監督符規 擁抱挑戰

MONITORING COMPLIANCE EMBRACING CHALLENGES

私隱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。

PCPD monitors and promotes data users' compliance with the provisions of the PDPO. 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

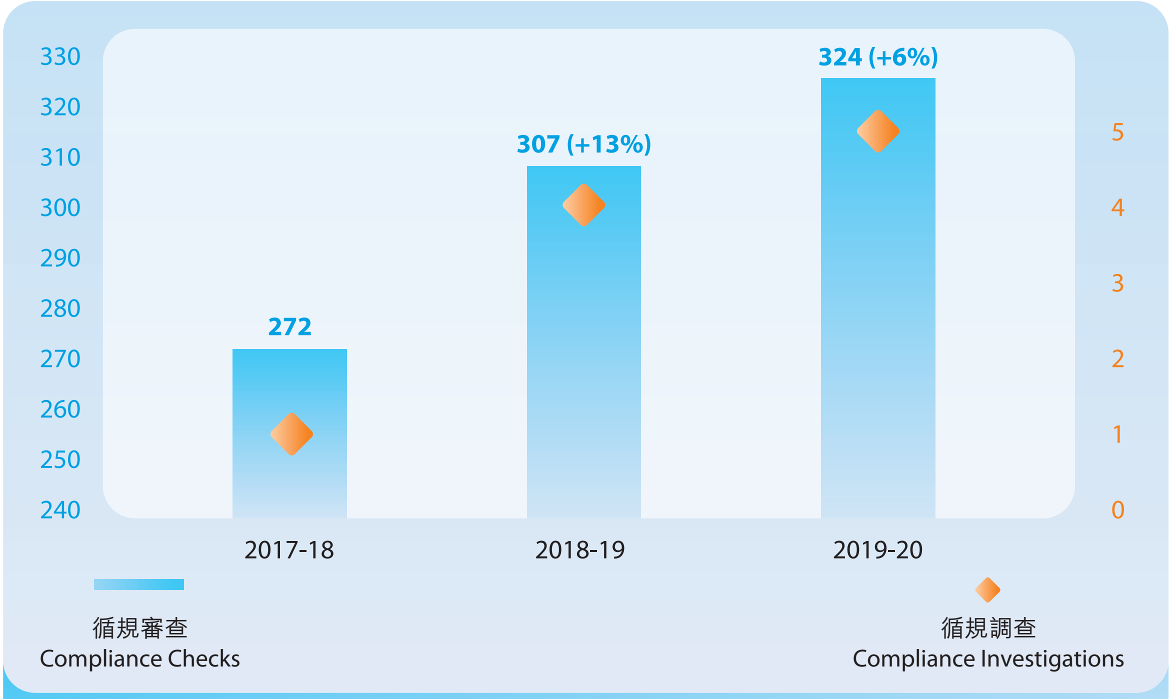
當有足夠理由相信有機構的行事方式與《私隱條例》規定不相符時，私隱專員會展開循規審查或調查。在完成循規審查或調查後，私隱專員會書面告知有關機構，指出與《私隱條例》規定不符或不足之處，並促請有關機構採取適當的補救措施，糾正可能違規的情況和採取預防措施。

在報告年度內，私隱專員共進行了324次循規審查，較2018/19年度的307次上升6%。在報告年度內亦主動進行五次循規調查，較2018/19年度的四次上升25%。

COMPLIANCE ACTIONS

The Privacy Commissioner conducted compliance checks or investigations into practices that he had sufficient grounds to consider to be inconsistent with the requirements under the PDPO. Upon completion of a compliance check or investigation, the Privacy Commissioner alerted 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 324 compliance checks and five compliance investigations, as compared to 307 compliance checks and four compliance investigations in 2018/19, representing 6% and 25% increases respectively.



2017/2018至2019/2020年報告年度內循規審查及循規調查數目
Numbers of Compliance Checks and Compliance Investigations during the reporting year from 2017/2018 to 2019/2020

下文重點介紹在年內進行的部分循規行動。

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

循規調查

某政府部門遺失一本經劃線的正式選民登記冊

2019年4月9日，某政府部門就遺失一本2016年立法會換屆選舉「經劃線的正式選民登記冊」（該登記冊）向私隱公署作出資料外洩事故通報。該登記冊載有8,136名在該選舉中獲編配到位於葵青區的一所投票站的已登記選民的個人資料，包括姓名、性別、地址、香港身份證號碼、選民曾否到該投票站領取選票，及可獲編配的選票數目。由於該登記冊內載有選民的身份證號碼和其選舉或投票狀況等獨特及敏感的個人資料，私隱專員就事件展開調查，並於2019年8月29日發表調查報告。

調查結果

調查顯示該政府部門在資料保安的做法上存在下列問題：

資料保安

- 沒有制定清晰及足夠的政策、處理方式、程序和機制，以保障性質獨特及敏感的個人資料；
- 多次連同大量文件與該登記冊轉移至不同的儲存地點，但沒有就相關的保安風險及由這些風險所引致對個人資料所產生的潛在影響方面進行檢視及評估；
- 沒有妥善及充分備存適當的資料轉運及庫存記錄，亦沒有部門職員和外界人員存取資料的機制；
- 沒有考慮就經劃線的正式選民登記冊內所載的獨特及敏感的個人資料制訂及推行獨立而具針對性的保安措施，尤其是在選舉後不再需要相關登記冊時的措施；
- 沒有就疏忽的人為錯誤進行風險評估；
- 沒有就安全處理資料事宜與所有相關人士溝通及提供足夠培訓；及
- 沒有制定資料外洩事故應變計劃。

COMPLIANCE INVESTIGATION

Loss of a marked final register of electors by a government department

On 9 April 2019, a government department submitted a data breach notification to PCPD informing it that a marked final register of electors used in the 2016 Legislative Council General Election was lost. The marked final register of electors contained the personal data of 8,136 registered electors assigned to a polling station in Kwai Tsing District in the election, including name, gender, address, Hong Kong Identity Card number, whether an individual elector had collected ballot papers at the said polling station and the number of ballot papers that he might be issued with. Since the personal data contained in the marked final register of electors included the unique and sensitive information about electors' identity card numbers and their election or polling status as registered electors, the Privacy Commissioner initiated an investigation. The investigation report was published on 29 August 2019.

Result of investigation

The investigation revealed the following issues in relation to the data security practices of the government department:

Data security

- Failure to have in place clear and adequate policies and handling practices, procedures and systems to protect personal data of this unique and sensitive nature;
- Failure to assess and evaluate the security risks and the potential impacts of the risks on the personal data handled in relation to the multiple transfers and storage venues for large number of documents, including the marked final register of electors;
- Failure to maintain proper and adequate records of inventory and retrieval systems by both internal and external staff handling the data;
- Failure to consider formulating and implementing separate and specific security measures for the unique and sensitive data in the marked final register of electors especially where it would not be required after the poll;
- Failure to assess the risk of inadvertent human error;
- Failure to communicate with all relevant persons and conduct adequate training on the secure handling of the data; and
- Failure to have in place a data breach response plan.

資料外洩事故通報

現行的《私隱條例》沒有規定資料使用者須向私隱專員及受影響的選民通報資料外洩事故，亦沒有規定他們須在指定時間內作出通報。在此範疇上該政府部門雖則沒有違反《私隱條例》的規定，但私隱專員認為事件涉及獨特而敏感的個人資料，該政府部門應可在更早的時間作出通報。

鑑於本案所揭示的事實及所有相關情況，私隱專員認為該政府部門沒有採取所有合理地切實可行的步驟，確保該登記冊內已登記選民的個人資料受到保障而不致遺失或在超過30個月的反覆搜尋下仍未能尋回，因而違反了《私隱條例》附表1的保障資料第4(1)原則下有關資料保安的原則。

執行通知

私隱專員向該政府部門送達執行通知，指示該政府部門：

- 把經劃線的正式選民登記冊的處理及儲存與其他選舉文件分開，包括：分開收拾及把所有經劃線的正式選民登記冊集中儲存於指定及適當的地方；
- 制定程序以妥善及有效地規管經劃線正式選民登記冊的物流管理；
- 制定有關妥善記錄選舉文件的傳運程序、存取機制，以及檔案檢視的程序；
- 制定個人資料審計指令，以處理遺失個人資料的事宜及相關的搜尋程序；及
- 制定和推行有效及足夠措施和培訓，以確保該政府部門、投票站及其他相關職員遵從上述的程序和指令。

Data breach notification

There being no statutory requirements under the PDPO for a data breach notification, whether to the Privacy Commissioner or the affected electors, and whether within a particular period of time or otherwise, the Privacy Commissioner found no contravention of the PDPO in this connection. However, considering the unique and sensitive nature of the personal data involved, the government department should have given data breach notification earlier.

In light of the facts found and in all the circumstances of the case, the Privacy Commissioner concluded that the government department contravened Data Protection Principle (DPP) 4(1) of Schedule 1 to the PDPO (Data Security Principle) by not taking all reasonably practicable steps to ensure that the personal data of the registered electors contained in the marked final register of electors was protected against its loss, or not being located after repeated searches over a period of 30 months.

Enforcement Notice

The Privacy Commissioner served an Enforcement Notice to direct the government department to:

- Separate the handling and storage of the marked final register of electors from other electoral documents including separate packing and centralising storage of all marked final registers of electors in designated and adequate storage locations;
- Set up procedures governing properly and effectively the logistical management of the marked final registers of electors;
- Set up procedures in respect of proper recording of movements of electoral documents, retrieval systems and dossier reviews;
- Set up personal data audit directives to address, in particular, the issue of loss of personal data and the associated searching process; and
- Set up and implement effective and sufficient measures and training to ensure compliance with the above procedures and directives by staff of the government department itself, polling station and other related staff.

借鑒

現今環球趨勢著重數據道德管治，其中問責原則漸被視為有效的個人資料保障管理工具，透過採取適當的技術性和機構性措施，彰顯合規要求，以防止資料外洩事故發生，積極保障個人資料私隱的權利。資料使用者，包括公營機構，應參考上述的問責原則並建立其私隱管理系統，確保實施足夠的保安措施以對應所持有的資料的敏感度，從而滿足資料當事人對其個人資料的合理私隱期望。

Lesson learnt

Nowadays, ethical data governance has become a worldwide trend, in which the accountability principle, essentially putting in place appropriate technical and organisational measures to ensure and to demonstrate compliance with the data protection law, is increasingly seen as an effective management tool to proactively protect personal data privacy right and prevent data breaches. Data users, including public organisations, are recommended to make good reference to the accountability principle and to develop their privacy management programmes to ensure adequate security measures which are commensurate with the sensitivity of the data being held are in place, in order to meet the reasonable privacy expectation of data subjects who are the owners of their personal data.

未經授權網上查取信貸報告

2018年11月28日，私隱專員接獲一間信貸資料機構（該機構）就第三者懷疑未經授權通過該機構的網上認證程序而取得數名公眾人士的信貸報告（該事件）而作出的資料外洩事故通報。2018年11月30日，私隱專員展開循規調查。

該事件發生時，個人可透過該機構網站及其五個夥伴的網站／手機程式申請及查取信貸報告。該機構設定及核准於網上申請及查取信貸報告的認證程序，將同一程序和標準應用於其網站和五個夥伴的網站／手機程式。認證決定由該機構作出。

網上認證程序包括 (1) 將個人輸入的全名、出生日期和香港身份證號碼與該機構的資料庫配對；(2) 評估進入系統的裝置的風險；(3) 三或五條「基於知識的認證」選擇題；及 (4) 在高風險的情況下，發送一次性密碼至個人的手機號碼。

在該機構與五個夥伴的聯合運作中，該機構使用其持有的個人資料認證個人的身分，並在該人所選的網站／手機程式中顯示信貸資料。該機構亦會轉移個人資料予其中三個夥伴。

該事件涉及的法律事宜集中在《私隱條例》附表1的保障資料第3原則（資料使用）及保障資料第4原則（資料保安）的規定。

Unauthorised online access to credit reports

On 28 November 2018, the Privacy Commissioner received a data breach notification lodged by a credit reference agency (Company) in respect of the suspected unauthorised access by a third party passing through the online authentication procedures of the Company and obtaining the credit reports of a number of public figures (the Incident). The Privacy Commissioner initiated a compliance investigation on 30 November 2018.

At the time of the Incident, online application for and access to credit reports by individuals were available through the Company's website and its five partners' websites/mobile application. The Company set and verified the online authentication procedures for application for and access to credit reports, and applied the same procedures and standards across its own website and the five partners' websites/mobile application. It was the Company that made the authentication decision.

The online authentication procedures covered (1) the matching of the full name, date of birth and Hong Kong Identity Card number input by the individual against the Company's database; (2) the assessment of the risk associated with the device used to access the system; (3) a set of three or five multiple-choice knowledge-based authentication questions; and (4) the sending of a one-time password to the individual's mobile number for high risk cases.

In the joint operation with the five partners, the Company used the personal data it held to authenticate an individual's identity and display the credit data on the website(s)/mobile application chosen by the individuals. The Company also transferred the individuals' personal data to three partners.

The legal issues involved focused on data use and data security set out in Data Protection Principle (DPP) 3 (Data Use Principle) and DPP 4 (Data Security Principle) of Schedule 1 to the PDPO.

調查結果

資料使用 - 資料顯示及轉移資料予夥伴 - 不違規

私隱專員認為該機構使用個人資料作身分認證及向有關個人顯示信貸資料的目的與收集資料的目的一致。另一方面，轉移個人資料予部分夥伴的目的則並非該機構收集相關資料的原本目的或與該目的直接有關，所以如此轉移需按照《私隱條例》附表1的保障資料第3(1)原則(資料使用)的規定取得有關個人的訂明同意。私隱專員審視了申請程序的每個步驟，並無發現如此轉移違反保障資料第3(1)原則。

資料保安 - 網上認證程序存在漏洞 - 違規

私隱專員認為該機構在網上認證程序中沒有採取所有切實可行的步驟以確保由其持有的個人資料受保障而不受未獲准許的或意外的查閱或使用，因而違反了《私隱條例》附表1保障資料第4(1)原則(資料保安)，基於：

- 個人所輸入的全名和出生日期無須與該機構資料庫的紀錄完全脗合；
- 「基於知識的認證」採用了 (i) 與個人年齡範圍及生肖這些與該機構獨有交易無關的問題，及 (ii) 過時而易被剔除的答案；
- 其他網站／手機程式的查取途徑沒有因個人未能通過某一網站／手機程式的認證程序而被封鎖；及
- 非所有申請均使用雙重認證。

Result of investigation

Data use – data display and transfer of data to partners – no contravention

The Privacy Commissioner considered that the use of personal data for identity authentication and display of credit data to the individual was a purpose consistent with the purpose for which the data was collected. The purpose of transferring personal data to some of the Company's partners, on the other hand, did not fall within the original purpose or a directly related purpose for which the Company collected the concerned data, and such transfer would therefore call for the individual's prescribed consent as required under DPP 3(1) of Schedule 1 to the PDPO (Data Use Principle). The Privacy Commissioner went through the application procedures step by step. No contravention of DPP3(1) was found on such transfers.

Data security – vulnerabilities in online authentication procedures – contravention

The Privacy Commissioner found that the Company contravened DPP4(1) of Schedule 1 to the PDPO (Data Security Principle) in respect of its online authentication procedures in that it failed to take all practicable steps to ensure that the personal data held was protected against unauthorised or accidental access or use, on the grounds that:

- An exact match of the full name and date of birth input by an individual against the records of the Company's database was not required;
- The knowledge-based authentication used (i) questions that asked about the age range and Chinese zodiac sign of the individuals instead of unique dealings with the Company, and (ii) outdated answers that could be easily screened out;
- Access through other websites/mobile application was not blocked after an individual failed the authentication procedures on one website/mobile application; and
- Two-factor authentication was not applied to all applications.

執行通知

私隱專員向該機構送達執行通知，指令該機構糾正及防止該項違反再發生：

i. 停止在未經一次性密碼認證核實的情況下透過任何網站／手機程式在網上發放信貸報告；

ii. 當一次性密碼認證核實不適用於網上信貸報告申請時，須進行親身認證；

iii. 制定清晰的程序，指明有關步驟、時限及監察措施，以確保為「基於知識的認證」問題中所產生的答案是相關、具效能和合時的。

借鑒

在現今資訊及通訊科技急速發展的世代，網上服務已是商業營運及日常生活中不可或缺的一部分。網上服務為個人帶來方便，但同時有賴可靠及穩健的資訊保安措施，包括網上認證程序。公眾合理預期一間收取及處理大量信貸資料的信貸資料機構有責任持續檢討及改善其網上認證程序，以阻止騙徒查取信貸資料。鑑於科技進步，信貸資料機構應進行定期檢討，以查找及修補漏洞，並改善認證程序（包括評估使用生物特徵認證的合適性）。

Enforcement Notice

The Privacy Commissioner served an Enforcement Notice on the Company directing it to remedy and prevent any recurrence of the contravention:

i. Cease to release any credit reports online through any website/mobile application without one-time password verification;

ii. Conduct in-person authentication for all online applications of credit reports where one-time password verification is not applicable; and

iii. Devise clear procedures to specify the steps, time limits and monitoring measures to ensure the answers generated for knowledge-based authentication questions are relevant, functional and up-to-date.

Lesson learnt

In this age of rapid development of information and communication technologies, online services have become indispensable to business operations and our daily lives. Online services offer convenience to individuals but at the same time necessitate reliable and robust data security measures, including online authentication procedures. It is legitimately expected that a credit reference company which receives and processes a considerable amount of credit information is duty bound to continuously review and improve its online authentication procedures in order to block fraudsters from accessing credit data. In view of technology advancement, periodic reviews with the aim of identifying and fixing loopholes as well as improving the authentication procedures (including assessing the appropriateness of using biometric authentication) should be conducted.

循規審查

未獲授權取覽公立學校網上應用系統內的個人資料

四所公立學校向私隱公署通報，指由負責推行教育的政策局所開發並由他們營運的網上應用系統（該系統）遭黑客入侵，導致儲存在內的資料被盜。公署就事件偵訊該四所學校及該政策局。

循規行動顯示該政策局負責向學校提供該系統的技術支援、指引和培訓，而學校作為該系統的用戶則負責操作和維護該系統，以及處理當中所載的學生個人資料。

該政策局不時發布該系統的更新版本，以提供解決網絡安全問題的附加功能。在偵測到未獲授權取覽該系統後，該政策局已發布該系統的更新版本以修補保安漏洞，並要求學校在兩周內把該系統更新至最新版本。然而，並非所有遭受攻擊的學校都及時進行更新。

因應該事件，該政策局向學校發布了通告，提醒他們須根據項目表定期檢查運行該系統的伺服器和日誌記錄。該政策局還承諾在出現高風險的情況下及必須即時進行重大的安全更新時，會與學校進行更直接的溝通。另一方面，該政策局確認該系統正逐步轉移至中央雲端平台，以便更有效地監察該系統的可疑活動，及更適時採取保護措施或應用新版本。

借鑑

沒有機構可完全免受網絡攻擊，對於資料使用者而言，採取所有合理的預防措施來保護其系統免受網絡攻擊是非常重要的。雖然該政策局在這次事件中並非資料使用者，但作為該系統的提供者和公立學校的監督機構，可採取更主動的方法指示其用戶適時安裝所有重大更新。學校一旦收到由該政策局發布就該系統的更新通知時，亦應立即採取相應行動，以保障資料的完整性和安全。

COMPLIANCE CHECK

Unauthorised access of personal data held by public schools via a web-based application system

Four public schools reported to PCPD that a web-based application system operated by them and developed by the government bureau responsible for education (the System) was compromised and the data contained therein were stolen. PCPD inquired the four schools and the bureau regarding the incident.

The compliance actions revealed that the bureau was responsible for providing technical support, guidelines and training to the schools regarding the System, whereas the schools being the System users were responsible for operating and maintaining the Systems as well as handling students' personal data contained therein.

The bureau provided updated versions of the System from time to time with additional functions addressing cybersecurity issues. After detecting an unauthorised access into the System, the bureau released an updated version of the System fixing the security vulnerabilities, and requested the schools to update to the latest version within two weeks. However, not all schools suffering from the attack applied the update promptly.

In response to the incident, the bureau issued notices to schools reminding them to regularly review the operation of the System server and logs according to the applicable task list. The bureau also committed to having more direct communication with schools if a high risk situation arose and an immediate critical security update was warranted. On the other hand, the bureau confirmed that the System was gradually moving to a centralised cloud platform so as to better monitor the suspicious activities and apply protective measures or new versions in a timely manner.

Lesson learnt

No organisation could be completely immune from cyberattacks. It is therefore important for data users to take all reasonable precautions to protect their systems from cyberattacks. Although the bureau is not the data user in this incident, being the System provider as well as the supervisory body of public schools, the bureau could adopt a more proactive approach to direct its users to install all critical updates. On the other hand, the schools should have acted promptly once they received any notice regarding the update of the System from the bureau so as to safeguard data integrity and security.

員工未經授權轉移公司持有的個人資料至其私人電腦

某金融機構向私隱公署通報，指其行政人員在未經授權下以其個人USB記憶體從公司桌上電腦抄寫了4,000多個檔案至其私人手提電腦，當中51個檔案載有約6,600名客戶、30名員工及落選求職者的個人資料。涉及的個人資料包括有關客戶的金融戶口資料、員工的人力資源資料及落選求職者的履歷。得悉事件後，公署決定展開循規審查。

在循規審查的過程中，私隱公署發現該名員工是該機構唯一因工作關係而獲授權使用有讀寫功能的USB記憶體的員工，涉事的檔案則在沒有以密碼保護的情況下被儲存於其公司桌上電腦的本地驅動器內。該名員工解釋因事發時其公司電腦的運算速度變慢，故抄寫檔案至其私人手提電腦以便清空公司電腦的硬碟空間。

A staff member transferred personal data held by his employer to his personal computer without authorisation

A financial institution reported to PCPD that an administrative staff member copied more than 4,000 files from the office desktop computer to his personal laptop via his own USB flash drive without authorisation. Among those files, 51 of them contained personal data of around 6,600 customers, 30 staff members and unsuccessful job applicants. Personal data involved included financial account details of customers, human resources data of staff members and curricula vitae of unsuccessful job applicants. On knowing the incident, PCPD initiated a compliance check.

In the compliance check process, PCPD found that the staff member concerned was the only staff who was granted permission to use USB flash drive with read-and-write functions in discharging his duties. The files concerned, which were encrypted and password-protected, were stored on the local drive of his office desktop computer, which was not password-protected. The staff member explained that he copied the files to his personal laptop with a view to cleaning up the space of the hard disk of his office computer which was running slow at the material time.

經過內部調查後，該金融機構認為該名員工未有披露資料當事人的個人資料或意圖在事件中為其自身或任何其他人獲得金錢或財產得益，或導致資料當事人蒙受金錢或財產損失。無論如何，該名員工已簽署保密協議確認並沒有向任何第三者披露檔案中的資料，並已即時及永久刪除有關檔案。

事件發生後，該金融機構撤回該名員工的USB記憶體的抄寫權限。此外，該機構亦向所有員工發電郵提示他們其機構就安全使用便攜性儲存裝置所制定的全球性政策，以及安排所有員工參加資訊保安風險培訓課程。

借鑑

員工在企業環境中無可避免地可接觸個人資料。一般而言，負責行政及人事管理的員工因工作性質需要處理大量敏感性的個人資料。機構應重視數據管治及尊重保障私隱的文化，要達至此目標，機構必須定期檢視及監察員工查取個人資料的權限，確保其員工嚴格按「有需要知道」的原則處理個人資料。

After internal investigation, the financial institution considered that the staff member concerned had not disclosed any personal data of a data subject and that the staff member had no intent to obtain gain in money or other property (for any person's benefit) or to cause loss in money or other property to any data subject involved in this incident. In any event, the staff member concerned signed a Non-Disclosure Agreement specifying that he had not disclosed any data contained in the files to any third party and had deleted the files immediately and permanently.

In the wake of the incident, the financial institution revoked the USB write-access right of the staff member concerned. The institution also sent an email to all staff members reminding them of the institution's global policy on secure use of removable storage devices and arranged training for all staff members in information security risk.

Lesson learnt

In business environment, it is inevitable that staff members have access to personal data. In general, those who are responsible for administrative and human resources-related matters have to handle a large amount of sensitive personal data. Organisations should attach great importance to data governance and the culture of respecting and protecting privacy. To this end, organisations should regularly review and monitor their staff members' access right to personal data to ensure that they would handle personal data on a "need-to-know" basis.

資料外洩通報

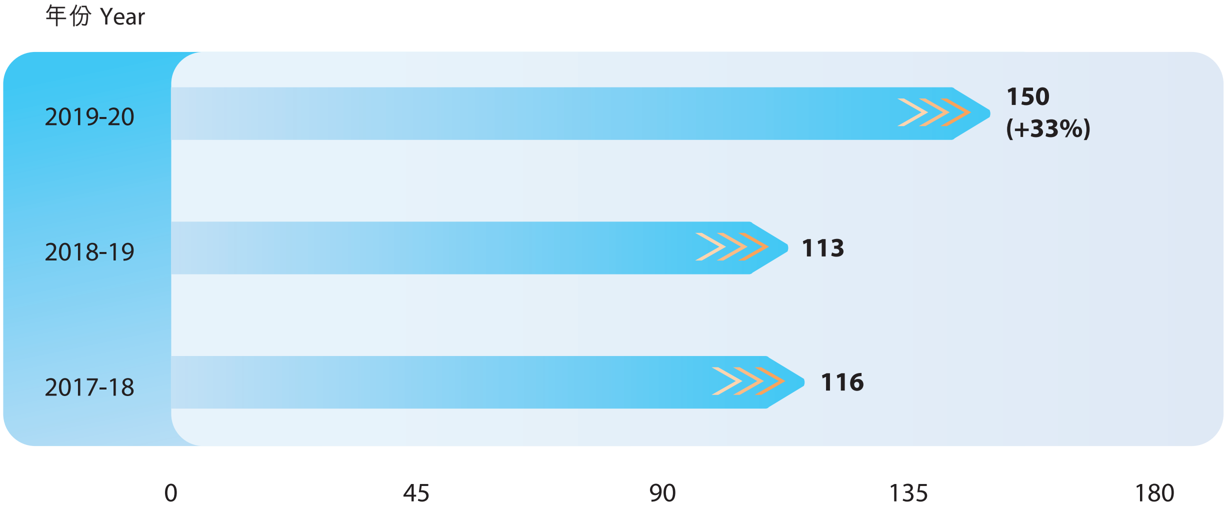
資料外洩事故一般是指資料使用者所持有的個人資料保安不足，以致洩露資料，令資料可能被人未經授權或意外地查閱、處理、刪除、喪失或使用。資料外洩事故可能構成違反保障資料第4原則。雖然《私隱條例》並未有規定資料使用者就資料外洩事故作出通報，但為符合數據道德標準，私隱公署一直鼓勵資料使用者一旦發生資料外洩事故，須通知受影響的資料當事人、私隱專員和其他相關人士。

私隱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。

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 PDPO does not require data users to give data breach notification (DBN), PCPD has always encouraged data users, in line with 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 PCPD-designated DBN form or other means of communication), 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.



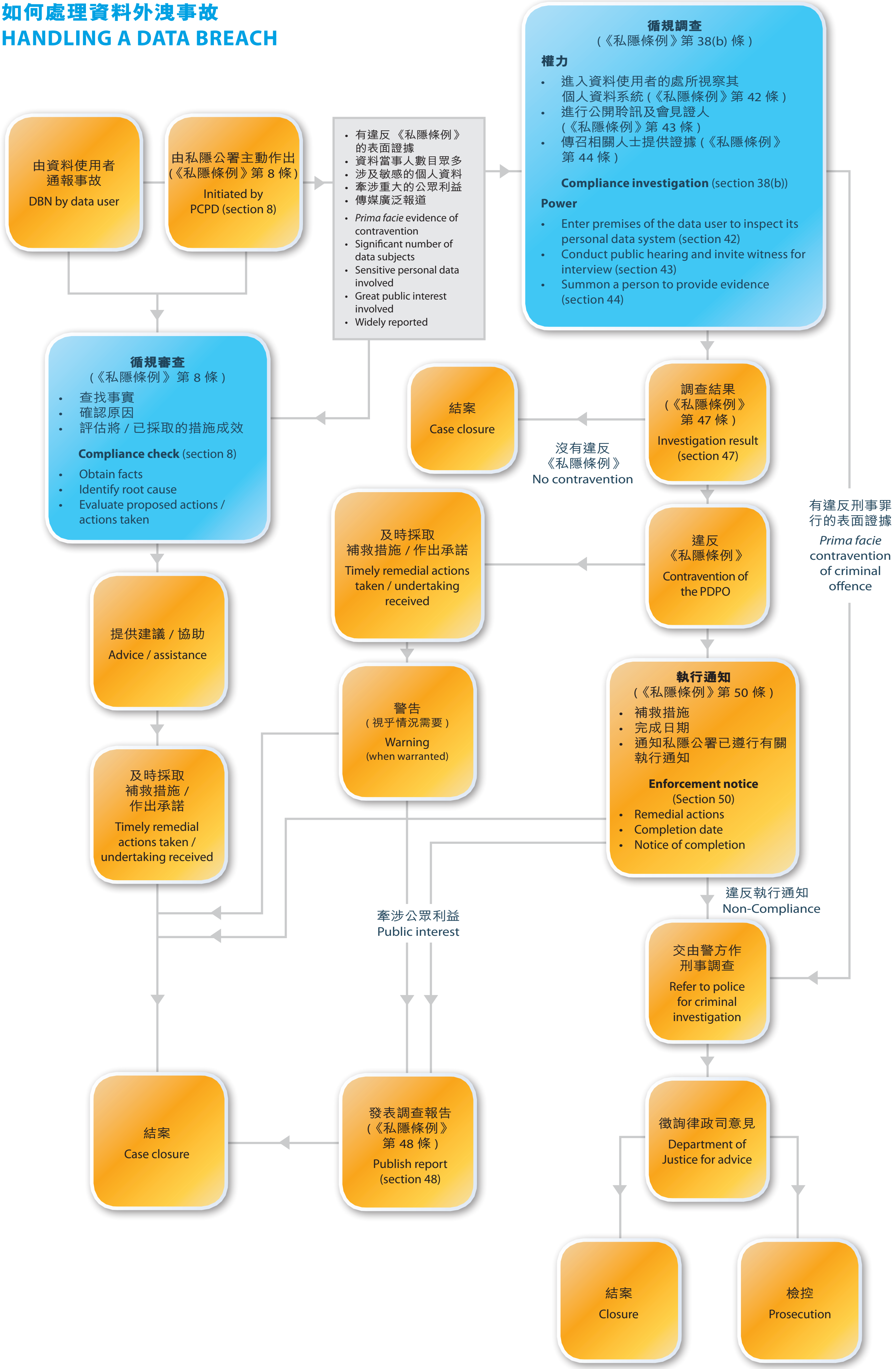
2017/2018至2019/2020年度內資料外洩通報數目

Numbers of Data Breach Notifications
from 2017/2018 to 2019/2020

在本報告年度內，私隱公署接獲150宗資料外洩事故通報（64宗來自公營機構；86宗來自私營機構），較上一報告年度的113宗上升33%，牽涉約290萬名人士的個人資料。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150宗事故均展開循規審查行動。

During the reporting year, PCPD received 150 DBNs (64 from the public sector and 86 from the private sector), a 33% increase as compared to last year (113 DBNs), involving personal data of about 2.9 million 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. PCPD conducted compliance check in each of these 150 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

由私隱公署主動作出（《私隱條例》第 8 條）

Initiated by PCPD (section 8)

- 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)

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

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 PDPO

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
- 通知私隱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)

違反執行通知

Non-Compliance

有違反刑事罪行的表面證據

Prima facie contravention of criminal offence

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

個人資料的核對程序

個人資料的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49宗來自政府部門及公營機構的個人資料核對程序申請，較2018/19年度的38宗申請上升29%。增加主要歸因於政府和公營機構推出多項紓困措施和資助房屋計劃，需透過執行核對的程序以核實申請人的資格，從而確保適當地運用公帑於目標群組。

經審閱後，私隱專員在有條件的情況下批准了47宗申請，一宗申請不屬《私隱條例》釋義所指核對程序，而另一宗申請則被撤回。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 49 applications from government departments and public sector organisations for approval to carry out matching procedures, representing a 29% increase when compared to 38 applications received in the previous year. The increase was mainly attributable to a number of relief measures and subsidised housing schemes implemented by the Government and public bodies, which needed to ascertain the applicants' eligibility through procedures for checking applications in order to ensure proper allocation of public money to the target groups.

Upon examination, 47 applications were approved, subject to conditions imposed by the Privacy Commissioner; one application was found not to be matching procedure as defined under the PDPO; and one application was withdrawn. Some of the examples of matching procedures approved by the Privacy Commissioner are as follows:

提出要求者 Requesting Parties	核准的資料核對程序詳情 Details of the Approved Data Matching Procedure
教育局 Education Bureau	把教育局從「學生津貼」計劃申請人收集的個人資料，與入境事務處用作處理簽證、永久性居民身份證及出生登記的申請等的個人資料互相比較，以核實申請人的資格。 Comparing the personal data collected by the Education Bureau from applicants of the Student Grant scheme with the personal data collected by the Immigration Department for processing applications of visa, permanent identity card and birth registration, etc. in order to ascertain the eligibility of the applicants.
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「在職家庭津貼」受助人（於立法會批核有關撥款當日的前六個歷月內作出申請）收集的個人資料，與社會福利署從「綜合社會保障援助計劃」受助人（以立法會批核有關撥款當日為限）收集的個人資料互相比較，以避免給予雙重額外一個月的津貼。 Comparing the personal data collected by the Working Family and Student Financial Assistance Agency from the recipients of Working Family Allowance (whose applications were made within six calendar months immediately before the date on which funding approval was given by the Legislative Council) with the personal data collected by the Social Welfare Department from the recipients of Comprehensive Social Security Assistance (on the date of funding approval obtained from the Legislative Council), in order to avoid paying duplicate one-month extra allowance to the recipients.
選舉事務處 Registration and Electoral Office	把選舉事務處從選民收集的個人資料，與房屋署從新近成為資助房屋租戶或業戶的個人資料互相比較，以識別未有通知選舉事務處更改居住地址的選民。 Comparing the personal data collected by the Registration and Electoral Office from electors with the personal data collected by the Housing Department from tenants and owners who had taken up tenancy or ownership of the flats under subsidised housing schemes recently, in order to identify electors who did not inform the Registration and Electoral Office of their changes of residential addresses.
香港房屋協會 Hong Kong Housing Society	把香港房屋協會從「未補價資助出售房屋出租計劃」的「參與計劃證明書 - 租客」申請人及其於申請中列明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租戶、業戶及申請人收集的個人資料互相比較，以確保沒有提供雙重房屋福利。 Comparing the personal data collected by the Hong Kong Housing Society from the applicants for "Certificate of Participation – Tenant" under the Letting Scheme for Subsidised Sale Developments with Premium Unpaid and their family members listed on the applications with the personal data collected by the Hong Kong Housing Authority from tenants, owners and applicants of various subsidised housing schemes, in order to ensure no duplication of subsidised housing benefits.