違《私隱條例》下不過度收集資料的原則和收集最少資料的行事方式。

結果亦顯示：

- 部分商場會員計劃收集的個人資料，除了基本的聯絡資料（如姓名、電話、地址和電郵地址）外，亦包括較敏感的個人資料（如生日資料、年齡、香港身份證號碼），以至個人及家庭狀況（如每月收入、婚姻狀況、是否車主，及車牌號碼等）；
- 有三個會員計劃（佔52 個會員計劃之中的6%）收集18 項個人資料；
- 有20 個會員計劃（佔52 個會員計劃之中的38%）要求會員強制提供不必要的個人資料；及
- 有八個會員計劃（佔52 個會員計劃之中的15%）在設計上強迫顧客同意有關機構可使用其個人資料作直接促銷用途，而顧客就此沒有其他選擇。

[1] 循規審查報告於2019 年4 月25 日發表。

[2] 41 間商場合共設有52 個會員計劃。

COMPLIANCE CHECK

Personal Data Collection in Shopping Mall Membership Programmes and Online Promotion Activities

In order to understand the collection of personal data by shopping mall operators in Hong Kong, and in response to the concerns about personal data collection during online promotion activities, PCPD visited 100 shopping malls and reviewed 300 webpages requesting personal data in exchange for benefits in 2018, and subsequently initiated compliance checks[1] against 41 shopping malls that had membership programmes and 19 website operators that appeared to have excessive collection of personal data.

Shopping mall membership programmes

The results of the compliance checks on shopping malls revealed that 31 membership programmes (60% of a total of 52[2] membership programmes found in the site visits) adopted a "the more the merrier" approach when collecting personal data including contact information, sensitive personal data and information relating to personal and family status, contrary to the no excessive data collection principle under the Ordinance and the practice of collecting minimum information for the purpose of data collection.

The results also showed that:

- Apart from collecting basic contact information (e.g. name, telephone number, address and email address), some shopping mall membership programmes also collected sensitive personal data (e.g. date of birth, age, Hong Kong Identity Card number) and personal data relating to personal and family status (e.g. monthly income, marital status, whether a car owner or not and vehicle registration mark);
- Three membership programmes (6% of the 52 membership programmes) required collection of 18 personal data items;
- 20 membership programmes (38% of the 52 membership programmes) required compulsory provision of unnecessary personal data; and
- The design of eight membership programmes (15% of the 52 membership programmes) forced customers to agree that the relevant organisations could use their personal data for direct marketing purposes, leaving individual customers with no choice at all.

[1] The compliance checks report was published on 25 April 2019.

[2] These 52 membership programmes were hosted by the 41 shopping malls.

在上述「綑綁式同意」的做法及設計下所獲取的同意，不能視為真正和有意義的同意。其做法及設計實際上構成不公平收集個人資料，因此應予以停止，而有關商場亦已作出相應更改。

就商場會員計劃所收集的個人資料方面，一般而言，私隱專員接受為識辨身份和通訊目的而收集聯絡資料。然而，會員計劃收集香港身份證號碼一般會被視為過度收集個人資料，因為香港身份證號碼屬敏感的個人資料，處理不當會造成如身份盜竊等不必要的風險。至於為市場分析及提供合適優惠的目的而收集個人及家庭狀況有關的個人資料，一般而言可以接受，但同時會員應有不提供這些資料的選擇。

就身份證號碼與個人及家庭狀況的個人資料方面，私隱專員欣悉在巡視的52個會員計劃之中：

- 45 個（佔52 個會員計劃之中的87%）未有收集會員的香港身份證號碼；及
- 32 個（佔52 個會員計劃之中的62%）給予會員可不提供部份個人資訊（如年齡、工作地區、職業等）及家庭狀況的選項，或完全沒有要求這些資料。

網上推廣活動

在網上推廣活動方面，是次循規審查行動的結果顯示：

- 相比其他行業，美容、教育、保健產品及服務業較多利用網上推廣活動，分別佔是次審查的300個網頁之中的44%、18%和8%；及
- 由於網上推廣活動的目的只為吸引顧客領取推廣優惠，只有20個網上推廣活動（佔300 個網頁之中的6%）涉及過度收集個人資料，包括香港身份證號碼、生日資料、年齡及每月收入。

補救措施

有關商場和網頁營運商已跟從公署的意見停止收集被視為超乎適度的個人資料，銷毀所有在以往收集的有關資料，並重新修訂申請表格及《收集個人資料聲明》以符合《私隱條例》中收集資料方面的要求。

The said "bundled consent" design and practice obtained no meaningful and real consent, and practically constituted unfair collection of personal data. Such practice therefore should be discontinued, and the malls concerned had rectified the situation accordingly.

With regard to personal data collected by shopping mall membership programmes, in general, the Privacy Commissioner accepts the collection of contact information for the purposes of identification and communication. However, the collection of HKID Card number by membership programmes is generally considered excessive because HKID Card number is sensitive in nature, and improper processing of this data may cause unnecessary risks such as identity theft, etc. Meanwhile, collection of personal data relating to personal and family status is generally acceptable for the purposes of market analyses and provision of suitable offers, but members should be given a choice of not providing such information.

Concerning the personal data related to HKID Card number as well as personal and family information, the Privacy Commissioner was pleased to note that:

- 45 membership programmes (87% of the 52 membership programmes) did not collect HKID Card number; and
- 32 membership programmes (62% of the 52 membership programmes) either provided members with an option not to provide certain personal information (such as age, working district, occupation, etc.) and family status or did not request such information at all.

Online promotion activities

For online promotion activities, the results of the compliance checks revealed that:

- Beauty, education institutions as well as health products and services industry used more online promotion activities than other industries did, accounting for 44%, 18% and 8% of the 300 webpages reviewed respectively; and
- Given that the purpose was simply to attract customers for promotional offers, only 20 online promotion activities (6% of the 300 webpages) involved excessive collection of personal data, such as HKID Card number, date of birth, age and monthly income.

Remedial actions

With the PCPD's advice, the shopping malls and website operators in question had ceased to collect personal data that was considered excessive, destroyed all such data collected previously, and revised the application forms and Personal Information Collection Statement to comply with the data collection requirements under the Ordinance.

借鑑

隨著大數據和資訊及通訊科技的發展及應用日增，衍生的網絡安全風險已上升至前所未見的高水平並日趨嚴重。收集的個人資料越多，相關的風險越大。私隱專員支持及提倡在不損害個人私隱權的情況下，合法運用大數據，並極力建議以收集最少個人資料的方式行事。

機構亦應將個人資料保障納入為其企業管治責任的一部分，並由董事局開始，以應用私隱管理系統於整個機構中為業務重點。私隱專員進一步建議機構應將數據管治和管理以至數據道德-尊重、互惠和公平，納入機構管治之中，方為長遠應對個人資料私隱保障的方案。

Lesson learnt

With the development and increasing application of big data, and information and communications technology, the resulting network security risks have elevated to an unprecedented high level and will only become more serious over time. The more personal data collected, the greater the risk associated. The Privacy Commissioner advocates and facilitates the legitimate use of big data without compromising individuals' privacy right, and highly recommends the practice of minimum collection of personal data.

Organisations should also embrace personal data protection as part of their corporate governance responsibilities and apply the programme as a business imperative throughout the organisation, starting from the boardroom. The Privacy Commissioner further recommends that organisations should incorporate data governance, stewardship and ethics – being respectful, beneficial and fair, as part of corporate governance and a long term solution for personal data protection.

循規審查

未經授權在社交媒體網絡中發放載有個人資料的機密文件

某政府部門向公署通報，表示其員工未經授權上傳了一份便箋至WhatsApp群組，當中載有138名即將參加內部考試的人員的姓名、職員編號、職級、職位、駐守單位和考試日期。

本案源於負責員工在收到便箋後，留意到所有即將參加考試的人員都已下班。由於她被要求通知有關人員其考試日期以便為考試作準備，她便輯錄了便箋的相關影像並將圖像發放給WhatsApp群組的成員，以防止不必要的延誤。在收到圖像後，WhatsApp群組中的一名成員進一步將圖像轉發給另一個由他的小隊成員組成的WhatsApp群組。

為了防止同類事件重演，該部門傳閱電子備忘錄，提醒員工須注意安全使用社交媒體網絡及正確處理個人資料和機密文件。同時，該部門亦透過引用此事件為例子，透過備忘錄向相關員工簡述遵守電子備忘錄的重要性，並提供持續培訓，以提高員工對保障個人資料隱私的意識。

借鑑

案中那類的即時通訊程式為通訊帶來便利。但如果使用不當，可能會對個人資料私隱產生不利影響。本案中負責的人員顯然沒有充分考慮到關於使用社交媒體網絡正確處理載有個人資料的機密文件的內部程序，有關行為可無意中導致個人資料外洩。這類行為應可避免。

COMPLIANCE CHECK

Unauthorised circulation of confidential documents containing personal data in social media network

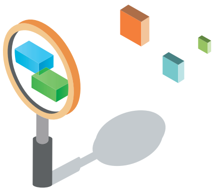
A government department reported to the PCPD that a staff member had uploaded a memo containing the names, service numbers, ranks, posting, stationed units and examination dates of 138 service members who would sit for an internal examination in a WhatsApp group without authorisation.

This case originated from the staff member concerned, who noted that all those service members who would sit for the examination were off duty when she received the memo. As she had been requested to disseminate the respective examination dates to the members concerned for preparation of examination, she captured the relevant pages of the memo and shared the image to the members involved in the WhatsApp group to prevent unnecessary delay. Upon receipt of the images, one member in the WhatsApp group further forwarded the image to another WhatsApp group comprising his squad members.

To prevent recurrence of similar incidents, the department circulated e-memos to remind its service members to observe the safe use of social media networks and the proper handling of personal data and confidential documents. The department also enhanced staff awareness of personal data privacy protection by issuing another memo citing this incident as an example, briefing the relevant staff members on the importance of compliance with the e-memos, providing ongoing training to all members concerned, etc.

Lesson learnt

Instant messaging applications like that in this case enhance convenience for communication. If used improperly, however, it may create adverse effects on the privacy of individuals in relation to personal data. The staff concerned in this case had obviously failed to give due consideration to the established protocols on the proper handling of confidential documents containing personal data when using social media networks. Such act could result in inadvertent disclosure of personal data which should be avoided.



招聘網站錯誤將載有工作履歷資料的電郵寄出

公署接獲某招聘網站通報，指他們錯誤將載有4,201名求職者履歷資料的電郵寄予1,692間公司。被洩漏的個人資料包括中英文姓名、居住地址、手提電話號碼、電郵地址、性別、出生日期、國籍、身份證號碼、婚姻狀況、教育背景及工作經驗。得悉事件後，公署決定展開循規審查。

在循規審查的過程中，公署發現該公司的伺務器因錯誤配置關係，導致有人手重寄過程的需要，而負責整理該人手重寄過程的職員犯下人為失誤，最終令致資料外洩。

事發後，該公司成立跨部門工作小組，以評估是次事故帶來的影響、解決問題、及與內外持份者溝通。為免同類事情再發生，該公司將採用全自動程序以及引入核對機制，以避免日後再需要人手操作。

借鑑

就算高度機械主導的系統也偶爾需要人手介入，而發生錯誤的機會也會因此而增加，所以公署欣悉有關的資料使用者遷移至全自動程序。儘管如此，一定程度的核對機制能確保個人資料私隱得到更佳的保障。

Recruitment platform wrongfully sent out emails containing CV information

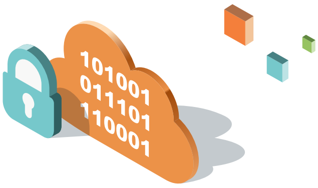
A recruitment platform reported to the PCPD that job application emails containing CVs of 4,201 job applicants were erroneously sent to 1,692 companies. Personal data involved included job applicants' full English and Chinese names, home addresses, mobile numbers, email addresses, genders, dates of birth, nationalities, identity card numbers, marital statuses, education background and work experience. On knowing the incident, the PCPD initiated a compliance check.

In the compliance check process, the PCPD revealed that the incident occurred when a server misconfiguration prompted a manual job application resending process, and a human sorting error caused the data mismatch and job applications being sent incorrectly to the companies.

After the incident, the recruitment platform formed a cross-functional task force to access impact, resolve the issue, and communicate with external and internal stakeholders. To remove the risk of data mismatch in the future, a fully automated process which eliminates the need for manual interaction with datasets was implemented in addition to a checking mechanism to ensure that job application emails will not be sent out to irrelevant companies.

Lesson learnt

Even systems which are predominantly machine-operated may at times require human intervention (such as server misconfiguration in this case). Human interaction is prone to errors. So, completely automated processes are mostly welcomed, albeit some form of auditing mechanism would still be beneficial.



視察行動

視察原因

本港私營補習服務業持續興旺，服務種類繁多；補習服務機構需要處理龐大數量的個人資料，加上其服務對象主要為學童，此群組人士的個人資料私隱尤其需要受到特別的保障，私隱專員遂根據《私隱條例》第36條，對三所不同營商模式（連鎖式、特許經營、網上平台）的補習服務機構的個人資料系統進行視察，就業界處理個人資料方面作出建議，藉以加強它們依從《私隱條例》的認知。

視察結果及建議

視察結果顯示三所補習服務機構在處理個人資料方面皆存有不同的理念及認知，導致它們的個人資料系統在不同範疇各有長短。整體而言，私隱專員滿意三所機構均視學童、家長及導師的個人資料為重要資產，不會胡亂處理或濫用個人資料，亦致力確保該等資料得到妥善管理。它們在營運過程及常規中均有採取保障個人資料的措施，但相關措施只在個別職能中體現，未能將私隱保障納入其企業管理中。

私隱專員指出，機構最佳的行事方式是建立及全面執行私隱管理系統。數據管治應涵蓋整體業務常規、操作程序、產品和服務設計、實體建築，以至網絡基礎設施。在策略層面，機構可採用私隱管理系統作為框架，輔以行之有效的檢討及監察程序，建立健全的私隱保障基建，藉以配合機構遵從《私隱條例》的規定，與顧客共享公平、尊重和互惠。

INSPECTION

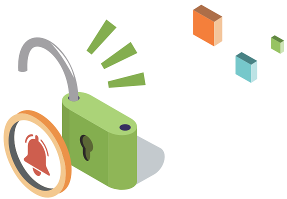
Reasons for inspection

The private tutorial services industry in Hong Kong continues to thrive and provides a wide range of services. Tutorial institutions need to handle a vast amount of personal data. Since the main target clients are minors, being an age group that should be given special protection of personal data privacy, the Privacy Commissioner conducted an inspection of the personal data systems of three private tutorial institutions (the Institutions) with different business models (chain-run, franchised, and online) pursuant to section 36 of the Ordinance. Through the inspection exercise, the Privacy Commissioner made recommendations to this class of data users in relation to the handling of personal data so as to promote compliance with the provisions of the Ordinance.

Findings and recommendations

The inspection showed that the institutions had different understanding and perceptions about personal data handling, resulting in different strengths and weaknesses of their personal data systems. On the whole, the Privacy Commissioner was satisfied that the Institutions viewed the personal data of children, parents and tutors as important assets and they would not handle or use the data indiscriminately. The Institutions were also committed to ensuring that the data was properly managed. They had taken measures to protect personal data in their operational procedures and practices. However, only fragmented measures were in place and data privacy protection was not included as part of their corporate governance.

The Privacy Commissioner considered that, as a best practice, organisations should formulate and maintain a comprehensive privacy management programme (PMP). Data stewardship should cover the overall business practices, operational processes, product and service design, physical architecture and network infrastructure. The PMP, supported by an effective ongoing review and monitoring process to facilitate its compliance with the requirements under the Ordinance, serves as a strategic framework to assist the organsations in building a robust privacy infrastructure and to share mutual fairness, respect and benefit with their customers.



參照全面的私隱管理系統的要求，以及按《私隱條例》的有關的規定，私隱專員對私營補習市場的機構提出以下建議：

- 將私隱保障納入企業管治，並從管理層中委任保障資料主任管理相關事務；
- 將私隱保障納入新產品及服務設計之中，並就個人資料私隱進行評估；
- 制定全面的私隱政策，並須適時通知所有僱員有關規定；
- 建立有效的個人資料匯報及監控系統和資料外洩事故通報機制；
- 定期提供教育及培訓予所有員工以提高其對私隱保障的意識；
- 檢視其收集個人資料的情況，停止不必要或過量收集個人資料；
- 訂立保留個人資料期限的政策，以及銷毀已超過保留期限的資料的程序及方式；
- 就使用個人資料情況進行全面檢視，確保其使用目的與當初收集資料的目的一致或直接有關，或已獲取資料當事人的訂明同意；
- 制定全面的資訊保安政策（包括資訊科技系統及實體保安措施）；
- 以合約方式規範資料處理者在處理其委託的個人資料的情況，並需定期進行監控及審查程序，確保符合有關私隱保障的要求；及
- 恪守更高的數據道德標準，在實際營運上符合持份者的期望。

Based on the elements of the PMP and the related requirements under the Ordinance, the Privacy Commissioner made the following recommendations to institutions in the industry:

- Integrate the ideas of data privacy protection into corporate governance, and to designate a data protection officer from top management to oversee data protection matters;
- Incorporate privacy protection when designing new products and services, and assess the relevant impact on personal data privacy;
- Formulate a comprehensive privacy policy, and inform all staff members about the related measures;
- Establish effective personal data reporting and monitoring mechanism, as well as data breach notification mechanism;
- Provide regular education and training to all employees in order to raise their awareness of privacy protection;
- Review personal data collection practices, and cease excessive or unnecessary data collection;
- Establish personal data retention policies as well as the procedures and methods for destroying such data;
- Conduct a comprehensive review on the use of personal data to ensure that such use is consistent with or directly related to the purpose for which the data was originally collected, or has obtained prescribed consent from the data subject concerned;
- Develop a comprehensive information security policy (covering information technology systems and physical security measures);
- Adopt contractual means to manage the personal data entrusted to data processors, and conduct regular monitoring and compliance procedures to ensure data processors' compliance with the requirements of privacy protection; and
- To be held to a higher data ethical standard that meets stakeholders' expectation in actual operation.

資料外洩通報

資料外洩事故一般是指資料使用者所持有的個人資料保安不足，以致洩露資料，令資料可能被人未經授權或意外地查閱、處理、刪除、喪失或使用。資料外洩事故可能構成違反保障資料第4原則。雖然《私隱條例》並未有規定資料使用者就資料外洩事故作出通報，但為符合數據道德標準，公署一直鼓勵資料使用者一旦發生資料外洩事故，須通知受影響的資料當事人、私隱專員和其他相關人士。

公署在接獲資料外洩事故通報（可用公署的指定表格或其他方式呈報）後，會評估有關資料，以考慮是否有需要對有關機構展開循規審查。私隱專員對相關資料使用者進行循規審查後，會書面指出明顯的不足之處，並建議他們採取補救措施，防止同類事故重演。

在報告年度內，公署接獲113宗資料外洩事故通報（61宗來自公營機構；52宗來自私營機構），與上一報告年度的116宗相約，牽涉349,545,512名人士的個人資料。這些外洩事故涉及黑客入侵、系統設定有誤、遺失文件或便攜式裝置、經傳真、電郵或郵遞意外披露個人資料等。公署對所有肇事機構均展開循規審查行動。

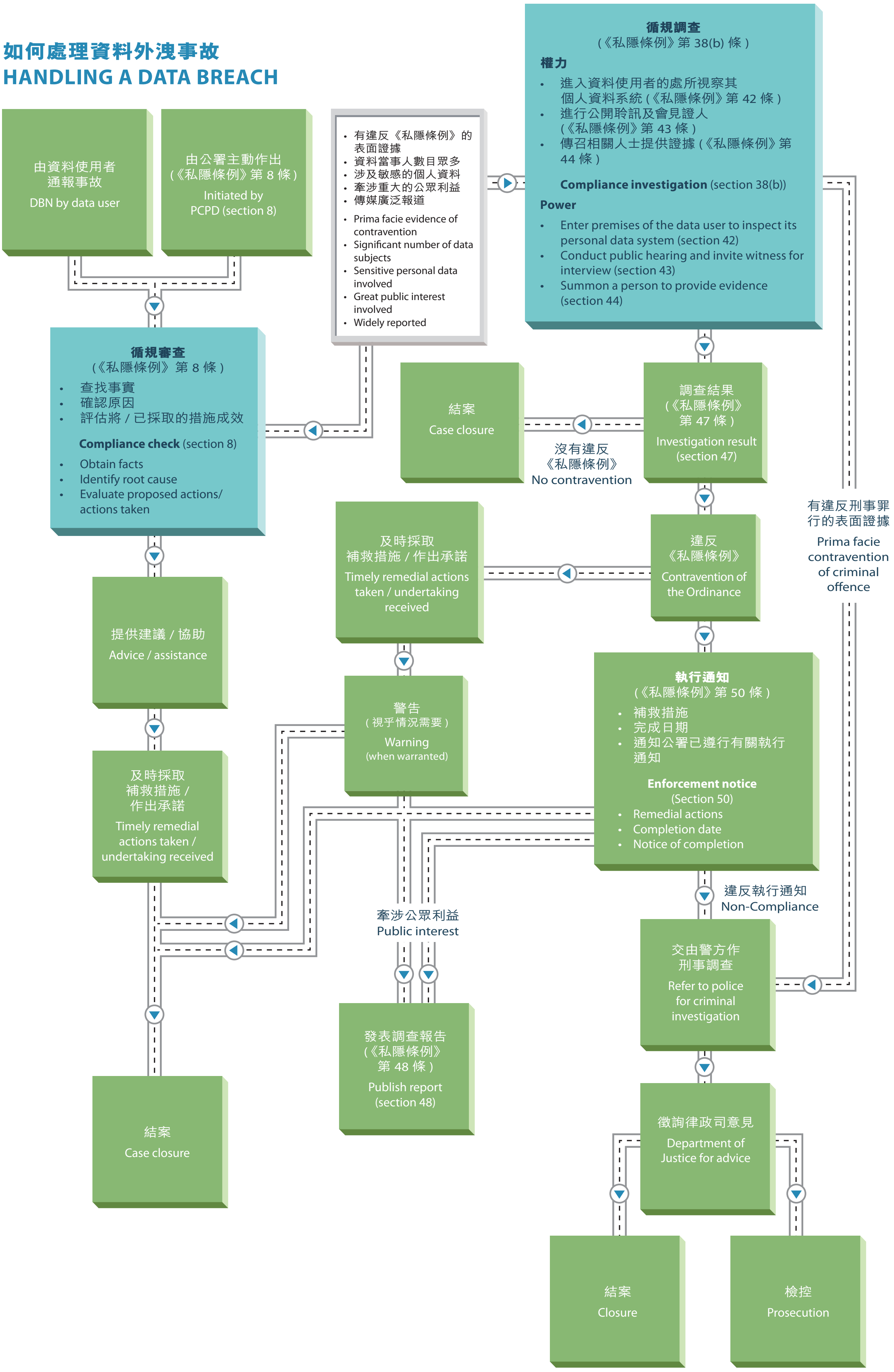
DATA BREACH NOTIFICATIONS

Generally speaking, a data breach is a breach of security of personal data held by a data user, which results in exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. The breach may amount to a contravention of Data Protection Principle 4. Although the Ordinance does not require data users to give data breach notification (DBN), the PCPD has always encouraged data users, in line of data ethical standards, to give such notification to the affected data subjects, the Privacy Commissioner, and other relevant parties when a data breach has occurred.

Upon receipt of a DBN from a data user (which could be submitted through the PCPD-designated DBN form or other means of communication), the PCPD would assess the information provided in the DBN and decide whether a compliance check is warranted. Upon completion of a compliance check, the Privacy Commissioner would point out the obvious deficiency and suggest the data user to take remedial actions to prevent recurrence of the incident.

During the reporting year, the PCPD received 113 DBNs (61 from the public sector and 52 from the private sector), which is comparable to 116 DBNs received in the preceding year, and involved personal data of 349,545,512 individuals. The data breach incidents involved hacking, system misconfiguration, the loss of documents or portable devices, inadvertent disclosure of personal data by fax, email or post, etc. The PCPD conducted compliance check in each of these 113 incidents.

如何處理資料外洩事故
HANDLING A DATA BREACH



由資料使用者通報事故

DBN by data user

由公署主動作出（《私隱條例》第 8 條）

Initiated by PCPD (section 8)

循規審查（《私隱條例》第 8 條）

- 查找事實
- 確認原因
- 評估將 / 已採取的措施成效

Compliance check (section 8)

- Obtain facts
- Identify root cause
- Evaluate proposed actions/ actions taken

- 有違反《私隱條例》的表面證據
- 資料當事人數目眾多
- 涉及敏感的個人資料
- 牽涉重大的公眾利益
- 傳媒廣泛報道

- Prima facie evidence of contravention
- Significant number of data subjects
- Sensitive personal data involved
- Great public interest involved
- Widely reported

循規調查（《私隱條例》第 38(b) 條）

權力

- 進入資料使用者的處所視察其個人資料系統（《私隱條例》第 42 條）
- 進行公開聆訊及會見證人（《私隱條例》第 43 條）
- 傳召相關人士提供證據（《私隱條例》第 44 條）

Compliance investigation (section 38(b))

Power

- Enter premises of the data user to inspect its personal data system (section 42)
- Conduct public hearing and invite witness for interview (section 43)
- Summon a person to provide evidence (section 44)

提供建議 / 協助

Advice / assistance

及時採取補救措施 / 作出承諾

Timely remedial actions taken / undertaking received

結案

Case closure

調查結果（《私隱條例》第 47 條）

Investigation result (section 47)

沒有違反《私隱條例》

No contravention

結案

Case closure

違反《私隱條例》

Contravention of the Ordinance

及時採取補救措施 / 作出承諾

Timely remedial actions taken / undertaking received

警告（視乎情況需要）

Warning (when warranted)

執行通知（《私隱條例》第 50 條）

- 補救措施
- 完成日期
- 通知公署已遵行有關執行通知

Enforcement notice (Section 50)

- Remedial actions
- Completion date
- Notice of completion

牽涉公眾利益

Public interest

發表調查報告（《私隱條例》第 48 條）

Publish report (section 48)

有違反刑事罪行的表面證據

Prima facie contravention of criminal offence

違反執行通知

Non-Compliance

交由警方作刑事調查

Refer to police for criminal investigation

徵詢律政司意見

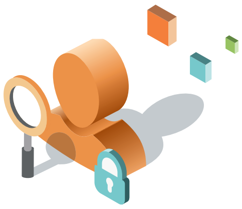
Department of Justice for advice

結案

Closure

檢控

Prosecution



2018年抽查報告：資料使用者實施私隱管理系統的情況

在2018年，香港個人資料私隱專員公署（公署）連續第六年參與「全球私隱執法機關網絡」(Global Privacy Enforcement Network)的抽查行動。本年抽查行動的主題是「私隱問責制的實施」。18個來自世界各地的私隱執法機關（包括公署）參與了抽查行動，當中主要透過分析機構實施私隱管理系統的情況，以評估機構在保障個人資料方面達致問責的程度，及他們在業務過程中管理私隱風險的能力。

公署於2018年10月至11月期間向26間不同行業的機構（包括保險、金融、電訊、公用事業及交通運輸）進行抽查行動，以了解它們實施私隱管理系統的情況。

全球方面，私隱執法機關共聯絡了356間不同行業的機構參加抽查行動，包括（但不限於）教育、電子商務、金融及保險、健康護理、法律、市場推廣、公共事業（包括中央及地區政府）、零售、電訊、旅遊、交通及康樂。

主要觀察結果

公署在香港的抽查結果大致與全球抽查結果一致。公署在抽查行動所得的主要觀察結果簡述如下：

1. 所有參加機構均有制訂符合法律要求的內部個人資料私隱政策，並將有關政策納入機構日常運作中。
2. 儘管並非《私隱條例》的規定，大部分參加機構已委任高級人員負責私隱管治和管理的事宜。
3. 大部分機構均向員工提供全面的保障個人資料培訓。
4. 所有參加機構均將其私隱政策上載於機構的網站中，並易於查閱。

PRIVACY SWEEP 2018 – IMPLEMENTATION OF PRIVACY MANAGEMENT PROGRAMME BY DATA USERS

The PCPD participated in the Privacy Sweep of the Global Privacy Enforcement Network (GPEN) for the sixth consecutive year in 2018. The theme of the global Privacy Sweep 2018 was “Privacy Accountability”. 18 privacy enforcement authorities from around the world, including the PCPD, participated in the Privacy Sweep to assess how well organisations have implemented accountability principle through Privacy Management Programme (PMP) and their ability to manage privacy risks in all business processes.

During the Sweep period between October and November 2018, the PCPD examined 26 organisations from different sectors (including insurance, finance, telecommunications, public utilities and transportation) to understand their implementation of PMP within their organisations.

Globally, the privacy enforcement authorities made contact with a total of 356 organisations from various sectors including (but not limited to) education, electronic commerce, finance and insurance, health industry, legal, marketing, public sector (including central and local governments), retail, telecommunications, tourism, transport and leisure.

Key observations

The PCPD’s observations about the local situation were largely in line with the global ones. The key observations of the PCPD are summarised below:

1. All participating organisations had internal data privacy policy (in compliance with legal requirements) and this had been embedded into everyday practices.
2. Although not a legal requirement under the Ordinance, majority of the participating organisations had appointed sufficiently senior level staff for handling privacy governance and management matters.
3. Majority of the participating organisations provided comprehensive training on personal data protection to their staff.
4. All participating organisations maintained privacy policies easily accessible on their websites.

5. 幾乎所有參加機構有書面制訂資料外洩事故的處理程序。

6. 只有部分參加機構有就發生資料外洩事故時通知受影響的資料當事人及向監管機構匯報方面制訂相關程序。

7. 絕大部分參加機構在計劃推出新項目、產品或服務前，會進行私隱影響評估，並有書面記錄。

8. 部分參加機構備有完整的個人資料庫存。

9. 部分參加機構有就轉移個人資料給第三方備存完整記錄。

建議

公署對機構在推行私隱管理系統方面有以下建議，藉以遵從《私隱條例》的規定的同時，亦能與客戶及員工共享公平、尊重和互惠：

1. **提供足夠的保障資料培訓：**確保員工了解《私隱條例》的規定及遵守有關保障個人資料的政策。如機構處理個人資料的政策或《私隱條例》有修訂，機構應立即通知員工。

2. **定期進行審核：**定期審核機構處理個人資料的做法是否符合《私隱條例》的規定，以及是否有優化的空間。

3. **資料外洩事故的處理：**制訂書面程序，述明發生資料外洩事故時通知受影響的個人及向監管機構匯報所需考慮的因素、機制及行事方式。

4. **完整的個人資料庫存：**各部門應擬備部門所屬的個人資料庫存，就轄下載有個人資料的系統作記錄。

5. **轉移個人資料的記錄：**對所轉移的個人資料備存記錄。日後如有需要，便可迅速地翻查有關資料。

5. Almost all participating organisations maintained a documented incident response procedure.

6. Only some of the participating organisations had a procedure in place to notify affected individuals and report the breach to the regulator.

7. Majority of the participating organisations conducted and documented Privacy Impact Assessment (PIA) before introducing a new product or service.

8. Some of the participating organisations maintained a comprehensive personal data inventory.

9. Some of the participating organisations maintained a record of data transfer to third parties.

Recommendations

To assist organisations in complying with the requirements of the Ordinance and enjoying fairness, respect and benefit with their customers and employees, the PCPD had the following recommendations to organisations in implementation of PMP:

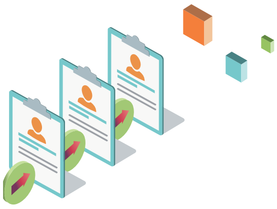
1. **Provide adequate data protection training:** organisations should ensure that their staff members understand the requirements under the Ordinance and to observe the organisation's policy in relation to personal data handling. If amendments are made to the organisation's policy in relation to personal data handling or the Ordinance, the organisation should notify its staff immediately.

2. **Conduct regular audit:** Conduct regular audit to ensure that the policies and practices of the organisations are in compliance with the Ordinance and to identify whether there is room for improvement.

3. **Handling of data breach incident:** Devise written procedures in relation to the factors to be considered, mechanism and practices when assessing whether data breach notification should be given to affected individuals and regulatory bodies.

4. **Maintain a comprehensive personal data inventory:** Each department of an organisation should prepare its own inventory of personal data held.

5. **Maintain a record of data flow:** Recording data flow can facilitate organisations to easily check and retrieve relevant information in future when necessary.



個人資料的核對程序

核對程序是指以電子方法比較因不同目的而收集的個人資料，從中得出的結果可用作對有關資料當事人採取不利行動的程序。資料使用者如無資料當事人的訂明同意或私隱專員的同意，不得進行核對程序。

在本年度，私隱專員共收到38宗個人資料核對程序申請，全部來自政府部門及公營機構。

經審閱後，私隱專員在有條件的情況下批准了全部申請。以下是私隱專員核准進行個人資料核對程序的部分個案。

DATA MATCHING PROCEDURE

A data matching procedure is a process by which personal data collected for one purpose is compared electronically with personal data collected for other purposes with the aim of taking adverse action against the data subjects concerned. A data user shall not carry out a matching procedure unless it has obtained the data subjects' prescribed consent or the Privacy Commissioner's consent.

During the reporting year, the Privacy Commissioner received 38 applications for approval to carry out matching procedures. All of these applications came from government departments and public-sector organisations.

Upon examination, all applications were approved, subject to conditions imposed by the Privacy Commissioner. The followings are some of the matching procedures approved by the Privacy Commissioner.

提出要求機構 Requesting Parties	核准的資料核對程序詳情 Details of the Approved Data Matching Procedures
衞生署 Department of Health	把衞生署從「大腸癌篩查先導計劃」參加者收集的個人資料，與入境事務處的人事登記記錄中的個人資料互相比較，以核實參加者的資格。 Comparing the personal data collected by the Department of Health from the participants of the Colorectal Cancer Screening Programme with the personal data held in registration of persons records of the Immigration Department, in order to assess the eligibility of the participants.
香港海關 Customs and Excise Department	把香港海關從部門宿舍申請人及居住人與其配偶收集的個人資料，與香港房屋委員會從資助房屋業戶、租戶及申請人收集的個人資料互相比較，以避免給予雙重房屋福利。 Comparing the personal data collected by the Customs and Excise Department from the applicants and occupants of departmental quarters and their spouses with the personal data collected by the Hong Kong Housing Authority from the owners, tenants and applicants of subsidised housing, in order to prevent the collection of double housing benefits.
市區重建局 Urban Renewal Authority	把市區重建局從「港人首次置業先導項目」申請人及其於申請表列出的家庭成員收集的個人資料，與香港房屋委員會從資助房屋業戶、租戶及申請人收集的個人資料互相比較，以防止濫用公共房屋資源。 Comparing the personal data collected by the Urban Renewal Authority from the applicants and listed family members of the Starter Home Pilot Project and with the personal data collected by the Hong Kong Housing Authority from the owners, tenants and applicants of subsidised housing, in order to prevent abuse of public housing resources.
在職家庭及學生資助事務處 Working Family and Student Financial Assistance Agency	把在職家庭及學生資助事務處從「關愛共享計劃」申請人收集的個人資料，與社會福利署從「綜合社會保障援助計劃」及「公共福利金計劃 」受助人收集的個人資料互相比較，以辨識符合資格的申請人。 Comparing the personal data collected by the Working Family and Student Financial Assistance Agency from the applicants of the Caring and Sharing Scheme with the personal data collected by the Social Welfare Department from beneficiaries of the Comprehensive Social Security Assistance and Social Security Allowance Scheme, in order to assess the eligibility of the applicants.