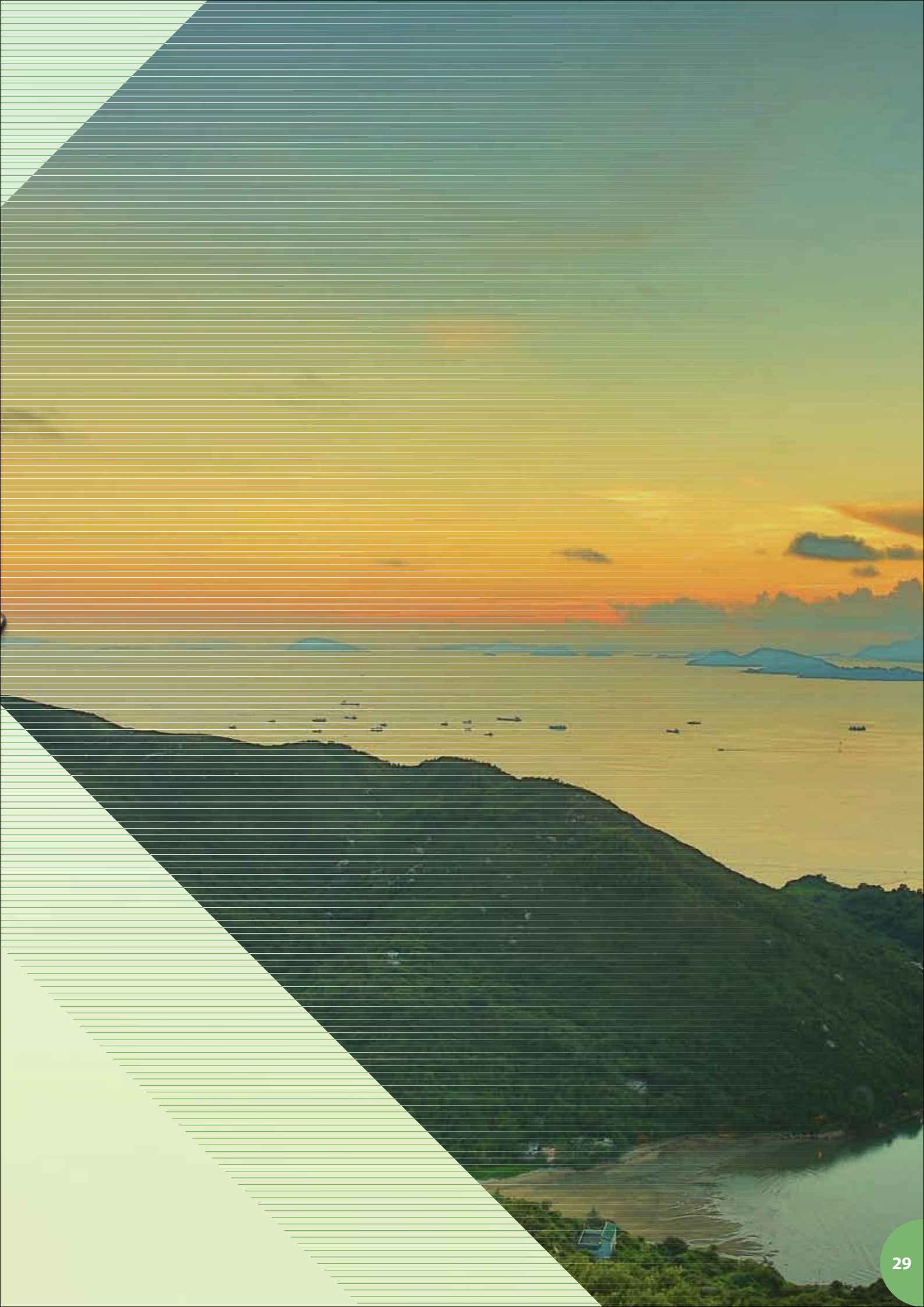
Monitoring Compliance Embracing Challenges

監督符規 擁抱挑戰

合規部監察和推動資料使用者要循規以符合條例的規定。隨著資訊科技急速發展而衍生的私隱風險，我們鼓勵和支援機構採取所有方法和手段，以保障個人資料，並尊重消費者的個人資料私隱。

The Compliance Division monitors and promotes compliance with the provisions of the Ordinance. In view of the privacy risks brought about by the rapid advances in information and communication technology, we encourage and facilitate organisations to apply all means to ensure personal data protection and respect consumers' personal data privacy.



私隱抽查行動2016——物聯網裝置

於2016年5月，私隱專員聯同全球其他24個私隱執法機關進行了私隱抽查行動。有關行動由「全球私隱執法機關網絡」(Global Privacy Enforcement Network)負責組織協調。本年的抽查目標為物聯網裝置，物聯網是指不同物件透過安裝電子感應器及軟件，令該些物件彼此能通過互聯網互相交換資料，目的是了解它們在私隱方面與用戶溝通的足夠程度。本年被抽查的物聯網裝置合共314個。

本地及全球的抽查結果均顯示物聯網裝置的製造商與用戶在私隱方面的溝通做得不太理想。

全球抽查結果

2016年的抽查行動顯示，大部份製造商均沒有向用戶披露物聯網裝置確實會收集哪些個人資料，以及所收集得的資料會被如何處置。以下是綜合25個私隱執法機關在本次抽查行動中的一些重要結果：

- 59%的製造商沒有向用戶充份解釋他們的個人資料會被如何收集、使用及披露；
- 68%的製造商沒有適當地向用戶說明個人資料會如何儲存；
- 49%的製造商沒有向用戶說明採取了甚麼保安措施以防止個人資料被未獲授權地讀取或處理；
- 72%的製造商沒有向用戶提供清晰指引以刪除在裝置或相關流動應用程式上的個人資料；及
- 38%的製造商沒有向用戶提供聯絡資料，以供他們查詢與私隱相關的事宜。

PRIVACY SWEEP 2016 - STUDY OF INTERNET OF THINGS (IOT) DEVICES

In May 2016, the Commissioner joined forces with 24 other privacy enforcement authorities around the globe to conduct the Privacy Sweep exercise coordinated by the Global Privacy Enforcement Network (GPEN). The targets of this year's Privacy Sweep were IoT devices. IoT is the network of physical objects embedded with electronic sensors and software that enables the physical objects to exchange data with one another via the Internet. The purpose was to examine the adequacy of privacy protection in the communications through the devices. A total of 314 IoT devices were examined by the privacy enforcement authorities.

Both the local and the global results of the Privacy Sweep showed that the privacy communications undertaken by the manufacturers of IoT devices to end users was generally unsatisfactory.

Global findings

The Privacy Sweep 2016 revealed that the majority of manufacturers did not provide sufficient information to their customers about the exact personal data collected by the devices and how the collected data would be processed. Below are some of the significant findings of the Privacy Sweep by the 25 privacy enforcement authorities engaged in the Privacy Sweep 2016:

- 59% of the manufacturers failed to adequately explain to users how their personal data would be collected, used and disclosed;
- 68% of the manufacturers failed to properly explain to users how their personal data would be stored;
- 49% of the manufacturers failed to inform users about how their personal data would be safeguarded against unauthorised access or processing;
- 72% of the manufacturers did not provide clear instructions to users on how to delete their personal data from the devices or the related mobile apps; and
- 38% of the manufacturers failed to provide easily identifiable contact details should the users have any privacy concerns.

本地抽查結果

在香港，公署抽查的五款本地生產的物聯網裝置，均為智能健身腕帶。智能健身腕帶是用戶配戴在手腕的電子感應器，用來追蹤及監察用戶的日常活動及生理狀況指標（例如步行距離、消耗的卡路里及心跳率）。其他私隱執法機關所抽查的物聯網裝置包括智能讀數錶、聯網玩具及聯網汽車。物聯網裝置通常都需要連同支援的流動應用程式一起使用。

抽查行動顯示超過一半的物聯網裝置都沒有在私隱政策中向用戶充份解釋如何收集和使用個人資料。下表列出抽查的主要結果，並將香港的抽查結果與全球的抽查結果作比對。

Local findings

In Hong Kong, the PCPD examined five locally manufactured IoT devices, i.e. fitness bands, during the Privacy Sweep 2016. A fitness band is an electronic sensor worn on the wrist of a user for tracking his daily activities and physiological signals, e.g., distance walked, calories burnt, and heart rate. The IoT devices examined by other privacy enforcement authorities included smart meters, connected toys, and connected cars. Very often, these IoT devices were used in conjunction with supporting mobile applications (apps).

The Privacy Sweep revealed that more than half of the IoT devices did not provide users with privacy policies that adequately explained collection and use of personal data. The table below summarises the major findings of the Privacy Sweep and compares the Hong Kong results with the global results.

	香港（五個智能健身腕帶） Hong Kong (five fitness bands)	全球（314個物聯網裝置） Global (314 IoT devices)
在私隱政策中充份解釋個人資料的收集和使用情況 Providing sufficient explanation on the collection and use of personal data in privacy policy	2 (40%)	41%
通知用戶個人資料在哪裡及以甚麼方式儲存 Informing users where and how to store personal data	0 (0%)	32%
承諾採取保安措施保障個人資料 Committed to protect the personal data collected from users	1 (20%)	51%
充份說明如何刪除個人資料 Providing sufficient instructions on deletion of personal data	1 (20%)	28%
提供聯絡資料以供用戶查詢與私隱相關的事宜 Providing contact information for privacy-related enquiries	2 (40%)	62%

觀察及建議

物聯網裝置可以收集很多私密的個人資料，例如身處位置及健康狀況。這些私密的個人資料會經互聯網傳送，甚至可能會分享予其他人士。由於物聯網裝置的內在私隱風險高，製造商應向用戶提供足夠資料，讓用戶衡量使用物聯網裝置的私隱風險。製造商亦應該在裝置上採用私隱友善的設計，並採取足夠措施防止由裝置收集的個人資料被未獲授權地讀取或處理。

Observations and recommendations

IoT devices may collect a lot of our intimate information, such as our location data and health conditions, and these intimate information can be transmitted, and may even be shared through the Internet. The inherent privacy risks of IoT devices being high, it is crucial for manufacturers of IoT devices to provide sufficient information for users to evaluate the privacy risks. The manufacturers should also adopt privacy-friendly designs in the devices, and take sufficient steps to safeguard personal data collected by the devices against unauthorised access and processing.

為加強處理個人資料的透明度及保安，公署建議智能健身腕帶及其他物聯網裝置的生產商應：

- 以簡單語言向用戶提供私隱政策，及協助用戶輕易地在私隱政策中找出重要資料（例如把私隱政策分為不同部分及在每個部分加上標題）；
- 清楚列明收集的個人資料的類別、收集目的、個人資料的潛在承轉人，以及為保障資料而採取的保安措施；
- 採取「貫徹私隱的設計」的做法，例如：減少資料的收集；在傳輸及儲存個人資料時採取足夠的保安措施；及為裝置及其流動程式採取私隱侵犯程度最低的預設設定；
- 若支援的流動應用程式會讀取智能手機內的資料，而這些資料（例如位置及聯絡人清單）與裝置的主要用途並非直接有關，則應容許用戶拒絕提供；
- 提供清晰的指示，讓用戶刪除他們在裝置、智能電話及遠端儲存媒體（例如生產商的後端伺服器，及（如合適）與運動有關的社交網絡）內的個人資料；
- 提供聯絡資料（例如聯絡人、電話號碼、電郵地址及辦公地址）讓用戶查詢有關私隱事宜，及向用戶提供適時回應以解決他們的私隱關注。

To enhance the transparency and safeguards in handling personal data, the PCPD recommends that manufacturers of the fitness bands and other IoT devices should:

- provide privacy policy in simple language to users, and help users locate important information in the privacy policy easily (e.g., by dividing privacy policy into different sections and adding headings to each section);
- clearly state the types of personal data to be collected, the purposes of collection, the would-be transferees of the personal data, and the security measures adopted for protecting the data;
- adopt "Privacy by Design" by, for example, minimising data collection, incorporating sufficient security safeguards for personal data in transmission and in storage, and adopting the least privacy intrusive settings as default on the devices and the mobile apps;
- offer opt-out choice to users if the supporting mobile apps would access data in smartphones that is not directly relevant to the main purpose of the device (e.g., location and contact list);
- provide clear instructions to users for erasing their personal data stored in the devices, smartphones and remote storage (e.g., the backend servers of the manufacturers and sports-related social networks where appropriate); and
- provide contact information (e.g., contact person, telephone number, email address, and office address) for users to pursue privacy-related matters, and respond promptly to users and address their privacy concerns.

智能健身腕帶及其他物聯網裝置的用戶亦有責任保障其個人資料私隱。公署建議用戶：

- 在購買前了解它對個人資料私隱的影響，以及裝置與其支援的流動應用程式收集的個人資料的類別及程度、所收集的個人資料擬用於的用途及現有的保安措施；
- 儘量使用假名進行帳戶登記；
- 為裝置設立專屬帳戶（例如專屬電郵帳戶），儘量避免把裝置的帳戶連結社交媒體帳戶；
- 檢測裝置及其流動程式的預設設定，儘量關閉不必要的功能（例如全球定位系統）；
- 自行設定高強度、複雜的密碼，切勿使用裝置的預設用戶名稱及密碼；
- 適時更新裝置的固件及流動程式，以提升保安程度；
- 在棄置或轉售物聯網裝置前，刪除內裏的資料。

Users of fitness bands and other IoT devices should also play a role in protecting their personal data privacy. The PCPD recommends that users should:

- carry out research on personal data privacy impact before purchase, ascertaining the types and extent of personal data to be collected by the devices and the supporting mobile apps, the intended use of the personal data collected, and the safeguards in place;
- use pseudonyms for account registration whenever possible;
- set up dedicated accounts (e.g., dedicated email accounts) for the devices, and avoid linking the device accounts with social media accounts whenever possible;
- review the default settings of the devices and the mobile apps, and turn off unnecessary functions (e.g., location data access) where possible;
- set strong and complex password by themselves, and never use default usernames and passwords provided by the devices;
- update device and mobile app software whenever possible to enhance security; and
- purge the data in the devices before disposal or resale.

循規審查及調查

當有足夠理由相信某機構的行事方式與條例規定（見附錄一）不相符時，私隱專員會展開循規審查。在完成循規審查或調查行動後，私隱專員會書面告知有關機構，指出與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預防措施以防止類似情況再發生。

A. 循規審查

在報告年度內，私隱專員共進行了256次循規審查行動。78%的循規審查對象為私營機構，其餘22%則關乎公營機構，包括政府部門、法定機構、非政府機構及政府資助教育機構。

下文重點介紹在年內進行的部分循規審查行動。

(i) 民間全民投票活動涉及不公平收集個人資料及投票系統保安不足

香港第五屆行政長官選舉於2017年3月舉行。一個民間團體於選舉前一個月籌辦了一個民間「全民投票」活動。年滿18歲的香港居民可利用該團體提供的電子投票系統分別於「民間提名階段」及「民間全民投票階段」進行投票，以表達對其制定的行政長官候選人的支持或反對。在活動的兩個階段中，共約19,000及65,000名人士參與投票。

該投票系統利用一個名為Telegram的即時通訊程式處理投票過程，並收集了參與投票人士的香港身份證號碼、手提電話號碼，及其Telegram帳戶號碼。根據所獲得的資料，私隱專員認為，(i)該團體在活動中沒有清楚說明收集個人資料的目的和用途的合法理據，(ii)籌辦該活動的資料使用者／控制者（主辦者）的身份不清晰；及(iii)該投票系統去識別化技術的可靠性成疑。

COMPLIANCE CHECKS & INVESTIGATIONS

The Commissioner conducts compliance checks or investigations of practices that he has sufficient grounds to take the view that they may be inconsistent with the requirements under the Ordinance (see Appendix 1). Upon completion of a compliance check or investigation, whether on receipt of reports or at his own initiative, the Commissioner alerts an organisation in writing, pointing out the apparent inconsistency or deficiency, and advising the organisation, if necessary, to take remedial actions to correct any breaches and prevent further breaches.

A. COMPLIANCE CHECKS

During the report year, the Commissioner carried out 256 compliance checks. Of these, 78% were conducted on private sector organisations, while the remaining 22% were on government departments and statutory bodies, non-government organisations, and government-funded educational institutions.

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

(i) Unfair collection of personal data and security of a voting system deployed in a civil referendum activity

The Fifth Term Chief Executive Election of Hong Kong was held on 26 March 2017. One month prior to the election, a civilian group organised a "civil referendum" activity in which any Hong Kong citizens aged 18 or above could cast their votes for or against a list of Chief Executive candidates prepared by the group in both the "nomination stage" and the "civil referendum stage" through a voting system operated by the group. About 19,000 and 65,000 participants cast their votes in the two stages.

The voting system used an instant communication application called Telegram for the voting process, which collected participants' Hong Kong Identity Card numbers, mobile phone numbers and Telegram IDs. Based on the information obtained, the Commissioner took the view that (i) there was no explanation on the purposes and lawful basis of personal data collection; (ii) the identity of the data users / controllers (organisers) was unclear; and (iii) the reliability of the de-identification technology adopted in the voting system was questionable.

2017年2月8日，公署對該團體展開循規審查，並要求該團體立即停止該活動及停用所涉的Telegram通訊程式。

應公署的要求，該團體採取了補救措施以增加該「全民投票」活動的透明度及增強問責性。該團體同時亦停用了原有的投票系統，並以新資料保安措施取代。在活動結束後，該團體向公署提供了一份由獨立專業人士發出的證書證明所收集的個人資料已被銷毀。

On 8 February 2017, the PCPD commenced a compliance check against the group, calling for the immediate suspension of the activity and the "Telegram" communication application.

In response to the PCPD's request, the group took remedial actions to enhance the transparency and accountability of the "civil referendum" activity. It also suspended the voting system and replaced it with new data security measures. After completion of the activity, the group provided the PCPD with an independent certification of the erasure of personal data.

(ii) 載有11,000名未經加密的病人資料的資訊科技系統遭入侵

一個政府部門向公署通報，表示其資訊科技系統遭入侵。遭入侵的伺服器載有超過11,000個未經加密的臨時檔案，當中載有病人的個人資料包括：姓名、香港身份證號碼、性別、病歷記錄及評估資料。在發現事件後，該部門立即停用該伺服器，並在其後的調查中發現只有少於4%的臨時檔案可能被黑客存取或下載。

根據該部門的調查，有關的臨時檔案是由一個程式設計介面所產生。由於程式故障，該些檔案在使用完成後卻沒有被立即銷毀。雖然該部門早於數個月前已得悉有關的程式故障，並已進行了第一批的檔案銷毀行動，但餘下的該些檔案仍可遭入侵。

在內部調查過程中，該部門找出了系統的保安漏洞並進行修復。同時，該部門在恢復使用其資訊科技系統前，對此進行了全面性的保安風險評估及私隱影響評估，並建議和制定了以下的長期措施以防止日後再發生類似事件：

- 為增強系統的保安，於一年內轉移其資訊科技系統至政府資訊科技總監辦公室提供的「電子政府基建服務」平台；
- 爭取使用資訊科技顧問服務，以增強其系統保安及監察；及
- 爭取資源強化內部資訊科技支援隊伍，以減少對外判商的依賴。

(ii) IT system containing over 11,000 unencrypted patients' records being hacked

A government department reported to the PCPD that its IT system had been hacked. The intruded server contained over 11,000 unencrypted temporary files, which included patients' personal data like their names, Hong Kong Identity Card numbers, gender, clinical histories and assessments. The department suspended the server immediately, and its subsequent investigation revealed that less than 4% of the temporary files might have been accessed or downloaded by the hacker.

The department's investigation also revealed that the temporary files were generated by an Application Programming Interface which was not deleted immediately after use, owing to a programming bug. Although the programming bug had already come to the department's knowledge several months before and the department had since conducted the first batch deletion, the remaining files were still susceptible to hacking.

The department identified the security vulnerability during the investigation and subsequently rectified the programming bug. It also conducted a comprehensive security risk assessment and privacy impact assessment before the resumption of its IT system. The following long-term measures were recommended and devised to prevent recurrence of similar incidents:

- Migrate the IT system to the e-Government Infrastructure Service provided by the Office of the Government Chief Information Officer in one year with a view to enhancing system security;
- Acquire an IT security consultancy service to enhance system security and monitoring; and
- Acquire resources to strengthen the in-house support team and minimise the reliance on its contractors.

B. 主動調查

(i) 遺失載有選委及選民個人資料的手提電腦

在2017年行政長官選舉翌日(即2017年3月27日),有關部門(處方)發現在2017年行政長官選舉的後備場地亞洲國際博覽館遺失了兩部手提電腦:第一部手提電腦載有約1,200名選舉委員會委員(選委)的姓名;第二部手提電腦則載有約378萬名包括選委的地方選區選民(選民)的姓名、身份證號碼、其所屬選區和界別及地址。

由於該些手提電腦載有的個人資料數量龐大並引起社會廣泛關注,私隱專員就事件展開調查[1]。

調查結果

為確保調查的準確性、縝密性及秉持一貫公平執法的原則,公署除多次向處方蒐集詳細事實資料外,亦徵詢電腦保安事故協調中心和香港警務處網絡安全及科技罪案調查科的專家、以及海外保障資料機構(包括美國聯邦貿易委員會、Israeli Law, Information and Technology Authority(ILITA)、加拿大私隱專員公署、新西蘭私隱專員公署及英國資訊專員辦公室、澳洲私隱專員公署)的類似經驗,反覆求證和深入討論所涉的事實和法律觀點。

公署的調查顯示處方(i)沒有充分檢視和評估在行政長官選舉中應否繼續使用和備存於便攜式儲存裝置(包括手提電腦)內全體選民資料的必要和私隱風險;(ii)沒有列明便攜式儲存裝置(包括手提電腦)儲存選民個人資料的清晰政策及內部指引;(iii)沒有向所有職員提供在行政長官選舉中保障選民資料的詳

[1] 調查報告於2017年6月12日發表。私隱專員亦出席了2017年6月19日舉行的立法會政制事務委員會會議。

B. PCPD INITIATED INVESTIGATIONS

(i) Loss of Notebook Computers containing Personal Data of Election Committee Members and Electors

On the day following the 2017 Chief Executive Election (namely 27 March 2017), the office concerned (office) found the loss of two notebook computers kept in Asia World-Expo, the fallback venue of the 2017 Chief Executive Election. The first notebook computer contained the names of about 1,200 Election Committee members, and the second notebook computer contained the names, Hong Kong Identity Card numbers, the constituencies in which they were registered, and the addresses of about 3.78 million Geographical Constituencies Electors, including Election Committee members.

In light of the voluminous personal data involved and the wide attention of the community, the Commissioner initiated an investigation[1].

Result of Investigation

To ensure the accuracy and thoroughness of the investigation and impartial enforcement of the law, PCPD collected detailed factual information from the office, and sought advice of experts from Hong Kong Computer Emergency Response Team Coordination Centre, Cyber Security and Technology Crime Bureau of Hong Kong Police Force, and the overseas data protection authorities (including Federal Trade Commission, the Israeli Law, Information and Technology Authority (ILITA), the Office of the Privacy Commissioner of Canada, the Office of the Privacy Commissioner of New Zealand, the Information Commissioner's Office in the United Kingdom, and the Office of the Australian Information Commissioner) for verifying and examining the factual and legal issues involved.

The investigation revealed that the office (i) did not fully review and evaluate the necessity and privacy risk of continuing to use and store all Electors' data in portable storage devices (including notebook computers) for the Chief Executive Election; (ii) did not set out clear policies or internal guidelines regarding the storage of Electors' personal data in portable storage devices (including notebook computers); (iii) did not provide all staff with detailed guidelines to protect Electors' personal data

[1] The investigation report was published on 12 June 2017. The Commissioner also attended the meeting of the Panel on Mainland Affairs of the Legislative Council held on 19 June 2017.

細指引；(iv)容許職員共用啓動已經加密的選民資料查詢系統的密碼和粗疏處理密碼；以及(v)後備場地的實體保安安排有欠周詳。

for the Chief Executive Elections; (iv) allowed staff to share passwords for activating the encrypted Voter Information Enquiry System and handle passwords without extreme care; and (v) had deficiencies in its physical security measures at the fallback venue.

第一部手提電腦

第一部手提電腦只載有選委的姓名，而有關資料已刊登在可供公眾查閱的選舉委員會正式委員登記冊內，公眾亦可在網上閱覽，屬公開資料，加上姓名本身不屬敏感的個人資料，私隱專員認為即使遺失第一部手提電腦而令選委的姓名外洩，為選委造成損害的機會不大。

此外，由於選委可於行政長官選舉中投票，私隱專員認為處方將選委姓名下載於第一部手提電腦以記錄補發選委名牌的做法可以接受。而在有關情況下，處方就載有個人資料（選委的姓名）的第一部手提電腦所採取的保安措施（包括以密碼保護資料及將有關電腦存放在已上鎖的房間內）尚屬足夠。私隱專員因而裁定處方沒有因遺失第一部手提電腦而違反保障資料第4(1)項「資料保安」原則。

The First Notebook Computer

The first notebook computer contained the names of Election Committee members only. Such information was available to the public in the Election Committee Final Register, and could also be viewed online. As an Election Committee member's name was public data, and given that a name in itself is not considered sensitive personal data, the Commissioner took the view that even if the names of Election Committee members were leaked as a result of the loss of the first notebook computer, harm would unlikely be done to the Election Committee members.

Moreover, as the Election Committee members could vote at the Chief Executive Election, the Commissioner considered it acceptable for the office to download the names of the Election Committee members to the first notebook computer for the purpose of recording re-issuance of name badges. The security measures (including using passwords to protect the data and storing the computer concerned in a locked room) taken by the office to protect the personal data (Election Committee members' names) stored in the first notebook computer were also considered adequate in the circumstances. Therefore, the Commissioner concluded that the office did not contravene DPP 4(1) (Data Security Principle) for the loss of the first notebook computer.

第二部手提電腦

第二部手提電腦除儲存可供公眾於正式選民登記冊查閱的全體選民姓名、地址外，還載有不作公開查閱兼屬敏感個人資料的選民身份證號碼。考慮過所有有關事實、情況和專家意見後，私隱專員認為有關第二部手提電腦遺失個案的案情獨特，亦沒有先例可援。雖然所涉及選民的個人資料已經過多重加密儲存，資料外洩風險低，但處方應可避免遺失載有全體選民個人資料的第二部手提電腦，因而引起的關注可以理解。

The Second Notebook Computer

The second notebook computer however contained, in addition to the name and address available to the public in the Final Register of Electors, the Hong Kong Identity Card numbers of all Electors, which are considered sensitive personal data and not accessible by members of the public. After considering all the facts and circumstances of the case and experts' opinions, the Commissioner found that the circumstances relating to the loss of the second notebook computer are unique and unprecedented. Although the personal data of the Electors involved had already undergone multiple layers of encryption and the chance of leakage was low, the loss of the second notebook computer containing the personal data of all Electors could have been avoided. Hence, the privacy concerns arising therefrom were understandable.

私隱專員認為，處方在檢視及審批使用載有選民的非公開並屬敏感的個人資料的查詢系統一事非常粗疏，蕭規曹隨，只顧依從過往做法，卻沒有適時按情況檢視或更新，從而制訂一套完善的制度。為了提供所聲稱的服務而備存全體選民的個人資料所帶來的效益與引申的風險亦不合符比例。所採取的保安措施與資料的敏感程度和資料洩漏可能引致的損害，平衡失據。調查結果顯示處方對個人資料私隱保障認知、警覺性和內部溝通不足，應用和實施各項指引的規例欠缺清晰或沒有依從，未能滿足大眾的期望，沒有按實際情況和需要採取所有合理地切實可行的步驟，確保選民的個人資料受保障而不受意外的喪失所影響，因而違反條例下的保障資料第4(1)原則。

The Commissioner was of the view that the assessment and approval of the use of the enquiry system containing the Electors' data, which included personal data not being open to the public and sensitive, was especially not well thought out or adaptive to the circumstances of the case. The office simply followed past practices and failed to review, update or appraise the existing mechanism in a timely manner and in light of the circumstances. The claimed effectiveness of the need for storing personal data of all Electors was not proportional to the associated risks. The security measures adopted by the office were not proportional to the degree of sensitivity of the data and the harm that might result from a data security incident either. The result of the investigation showed that the office lacked the requisite awareness and vigilance expected of it in protecting personal data, rules of application and implementation of various guidelines were not clearly set out or followed, internal communication was less than effective, and hence failed to take all reasonably practicable steps in consideration of the actual circumstances and needs to ensure that the Electors' personal data was protected from accidental loss, thereby contravened Data Protection Principle (DPP) 4(1) under the Ordinance.

執行通知及建議

Enforcement Notice and Recommendations

私隱專員向處方送達執行通知，指令處方(i)禁止為行政長官選舉活動下載或使用地方選區選民的個人資料(姓名及地址除外)以作查詢之用並就此項指令定期向有關職員發出通告；(ii)制定有關選舉活動中就處理個人資料的內部指引，當中須包括技術和實體保安措施及使用手提電腦或其他便攜式儲存裝置的行政措施；以及(iii)實施確保職員遵從這些內部指引的措施。

The Commissioner served an Enforcement Notice on the office directing it to (i) prohibit the download or use of Geographical Constituencies Electors' personal data (except their names and addresses) for the purpose of handling enquiries in Chief Executive Elections and issue notice on this to the relevant staff members on a regular basis; (ii) set internal guidelines for the processing of personal data in all election-related activities (including technical and physical security measures, and administrative measures on the use of notebook computers and other portable storage devices); and (iii) implement effective measures to ensure staff members' compliance with the above policies and guidelines.

此外，私隱專員亦建議處方須確保在選舉中只採用「需要」的個人資料；嚴格審批及監察所有載有選民個人資料的系統的下載或複製；使用便攜式儲存裝置儲存選民個人資料時採取有效的技術保安措施；制訂、有系統地檢視及更新個人資料保安政策；適時進行私隱影響評估以及由上而下切實推行私隱管理系統，以重建選民的信心。

The Commissioner also recommended that the office should use only "necessary" personal data in different elections; strictly review, approve, and monitor the download and copying of systems containing Electors' personal data; adopt effective technical security measures when storing Electors' personal data; formulate, systematically review, and update personal data security policy; conduct Privacy Impact Assessment in a timely fashion; and adopt the Privacy Management Programme as a top-down organisational imperative to regain the confidence and trust of the Electors.

(ii) 一間玩具製造商遭網絡攻擊引致6.6百萬兒童資料外洩

一間玩具製造商的客戶數據庫及伺服器遭黑客入侵，外洩全球約5百萬名家長和6.6百萬名相關兒童的個人資料，包括家長的姓名、電郵地址、郵寄地址、IP地址、密碼、用以獲取密碼的秘密提示問題與答案和下載記錄；兒童的姓名、性別和完整出生日期；以及聊天和語音訊息、照片和布告板內容。

由於事件牽涉的人數眾多，且涉及兒童，加上該公司的總部設於香港，私隱專員就事件主動展開調查，以確定該公司有否違反保障資料第4(1)原則（即保安原則）和第1(1)原則（即收集資料原則）。公署按國際間私隱執法機構一貫的合作安排，與其他地區的私隱機關互相通報調查進度。

調查結果

調查發現事件不涉及香港客戶。在資料保安方面，調查顯示受黑客攻擊的系統欠缺最新的保安措施，反映該公司的資訊系統保安政策及指引並不追溯至舊系統。此外，該公司沒有監察資訊系統安全政策及指引的落實情況、定期檢視以及因應最新科技發展更新相關政策及指引。該公司亦沒有採取一些基本的保安措施，包括採取防止SQL插入攻擊的措施、安裝網上應用系統防火牆、及加密包括姓名、電郵地址、郵寄地址和出生日期等個人資料。

私隱專員因此認為該公司沒有採取所有合理地切實可行的步驟，確保個人資料受保障而不受未獲准許的查閱所影響，故此違反條例下的保障資料第4(1)原則。

在資料收集方面，私隱專員質疑為何該公司在登記兒童帳戶時須收集兒童完整的出生日期。該公司解釋若干遊戲的評分需要按兒童的年齡來計算。私隱專員認為該公司就遊戲評分這一目的而言，收集兒童的年齡或出生年份已足夠。故此，該公司因過度收集兒童的完整出生日期而違反保障資料第1(1)原則。

(ii) Cyberattack on a toy maker leaked personal data of 6.6 million children

The customer databases and servers of a toy maker were hacked, leading to the leak of the personal data of about 5 million parents and 6.6 million related children. The data included parents' names, email addresses, mailing addresses, IP addresses, passwords, secret questions and answers for retrieving the passwords, and download history; children's names, gender, and full dates of birth; and chat and voice messages, photos, and bulletin board postings.

As the incident involved a large number of data subjects including children and the company was based in Hong Kong, the Commissioner initiated an investigation into the incident to ascertain whether the company had contravened the data security principle and data collection principle. In accordance with the international practice and cooperation arrangement, PCPD kept privacy enforcement authorities in other jurisdictions informed of the investigation progress.

Findings

The investigation showed that no Hong Kong customers were involved in the incident. In respect of data security, the investigation revealed that the systems under attack were not protected by new security measures. The company's IT security policies and guidelines did not retroact upon systems that had existed before those policies and guidelines were introduced. Moreover, the company failed to monitor the implementation of its IT security policies and guidelines and did not regularly review and update them in light of the latest technology development. The company also did not take certain basic security measures, including countermeasures to prevent SQL injections, installing web application firewalls, and encrypting personal data such as names, email addresses, mailing addresses, and dates of birth, etc.

The Commissioner therefore determined that the company had contravened DPP 4(1) under the Ordinance for failing to take all reasonably practicable steps to ensure that the personal data was protected against unauthorised access.

Regarding data collection, the Commissioner questioned the need to collect children's full dates of birth for child account registrations. The company explained that it required the children's age for grading their performance in certain games. The Commissioner took the view that the company needed only the children's age or their years of birth for the purpose of grading, and therefore determined that the company had contravened DPP 1(1) (Data Collection Principle) by collecting excessively the dates and months of birth of the children.

補救措施

事件發生後，該公司採取了以下一系列的補救措施，包括：

- 加強防禦措施以免資料遭不獲授權的查閱，例如採取嚴謹的認證管控措施、定期進行網絡掃描等；
- 制定新的資料保安政策；
- 成立由集團主席為首的資料保安管治委員會，負責作出有關資料保安政策的決定、監督政策的實施和定期進行檢討；及
- 停止在登記帳戶時收集兒童的出生月份及日期。

私隱專員就該公司已採取補救措施糾正該些違反感到滿意，因此未有向該公司送達執行通知。考慮到事件可能對資料當事人尤其是兒童帶來深遠的負面影響，私隱專員已向該公司作出警告，如該公司日後在類似情況中沒有遵守條例的相關規定，私隱專員會採取執法行動。

Remedial actions

After the incident, the company took the following remedial actions:

- Enhanced its protective measures against unauthorised data access by administering strict authentication controls, conducting regular network scans, etc.;
- Promulgated a new Data Security Policy;
- Formed a Data Security Governance Board chaired by the Group Chairman to decide on matters concerning the Data Security Policy, oversee the Policy's implementation, and review it periodically; and
- Stopped collecting the children's dates and months of birth during account registration.

The Commissioner was satisfied that the company's contraventions had been remedied and therefore no enforcement notice was served to the company. Considering that the incident could have far-reaching adverse impact on the affected data subjects, the children in particular, the Commissioner warned the company that enforcement action against it would be considered should it fail to comply with the Ordinance in similar circumstances in future.

資料外洩通報

資料外洩事故一般是指資料使用者懷疑其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。公署敦請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。若私隱專員決定進行循規審查，會書面通知相關的資料使用者，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88宗資料外洩事故通報（37宗來自公營機構；51宗來自私營機構），牽涉3,859,338名人士的個人資料。公署對肇事機構展開循規審查行動。

DATA BREACH NOTIFICATIONS

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 DPP4. Data users are strongly advised to give a formal data breach notification (DBN) to the affected data subjects, the Commissioner, and other relevant parties after a data breach has occurred.

Upon receipt of a DBN from a data user (which could be submitted through the designated DBN form or other means of communication), the PCPD would assess the information provided in the DBN and decide whether or not a compliance check is warranted. If a compliance check is to be conducted, the Commissioner would alert the data user in writing, pointing out the apparent deficiency and inviting him, where appropriate, to take remedial actions to prevent a recurrence of the incident.

During the report year, the PCPD received 88 DBNs (37 from the public sector and 51 from the private sector), affecting 3,859,338 individuals. The PCPD conducted a compliance check in each of these 88 incidents.

個人資料的核對程序

核對程序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專員的同意，不得進行核對程序。

在本年度，私隱專員共收到20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。

DATA MATCHING PROCEDURE

A matching procedure is a process by which personal data collected for one purpose is compared electronically with personal data collected for other purposes with 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 Commissioner's consent.

During the report year, the Commissioner received a total of 20 applications for approval to carry out matching procedures. All of the applications came from government departments and public-sector organisations.

以下是私隱專員核准進行個人資料核對程序的部分個案：

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

提出要求者 Requesting Party	核准的資料核對程序詳情 Details of the Approved Data Matching Procedures
市區重建局 Urban Renewal Authority	把市區重建局從資助出售房屋計劃成功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，以避免公共房屋資源遭到濫用。 Comparing the personal data collected by the Urban Renewal Authority from the successful applicants and listed family members of Subsidised Sale Flat Scheme with the personal data collected by the Hong Kong Housing Authority from the owners, tenants and applicants for subsidised housing, in order to prevent the 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葛量洪獎學基金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受助人收集的個人資料互相比較，以確保正確運用葛量洪獎學基金。 Comparing the personal data collected by the Working Family and Student Financial Assistance Agency from the applicants of Grantham Maintenance Grants with the personal data collected by the Social Welfare Department from the beneficiaries of Comprehensive Social Security Assistance, in order to ensure proper spending of funds under Grantham Maintenance Grants.
社會福利署 Social Welfare Department	把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，與入境事務處收集的個人資料互相比較，以識別哪些受助人是否曾於付款年度內離開香港或廣東超過所寬限的日數。 Comparing the personal data collected by the Social Welfare Department from the beneficiaries of Comprehensive Social Security Assistance and Social Security Allowance with the personal data collected by the Immigration Department, in order to identify whether the beneficiaries whose temporary absence from Hong Kong or Guangdong in a payment year have exceeded the permissible limit.
香港房屋委員會 Hong Kong Housing Authority	把香港房屋委員會從綠表置居先導計劃及居者有其屋計劃申請人收集的個人資料，與其從各個資助房屋計劃中所收集的個人資料互相比較，以確定申請人的資格。 Comparing the personal data collected by Housing Authority from applicants of the Green Form Home Ownership Pilot Scheme and Home Ownership Scheme with the personal data collected in Housing Authority's various subsidised housing schemes, in order to assess the eligibility of the applicants.