私隱專員的話
PRIVACY COMMISSIONER'S MESSAGE

黃繼兒
香港個人資料私隱專員
Stephen Kai-yi WONG
Privacy Commissioner for Personal Data,
Hong Kong

在過去一年，環球的個人資料保障形勢經歷重大改變.....我們作為規管者，一直有檢視法例，亦會參考《通用數據保障條例》。在檢視法例的過程中，我們亦會小心考慮必要的因素，例如改革的合法目的及迫切需要、擬議的更改與達致合法目的之間的相稱性、是否有其他實用和有效的方法處理這個問題、環球的資料私隱保障形勢、本地情況、所有持份者的利益，以及社會大眾的利益。

Global personal data protection landscape underwent significant changes in the past year.....We as a regulator have been reviewing our legislation with a view to better protecting and respecting personal data privacy right, with references to the GDPR, too. In the review process, we also took heed of imperative factors such as the legitimate purpose and pressing need of the reform, the proportionality between the proposed change and the pursuance of the legitimate purpose, whether there are any other practical and effective means to address the problem, the global data privacy landscape, the local circumstances, the interest of all stakeholders and the interest of the community at large.

2019-2020年度是個人資料私隱專員公署（私隱公署）自1996年成立近四分一個世紀以來，充滿新穎挑戰的一年。以投訴個案為例，我們接獲11,220宗投訴，創紀錄新高。即使我們不計算數以千計自2019年6月以來由社會事件而導致的空前「起底」事件的投訴，以及多宗引起社會廣泛關注的私隱相關事件，投訴數字仍有3,848宗，按年上升105%（2018-19年度為1,878宗）。多方的挑戰不單考驗公署在規管上的適應力和毅力，亦令個人資料私隱成為公眾關注的焦點，深化了公眾對如何平衡個人資料私隱權利與其他權益的考量和討論。

2019-20 was a year fraught with novel challenges for the Office of the Privacy Commissioner for Personal Data (PCPD) in its quarter-of-a-century history since its establishment in 1996. Taking the complaint caseload as an example, we received a record high of 11,220 complaints. Even if we discounted the thousands of complaints about unprecedented doxxing arising from social incidents since June 2019 and a number of privacy-related incidents which caused widespread social concerns, there remained 3,848 complaints, representing a 105% year-on-year increase (1,878 complaints in 2018-19). The multi-fold challenges not only put PCPD's regulatory resilience and stamina to the test, but also brought personal data privacy into focus and intensified public deliberations and dialogues about how to balance personal data privacy rights against other competing interests.

我們於2019年初就一間電訊公司外洩38萬名顧客及服務申請者的個人資料的事件發表調查結果之後，隨即獲悉一個政府部門發生資料外洩事故，涉及遺失選民個人資料。雖然這事故規模較小，涉及約8,100名人士，但仍然引起不少關注，因為事件是在發生約30個月後才曝光。2019年12月，私隱公署就一間信貸資料機構的網上認證程序漏洞發表了調查報告，該機構沒有採取所有切實可行的步驟，確保其持有的個人資料受到保障而免受未獲准許或意外的查閱或使用。

Right on the heels of concluding and publishing our investigation results in early 2019 on a telecommunications company having leaked personal data of some 380,000 customers and service applicants, we were hit with another data security breach incident by a government department concerning loss of voters' personal data. Though the scale of this data security breach was much smaller, involving only about 8,100 individuals, it caused no less concern as the incident did not come to light until some 30 months after it had happened. In December 2019, PCPD published an investigation report on the vulnerabilities of a credit reference agency's online authentication procedures caused by its failure to take all practicable steps to ensure that the personal held was protected against unauthorised or accidental access or use.

正如在其他法域區發生的資料外洩事故一樣，人為錯誤（例如惡意軟件、黑客入侵、網絡攻擊或類似情況）總是最常見的單一原因，遠超其他技術因素。不論資料使用者是公營機構或私營企業，採取技術性及機構性措施，充分和適當地培訓及再培訓管理個人資料的人員，以制度化的基礎管理由收集、持有、處理、使用，以至銷毀個人資料的整個流程，均至為重要。

Like so many other data security breach incidents in other jurisdictions, human errors were almost invariably the most common single cause. They trailed much ahead of technical factors such as malware, hacking, cyber security attacks or the like. No matter whether data users are public organisations or private enterprises, technical and organisational measures with sufficiently and appropriately trained and retrained personnel for managing personal data on a cradle-to-grave institutionalised basis from collection, holding, processing, use to destruction of personal data are instrumental.

誠然，以端對端問責系統管理個人資料私隱的整個生命周期是有幫助的，但絕對不能保證資料外洩事故不會發生。人是容易犯錯誤的。黑客入侵和網絡攻擊亦日趨複雜。因此，資料使用者透過數據道德爭取個人對其個人資料管理的信任和信心更為重要。

Admittedly, having an end-to-end accountability system to manage personal data privacy on a life cycle basis does help but it never guarantees no data breach. Humans are prone to making human errors. Hacking and cyber security attacks are becoming more sophisticated day by day. It is therefore all the more important that data users could command the trust and confidence of individuals in their personal data management through data ethics.

私隱公署自2017在香港舉辦國際資料保障及私隱專員研討會（2019年10月改稱為環球私隱議會）以來，一直在區內倡導數據道德。公署預期資料使用者在數據道德下會以尊重、公平及互惠的態度處理個人資料。如資料使用者能展示他們在處理個人資料時不只是依循法律要求，更奉行問責原則，萬一發生資料外洩事故，他們很可能會得到當事人的信任和信心。

PCPD has been pioneering the data ethical approach in the region since we held the International Conference of Data Protection and Privacy Commissioners (renamed as the Global Privacy Assembly (GPA) since October 2019) in 2017 in Hong Kong. Armed with data ethics, data users are expected to handle personal data through the prism of respect, fairness and benefits. In the event of a data security breach, it is probable for data users to manage garnering trust and confidence on the part of the individuals if they could also demonstrate that they take accountability, as opposed to mere compliance with the laws, as the added principle for protecting personal data.

沒有道德地使用個人資料所帶來的後果可以是非常嚴重的。由2019年6月中至2020年3月底，私隱公署接獲及發現接近5,000宗由社會事件引發的「起底」個案。2019年下半年，個人資料被武器化的情況前所未見，不單對個人造成心理傷害和恐嚇，亦煽動他人破壞公共秩序。受害人來自社會各階層。

The consequences of deploying personal data without ethics can be disastrous. Starting from mid-June 2019, PCPD received and uncovered close to 5,000 doxxing cases arising from social incidents as at the end of March 2020. We witnessed in the second half of 2019 unprecedented weaponisation of personal data to cause not only psychological harm but also intimidation of individuals and incitement against public order. Victims came from all walks of life.

如此將個人資料武器化可以說是我們所見最差的使用資料形式，它貶低了人的尊嚴和體統。由於私隱公署沒有刑事調查及檢控的權力，公署在完成初步調查後只能把涉嫌違反《個人資料（私隱）條例》（《私隱條例》）的刑事罪行轉介警方進行刑事調查，如證據充分，則由律政司作出檢控。

Such weaponisation is arguably the worst form of data in action we have ever seen. It derogates from human dignity and decency, too. Not equipped with criminal investigation and prosecution powers, PCPD, upon completion of initial investigations, could only refer suspected criminal offences under the Personal Data (Privacy) Ordinance (the PDPO) to the Police for following up criminal investigations and for prosecutions by the Department of Justice if warranted.

不過，私隱公署確已盡用其現有的法定或行政權力，以減低受害人的傷害。自2019年6月14日接獲這類投訴個案的首月，個案數目已遠超前八年有關網絡欺凌的投訴個案總數。公署因應運作需要成立了一個特別小組，主動搜尋載有非法貼文的網站連結。截至本報告年度為止，我們曾166次去信16個網上平台，促請它們移除2,867條「起底」網站連結，而在我們介入後，1,777條「起底」網站連結已被移除，即62%。我們亦就海外營運的網上平台聯絡海外的資料保障機構、向香港電腦保安事故協調中心尋求其對應機構的協助，並促請海外的網域註冊公司提供我們調查所需的資料。我們多次去信提醒平台營運商，高等法院已發出禁制令(HCA 1957/2019及HCA 2007/2019)，當中分別禁止(i)任何人非法地及故意地公開警員及/或其家人的個人資料，以恐嚇或騷擾他們；及(ii)社交媒體平台協助發布非法的貼文。我們在接獲或發現涉及懷疑違反有關命令的個案時，會轉介律政司跟進。我亦曾傳召一個海外平台的營運商，要求提供上載「起底」貼文的網民的登記資料及IP地址，以供我們調查之用，但該營運商沒有現身。公署為從根源處理「起底」問題，亦透過各種途徑(包括以現場及網上形式)進行公眾教育和推廣活動。

PCPD did, nevertheless, exhaust all its existing powers, statutory or administrative, to contain the harm suffered by the victims. The number of such complaint cases received in the first month since 14 June 2019 well exceeded the total number of complaint cases on cyberbullying in the preceding eight years. A special team was set up to cater for operational needs to proactively search for web links with unlawful postings. As at the end of the reporting year, we wrote to 16 online platforms 166 times urging the taking down of 2,867 doxxing web links, and after our intervention 1,777 doxxing web links, i.e. 62%, were taken down. We also liaised with overseas data protection authorities regarding online platforms operating overseas, sought the assistance of the Hong Kong Computer Emergency Response Team for enlisting help from its counterparts, and urged overseas internet domain registration companies to give us necessary information for our investigations. We repeatedly wrote to remind platform operators that the High Court had granted injunction orders (HCA 1957/2019 and HCA 2007/2019) to, *inter alia*, prohibit respectively (i) persons from unlawfully and wilfully disclosing personal data of police officers and/or their family members, intended or likely to intimidate or harass them; and (ii) social media platforms from assisting in the dissemination of unlawful posts. On receipt or discovery of cases involving suspected violations of the orders, we referred them to the Department of Justice for follow-up. I also summoned the operator of an overseas platform to provide registration information and IP addresses of the netizens who had uploaded the relevant doxxing postings for the purposes of our investigations, although it failed to turn up. In an attempt to tackle the problem of doxxing at its roots, PCPD also carried out public education and promotion programmes through various in-person and electronic channels.

總的來說，要打擊網上「起底」罪行須面對巨大的挑戰。首先，開立網上帳戶並無規定以實名登記，這令到要識別犯罪者至為困難。此外，絕大部分張貼「起底」貼文的平台是在香港以外的地方營運，而《私隱條例》在域外管轄權方面並無明確的條文。即使私隱公署有域外權力，個人資料的移轉是無疆界的，起底者可輕易地將資料由一個法域區轉移至另一個法域區，因此，現時要有效保障個人資料私隱，雙邊、區域性或多邊執法合作更具迫切性。

All in all, tackling online doxxing crimes comes with immense challenges. In the first place, there are no real name registration requirements for online accounts. This makes identifying the culprits most difficult. Besides, most, if not all, of the platforms on which doxxing takes place operate outside of Hong Kong and the PDPO does not have explicit provisions on extra-territorial jurisdiction. Even with extra-territorial powers, personal data sees no border and doxxers may easily migrate from one jurisdiction to another with ease, making bilateral, regional or multilateral enforcement cooperation much more pressing nowadays for effective personal data privacy protection.

事實上，2019年10月環球私隱議會在阿爾巴尼亞地拉那舉行的周年大會上，超過120個資料保障機構通過決議案，推動的議題包括打擊在社交媒體及網上涉及暴力、仇恨言論和極端主張的內容。會上亦通過另一項決議案，顯示跨境執法的重要性。私隱公署一直致力促進與其他私隱執法機構的跨境合作，在2019年5月，公署與澳門個人資料保護辦公室聯席主持第三屆全球私隱執法機關網絡執法人員研討會，共60名來自14個法域區的代表成員參與。同月，公署亦與新加坡個人資料保護委員會在日本簽訂諒解備忘錄，同心協力，進一步加強兩地在個人資料保障方面的合作關係。

As a matter of fact, GPA with more than 120 data protection authorities, adopted a resolution at its annual meeting in Tirana, Albania in October 2019 calling on, *inter alia*, combating violence, hatred and extremist content on social media and on the internet. At that meeting, GPA also underlined the importance of cross-border enforcement by passing another resolution. As part of our continuing effort to foster cross-border cooperation among privacy enforcement authorities, in May 2019 PCPD co-hosted with Macao's Office for Personal Data Protection the 3rd Global Privacy Enforcement Network Enforcement Practitioners' Workshop, which was attended by 60 delegates from 14 jurisdictions around the world. The same month also saw PCPD's signing of a Memorandum of Understanding, in Japan, with Singapore's Personal Data Protection Commission to strengthen cooperation in personal data protection in the two jurisdictions.

我們在國際方面的工作不限於此。私隱公署自2019年一直擔任環球私隱議會的人工智能的道德與數據保障常設工作小組的聯席主席。在這個數據驅動年代，人工智能一直被視為可提供競爭優勢的重要數據工具。我們正積極與小組其他成員合作，在發展和應用人工智能方面提升大眾的意識，以及制定最佳準則和行事方式。

Our work on the international front did not stop here. PCPD has since 2019 been co-chairing the Permanent Working Group on Ethics and Data Protection in Artificial Intelligence of the GPA. We are working earnestly with other members with a view to raising the awareness level and setting best standards and practices in the development and use of AI, which has always been seen as a critical data tool rendering competitive advantage in the data-driven era.

在過去一年，環球的個人資料保障形勢經歷重大改變：改革業務模式、普遍收集及未經同意使用資料、鼓勵涉及個人資料私隱的項目和其他有關資訊及通訊發展的創新做法。歐盟的《通用數據保障條例》於2018年5月25日生效後，引發世界各地進行法律改革浪潮，這並不令人感到意外。我們作為規管者，一直有檢視法例，亦會參考《通用數據保障條例》。在檢視法例的過程中，我們亦會小心考量必要的因素，例如改革的合法目的及迫切需要、擬議的更改與達致合法目的之間的相稱性、是否有其他實用和有效的方法處理這個問題、環球的資料私隱保障形勢、本地情況、所有持份者的利益，以及社會大眾的利益。

Global personal data protection landscape underwent significant changes in the past year, reformed business models, ubiquitous collection and non-consensual use of data, as well as encouraging initiatives involving personal data privacy and other innovative practices in relation to information and communications developments. Triggering a "legislative reform tsunami" around the world was no surprise after the coming into effect of the General Data Protection Regulation (GDPR) in the European Union on 25 May 2018. We as a regulator have been reviewing our legislation with a view to better protecting and respecting personal data privacy right, with reference to the GDPR, too. In the review process, we also took heed of imperative factors such as the legitimate purpose and pressing need of the reform, the proportionality between the proposed change and the pursuance of the legitimate purpose, whether there are any other practical and effective means to address the problem, the global data privacy landscape, the local circumstances, the interest of all stakeholders and the interest of the community at large.

我很高興政府在考慮我們的建議後，在2020年1月公開闡述《私隱條例》的初步修訂方向。初步修訂方向包括私隱公署所建議的較為迫切的議題，當中包括範疇（例如個人資料的定義及對資料處理者的直接規管）、過程（例如賦予公署刑事調查權力及檢控權力，包括提升處理「起底」罪行的權力）、阻嚇作用（例如設立強制性的資料外洩通報機制、賦權公署判處行政罰款及增加刑事罰款的最高款額），以及個人的權利（例如規定機構資料使用者提供個人資料的保留政策及保留時限）。

I am pleased that the Government, having considered our proposals, set out in public in January 2020 the preliminary amendment directions for the PDPO. The preliminary amendment directions encompass the more pressing issues proposed by PCPD relating to the scope (e.g. definition of personal data and direct regulation on data processors), the process (e.g. vesting criminal investigation powers and prosecution powers with PCPD, including enhanced powers to deal with offences like doxxing), the deterrent effect (e.g instituting a mandatory data breach notification system, empowering PCPD to administer administrative fines and increasing the maximum level of criminal fines) as well as the rights of individuals (e.g. requiring organisational data users to provide retention policy and maximum retention period for personal data).

這些方向顯然對改革《私隱條例》十分重要。私隱公署期望就修訂《私隱條例》與所有持份者敲定詳情。這肯定是公署來年的首要工作。

These are certainly the expected directions for significant reforms to the PDPO. PCPD looks forward to firming up details with all stakeholders on how the PDPO should be amended. This would undoubtedly be the top priority of PCPD's work in the coming year.

當個人資料私隱成為社會焦點之時，傳媒的興趣自然增加，我們更加有責任為公眾的利益適時解釋私隱議題。去年，私隱公署共主動發出69份新聞稿，創紀錄新高。此外，我們回應傳媒查詢的數字亦是過去十年最高的。今時今日，人們已習慣隨時隨地接收資訊，因此我們以「陽光中的私隱」作為主題，在不同的社交平台（Instagram, LinkedIn, Twitter及微博）推出全新形象，並更新Facebook專頁和YouTube頻道。我們在這些社交平台上的貼文和短片的對象是年輕一代、大中小微企、專業人士、中國內地和海外的資料保障人員及機構，希望他們能掌握私隱保障方面的最新消息。

When personal data privacy came into sharper focus in society, media interest naturally increased and we found ourselves even more obligated to enhance explainability of privacy issues in the interest of the community in a timely manner. Last year, PCPD took the initiative to issue a total of 69 media statements, setting a record high. In addition, the number of responses we made to media enquiries was the highest in the last decade. In this day and age when people are accustomed to receiving information anytime anywhere, we have launched a brand new image on online social media platforms (Instagram, LinkedIn, Twitter and Weibo), and revamped our Facebook page and YouTube channel, all under the new theme of "Privacy in Sunlight". Our postings and videos on these social media platforms aim to target at the younger generation; micro, small, medium and large enterprises, professionals, data protection personnels and authorities from the mainland and overseas, with a view to enabling them to follow the latest news and updates of the privacy landscape.

2019-20年度的年報中，不得不提2019冠狀病毒病全球大流行。疫情不單對全球的公共健康構成威脅，亦對在保障個人各項資料（例如健康資料、用作接觸追蹤的位置資料等）與快速有效遏止病毒之間應如何取得最佳的平衡帶來挑戰。

It would not be complete for an annual report for 2019-20 without mentioning the COVID-19 pandemic. Not only did the pandemic pose a threat to public health around the globe, it also challenged the best possible balance that should be struck to protect individuals' various data (such as health data, location data for contact tracing, etc) on the one hand and to enable expeditious and effective containment of the virus on the other.

環境瞬息萬變，但我們對保障及尊重個人資料私隱的承諾始終如一。在疫情期間，我們作為規管者會繼續擔當個人資料促進者和保護者的角色，不會忽略保障個人私隱權利的需要，以及促進機構為公眾利益而負責任地使用資料。私隱權是基本人權，但並非絕對權利，必須根據情況予以考慮，並與其他權益作出平衡，包括但不限於公共健康、公共秩序、公眾利益，就其合法性、合理連繫、必要性、相稱性及是否有迫切需要作為考慮準則。

私隱公署在便利採取抗疫措施與保障個人私隱方面堅定實踐這原則。在政府推出抗疫措施之前，我們向不同的政府部門和決策局提供觀察所得，例子包括涉及收集和使用個人資料的現金發放計劃、派發可重用口罩、「保就業」計劃等紓困措施。我們已向政府清楚說明，在考慮所有實際情況後，應嚴格依從保障資料原則行事，包括收集最少的資料、其他對私隱侵犯程度較低的方法（顧及達致合法目的之必要性及相稱性）、保留資料的時間不會超過所需的時間、收集個人資料政策的透明度和可解釋性等。為了便利政府在疫情期間向公眾迅速落實紓困措施，我們快速地處理政府的核對程序申請，有關申請是申請批准把為某目的而收集的市民個人資料以電子方式與為其他目的而收集他們的個人資料作比較。公署亦適時就疫情期間安全使用個人資料向公眾發出建議，包括早於2020年2月的強制檢疫措施所帶來的私隱議題，以及利用社交媒體追蹤潛在的帶病毒人士。當疫情開始影響營商和教育時，公署亦就僱主向僱員收集資料、使用視像會議軟件工具作教育和營商用途、已更為普遍的在家工作安排、兒童私隱等發出建議。

Circumstances always change but our commitment to protecting and respecting personal data privacy does not. In times of a pandemic, we as a regulator continue to serve both as a facilitator and a protector of personal data, without losing sight of the need for protecting individuals privacy right and facilitating responsible use of data in the interest of the public. While privacy is a fundamental human right, it is not an absolute right. It has to be considered and balanced contextually against other competing rights and interests, including but not limited to public health, public order and ultimately, public interests, applying the tests of legitimacy, rational connection, necessity, proportionality and any pressing need.

PCPD put this practice firmly into action to facilitate measures taken to combat the pandemic and to protect individuals' privacy. We provided our observations to various Government departments and bureaux before introducing their measures in combating the pandemic. Examples included relief measures such as Government's Cash Payout Scheme, the reusable masks, the Employment Support Scheme, etc where collection and use of personal data were involved. We made it quite clear to the Government, with all the practical circumstances considered, the data protection principles including minimum data collection, alternatives of less privacy-intrusive measures having regard to the necessity and proportionality for achieving the legitimate purposes, retention of data not longer than is necessary, transparency and explainability of the personal information collection policies, etc., would have to be followed strictly. To facilitate efficient implementation of relief measures for members of the public during the pandemic, we swiftly processed Government's applications for approval to carry out matching procedures where personal data of citizens collected for one purpose was compared electronically with their personal data collected for other purposes. PCPD also issued timely public advisories to facilitate the safe and secure use of personal data during the COVID-19 pandemic, including as early as in February 2020 on privacy issues arising from mandatory quarantine measures and the use of social media for tracking potential carriers of COVID-19. When the pandemic started to impact the way of businesses and education operated, PCPD issued advisories on the collection of data from employees by employers, the use of video-conferencing software tools for education or for businesses, the much more prevalent work-from-home arrangements, children privacy, etc.

個人資料在對抗這次疫情中扮演著不可或缺的角色。私隱公署透過環球私隱議會與其他法域區的規管者在規管方面互相合作和協調。公署積極參與環球私隱議會2019冠狀病毒病應變工作組的新興私隱議題分組的工作。我們在與其他成員的合作下，正整理證據和個案研究，編纂有關最佳行事方式的概要，以便在為公眾利益而使用資料之餘，仍能提供公眾預期的保障。公署亦繼續向該工作組所管理的網上資源圖書館提供有關資料保障及2019冠狀病毒病的最新指引和資訊。

為了減低疫情的干擾，持續舉辦公眾教育活動，我們改以網上模式為企業及個人提供專業研習班和講座，並採取足夠的資料保安措施。在特別工作安排和積極採取預防措施下，私隱公署能夠為公眾提供接近正常的服務。公署為員工提供安全可靠的資訊科技支援，在有需要時員工可以在家有效順暢地工作。我希望當你收到這本年報時，疫情已經完全受控。

今年是我五年任期的最後一年。我感到很榮幸及高興，身為人權律師能夠為公眾履行我的法定職責，尤其秉持法治中「無人能凌駕法律」的精神公正地執法，全不考慮違反《私隱條例》人士的政治背景和取向。這全賴私隱公署一群努力不懈的同事全力支持。我亦衷心感謝個人資料（私隱）諮詢委員會及科技發展常務委員會的成員，我從他們身上獲益良多。展望將來，在像香港般的數據驅動的智慧城市，保障個人資料私隱的工作會面對艱巨的挑戰，我期望與你們一起迎接這些新穎挑戰。

黃繼兒
大律師
香港個人資料私隱專員
2020年7月

Personal data has played an indispensable role in combating this pandemic. PCPD joined regulators from other jurisdictions through GPA for regulatory collaboration and coordination. PCPD actively played a role in the Sub-Group on Emerging Privacy Issues under the COVID-19 Response Taskforce of GPA. With other members' collaboration, we were collating evidence and case studies and would compile a compendium of best practices on enabling the use of data in the public interest and still providing the protections the public expects. PCPD also kept contributing latest guidance and information on data protection and COVID-19 to an online Resources Library managed by the Taskforce.

To minimise the disruption by the COVID-19 pandemic to our ongoing public education initiatives, PCPD offered professional workshops and seminars to enterprises and individuals in online mode, with sufficient data security measures in place. Under special work arrangements and with active preventive measures adopted, my office managed to provide overall close-to-normal public services with reliable and secure IT support enabling smooth and efficient operation of staff working from home when necessary. I just wish that when this report reaches you, the pandemic will have been fully under control.

This is the fifth and final year of my 5-year tenure. It has been a distinct privilege and real pleasure for me, being a human rights lawyer in the public service, to be able and real pleasure for me to discharge my statutory duties, particularly in enforcing the law fairly, upholding the Rule of Law in that nobody is above the law, and having no regard to the political background and orientation of those who contravene the PDPO. I could not have done it without the relentless efforts and staunch support of my colleagues. My sincere thanks also go to members of the Personal Data (Privacy) Advisory Committee and the Standing Committee on Technological Developments from whom I have learnt a great deal by picking their brains and unlocking their wealth of expertise. Looking ahead, I envisage formidable challenges to personal data privacy protection in a data-driven smart city like Hong Kong and look forward to working with you all to rise to these novel challenges.

Stephen Kai-yi WONG
Barrister
Privacy Commissioner for Personal Data, Hong Kong
July 2020