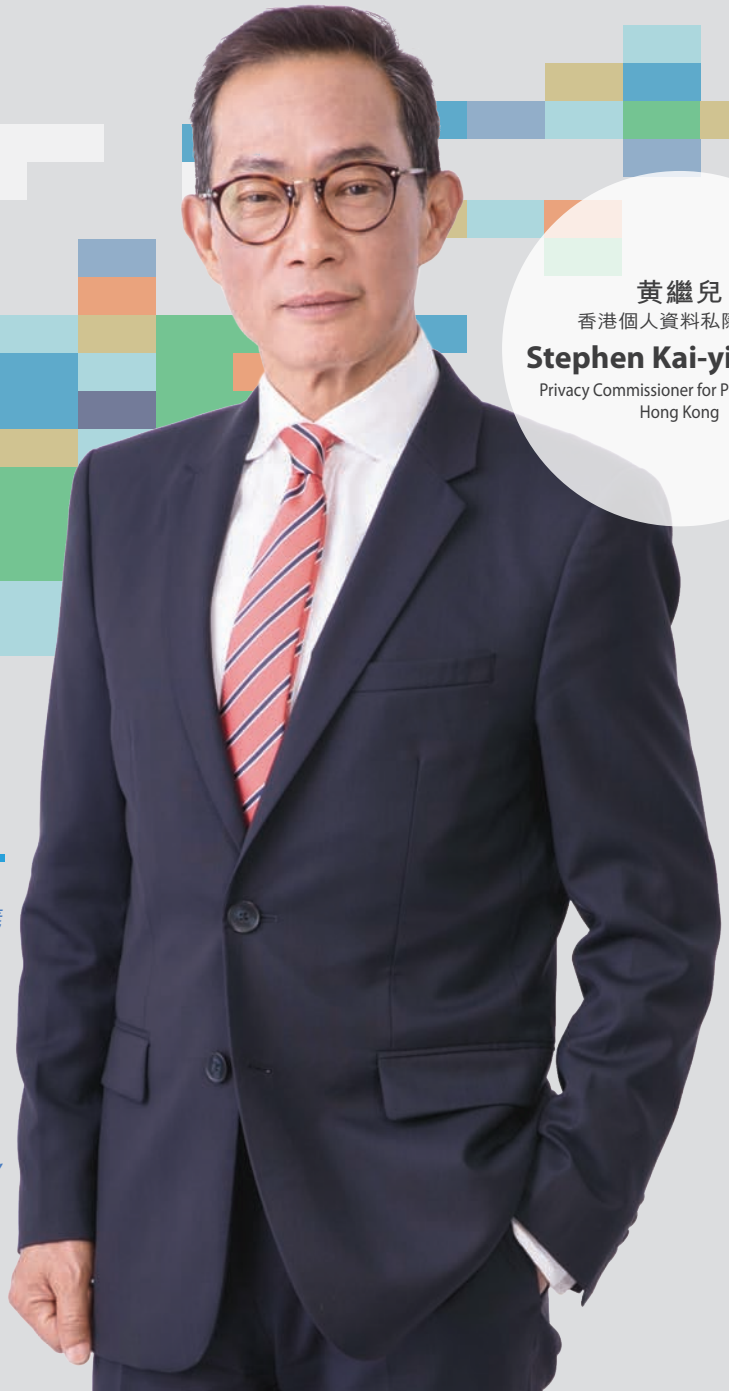
PRIVACY COMMISSIONER'S MESSAGE

私隱專員的話



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

「數據倫理和道德價值一般集中於公平、尊重及互惠。實際上是涉及真正的選擇、有意義的同意、沒有偏見或歧視，以及個人與機構之間的公平交易。」

"Data ethical values typically centre at fairness, respect and mutual benefits. In practical terms, they involve genuine choices, meaningful consent, no bias or discrimination and fair exchange between individuals and organisations."

這是我擔任香港個人資料私隱專員以來的第三份年報。2017-18 年度同樣是多姿多采、成果豐碩的一年。

This is my third annual report as Hong Kong's Privacy Commissioner for Personal Data. The year under review (2017-18) was another eventful and fruitful year.

數碼變革、資料生態系統演化的挑戰

DIGITAL REVOLUTION AND DATA ECOSYSTEMS EVOLUTION CHALLENGES

自 2015 年上任以來，我見證了數碼變革及資料生態系統的蛻變過程，資料是透過一系列的基礎設施、分析工具及應用程式而收集和分析。儘管可以從中獲得真知灼見，但資料生態系統確實以我們難以想像的速度深深地影響著我們的日常生活。我們的「數碼身份」不斷變化。通訊及科技不斷創新，大數據、物聯網、雲計算、數據分析、機械人技術、機器學習、人工智能等重塑了人類及其生活，由休閒到學習、由無現金購物到開放銀行、由直銷電話到程式化廣告、由徵求同意到不知情的行為追蹤或個人資料彙編、由數據探勘到數據管治、由個人評核檔案到公共設施和醫療、由網絡安全到資料共享。透過服務及程式窺探人們的通訊，例如強迫人們接納被監視才可以讀取網上內容，這種情況將會受到 2019 年生效的歐盟電子私隱條例規管，該條例旨在確保讀取網上資訊不用依賴入侵式監視措施。資訊及通訊科技不斷發展，總會帶來私隱顧慮。

Since I took office in 2015, I have witnessed parts of metamorphosis of the digital revolution and the evolution of data ecosystems, whereby data is captured and analysed through a collection of infrastructure, analytics and applications. Whilst useful insights are produced, data ecosystems do have a significant impact on our daily lives at a speed that we could not have dreamt of. Our "digital-self" is increasingly changing what it means to human beings. The continuing innovations in communication and technology in areas like big data, internet of things, cloud computing, data analytics, robotics, machine learning and artificial intelligence have helped re-shape human beings and the world they live in, from leisure to learning, from cashless shopping to open banking, from direct marketing calls to programmatic advertising, from invited consent to uninformed behavioural tracking or profiling, from data mining to data governance, from personal appraisal files to public utilities and care, and from cybersecurity to sharing of data. Snooping on people's communications through services and apps, such as forcing people to accept being monitored in exchange for accessing content online, will be addressed by the forthcoming EU ePrivacy regulation scheduled to come into effect in 2019, with a view to ensuring that access to information on the internet does not depend on invasive surveillance practices. Emerging ICT developments invariably bring with them privacy considerations.

正如其他法域區一樣，香港法律第 486 章《個人資料（私隱）條例》（《私隱條例》）亦大致根據 1980 年經濟合作與發展組織的私隱保障及個人資料跨境流通指引及 1995 年歐盟的資料保障指令而制定，當中列明公署的權力與責任。這是以原則為本、科技中立的條例，好處之一是顧及私隱上複雜細微的性質，在千變萬化的資訊及通訊科技發展和社會規範中，容許某程度的彈性，讓私隱在不同情況下獲得保障。但看來有些新興科技超越了限制，對這些基礎原則帶來挑戰。

Like other jurisdictions having their regulation generally based on the 1980 OECD Guidelines on the protection of Privacy and Trans-border Flows of Personal Data and the 1995 EU Data Protection Directive, the Personal Data (Privacy) Ordinance (the Ordinance) (Cap 486, Laws of Hong Kong), in which our powers and responsibilities are set out, is principle-based and technology-neutral. One of the benefits of having a principle-based and technology-neutral legislation is that it recognises the complex and nuanced nature of privacy, and allows a degree of flexibility in how privacy can be protected in varying contexts, alongside evolving ICT developments and social norms. Seemingly some of the emerging technologies are stretching their limits and are posing challenges to these underlying principles upon which the legislation is based.

國家及區域層面的海外規管機構為應對這些挑戰，已修改其法例及規管架構，明顯的例子是 2018 年 5 月 25 日生效的歐盟《通用數據保障條例》。這些資料保障機關很多已有權在行政上施加民事罰款，但香港是沒有這項法定權力的。《通用數據保障條例》是關於人類的尊嚴及消費者的信任，消費者應可控制其個人資料，而企業則可在公平的環境

Overseas regulatory authorities, national and regional, have responded to these challenges by reforming or revising their regulation and regulatory frameworks, notably the EU's General Data Protection Regulation coming into force on 25 May 2018. It should be noted that many of these data protection authorities have already had the power to, *inter alia*, impose civil monetary penalties administratively, a statutory power which we in Hong Kong do not have. The GDPR is about the dignity of human beings and the trust

營運。最重要是，《通用數據保障條例》引入了問責原則，這標誌著資料保障文化的轉變。

of the consumers, who should have the control over their personal data while businesses benefit from a level playing field. Most importantly, the GDPR introduces the principle of accountability, signifying a gear shift in the culture of data protection.

價值、文化、法律、倫理和道德

VALUES, CULTURES, LAW AND ETHICS

除了執法保障個人資料私隱權利外，有人提出思考在數碼年代保障私隱和資料所必備的價值，包括尊嚴、在數據驅動生活中的尊重，或稱為數據倫理和道德。2017 年 9 月在香港舉行的「第 39 屆國際資料保障及私隱專員會議」，以「連繫西方與東方保障、尊重資料私隱」為主題，期間討論了這些價值及相關的私隱文化。

Enforcement of the law to protect personal data privacy rights aside, calls have been made to reflect on our values in the digital era that underpin privacy and data protection, including dignity, respect in data driven life, otherwise known as data ethics. At the "39th International Conference of Data Protection and Privacy Commissioners" held in Hong Kong in September 2017, with the theme of "Connecting West with East in Protecting and Respecting Data Privacy", some of these values and the associated privacy cultures were canvassed.

私隱權在香港屬於基本人權，並受到 1991 年《香港人權法案條例》（第 383 章）及中國香港特別行政區的《基本法》所保護。這項權利被視為享受其他權利的先決條件及其他權利的基礎，包括言論自由。這些權利有時無可避免地互相矛盾。規管者有責任作出適當的平衡。

Privacy right is a fundamental human right in Hong Kong, protected also under the 1991 Hong Kong Bill of Rights Ordinance, Cap 383; and the Basic Law of the Hong Kong Special Administrative Region of the PRC. It is accepted as a pre-condition for enjoyment of, and the basis for many other different rights, including the freedom of expression. Inevitably, there are instances where these rights may conflict with one another. Regulators are duty bound to strike the proper balance.

去年在香港就東、西方私隱文化進行的討論和分享顯示，有些法域區基於傳統觀念、政治及社會發展，其傳統文化並沒有私隱這個概念。但在經濟改革後，人們的意識和期望逐漸提高，個人資料私隱保障亦愈益受到重視。不過，在某些法域區，私隱保障仍然是公民權利重於個人的基本人權。

The sharing and discussions in Hong Kong last year about privacy cultures of the West and East revealed that in some jurisdictions the concept of privacy virtually had not existed in their traditional culture, owing to their conventional philosophy, political and social development. But the demand for personal data privacy protection was picking up its momentum after going through economic reforms whereby awareness and expectation of their people gradually gathered force. Yet the notion of privacy protection was still more a civil right than a fundamental human right of an individual in certain jurisdictions.

雖然問責性開始佔一席位，但遵從資料私隱法律仍然是各持份者，包括公營機構及政府目前的主流態度。

Compliance with data privacy laws is currently the mainstream attitude among our stakeholders, public organisations and the government included, the resonance of accountability starting to tune up though.

倫理和道德是共同的社會價值。在充滿變化的時期，數據倫理和道德是培育個人資料保障的基石。歐盟已開展「倫理和道德倡議」，作為開始重點。例如，他們支持「需要有道德地設計人工智能」這個理念。

Ethics are shared societal values. Data ethics are the bedrock for nurturing and flourishing personal data protection in times of change. The EU has rolled out the "Ethics Initiative" as a key starting point. It supports, for example, the idea that artificial intelligence needs to be ethically designed.

數據倫理和道德價值一般集中於公平、尊重及互惠。實際上是涉及真正的選擇、有意義的同意、沒有偏見或歧視，以及個人與機構之間的公平交易。

Data ethical values typically centre at fairness, respect and mutual benefits. In practical terms, they involve genuine choices, meaningful consent, no bias or discrimination and fair exchange between individuals and organisations.

信任、參與和尊重

我們認為規管者應培養真正尊重個人資料的文化，確保資料保障實際有效及具持續性。正是這個原因，我們在 2017-18 年度把工作重點放於數據倫理和道德這個議題上。我們委託顧問進行研究，識別「道德的」或「公平的」資料處理的意思、道德的資料管理標準，及鼓勵企業秉持數據倫理和道德、建立信任及為所有持份者帶來附加價值的因素。該研究亦希望為機構開發具道德的資料影響評估框架，把數據倫理和道德付諸實行。

在管理個人資料方面，我們要求持份者在展開重大的項目前進行「私隱影響評估」。我們鼓勵他們實施「貫徹私隱的設計」，由始至終把個人資料保障徹底融入每個營運程序。總的來說，我們鼓勵持份者在所有程序中依從「私隱管理系統」。公署已為此刊發專題資料單張及為中小企開設熱線。

採用這些系統和程序，可以帶來透明度和問責性，可以減少對消費者帶來的驚訝，從而建立及維持信任。換句話說，信任帶來參與，繼而培養尊重。尊重建基於倫理和道德，而倫理和道德推動信任。

TRUST, PARTICIPATION AND RESPECT

We believe that regulators should cultivate a culture of genuine respect for personal data to ensure its protection is realistically effective and sustainable. It is precisely against this background that throughout 2017-18, we placed significant emphasis on the issue of data ethics. We commissioned a consultancy project aiming to identify the meaning of "ethical" or "fair" data processing, standard for ethical data stewardship and motivators for businesses to embrace data ethics, establish trust and generate added values for all stakeholders. It also aimed to develop an ethical data impact assessment framework for organisations to put data ethics into practice.

In managing personal data, we ask stakeholders to conduct "privacy impact assessment" in major assignments they take on. We encourage them to implement "privacy by design" such that personal data protection is weaved into business processes from cradle to grave. All in all, an end-to-end "Privacy Management Programme" is what we encourage all to follow. A specific information leaflet and hotline for the SMEs were also put in place.

With these programmes and processes, transparency and accountability would be in action. Surprises to consumers would be minimised. Trust, the very social fabrics for a functioning society, would also be built and sustained through this virtuous cycle. In perhaps simpler terms, trust draws participation, which in turn breeds respect. Respect is built on ethics and ethics drive trust.

資料外洩事故與網絡安全

去年，我們透過循規審查及／或調查處理了 116 宗資料外洩事故通報（按年增加 30%）。在香港，資料外洩事故通報並非強制性，完全屬於自願性質。關於多間旅行社遭網絡攻擊，資料遭黑客盜取，我們迅速地輔導他們採取即時補救行動，以遏止對消費者可能造成的損失；並採取措施重建消費者的信心及減少消費者變節。這一直是我們處理資料外洩事故通報的標準初步行動。

過往，網絡罪犯以不同方式作出破壞，例如病毒攻擊及網站篡改，通常只為了個人的滿足。現時，他們利用勒索軟件以獲取金錢利益，攻擊資料庫以取得資料作出售用途。其他網絡攻擊亦以商業電郵詐騙的形式出現。儘管我們不是網絡規管者，但我們會與其他持份者合作，致力應對資料保安的問題，尤其關注是否已採取法律規定的所有合理的步驟。就此，我們特別要感謝不同商會、貿易協會、傳媒、警方、金融管理局、政府資訊科技總監及生產力促進局的專業意見和協作。由於網絡攻擊無分國界，資料可儲存於不同法域區的多個伺服器中，循規審查及調

DATA BREACHES AND CYBERSECURITY

Last year, we attended to 116 data breach notifications (a 30% increase year-on-year) by way of compliance checks or/and investigations. It should be noted that data breach notifications in Hong Kong are not mandatory but entirely voluntary. As in the case of travel agents having been cyber-attacked and data hacked, we spared no time in engaging them to take immediate remedial actions to contain the possible damage to customers and steps to re-establish their consumers' confidence and reduce customers' defection. This has been our standard initial response to data breach notifications.

In the past, cybercriminals operated by all forms of vandalism, such as virus attack and webpage defacement, often for personal gratification only. Nowadays, ransomwares are employed for financial gain; databases are attacked for sale of data obtained. Other cyberattacks also take the form of a business email compromise. Whilst we are not a cyber regulator, partnership and concerted efforts with other stakeholders in the ecosystems to address the issues of data security vulnerabilities are warranted, especially whether all reasonable steps have been taken as required by the law. For this, we would like to thank, in particular, various chambers of commerce, trade associations, the media, Police Force, Hong Kong Monetary Authority, Office of Government Chief Information Officer and Productivity Council for their helpful expert advice and

查亦需要香港以外的規管者協助。我們亦衷心感謝其他法域區（包括澳洲、加拿大、以色列、澳門、荷蘭、新西蘭、菲律賓、新加坡、英國及美國）同業的鼎力支持和協助。

collaboration. As cyberattacks are borderless and data can be stored in multiple servers in different jurisdictions, compliance checks and investigations also call for the assistance of regulators outside Hong Kong. We also record our appreciation and gratitude for the most helpful support and succour tendered by our counterparts in other jurisdictions, including those in Australia, Canada, Israel, Macau, the Netherlands, New Zealand, the Philippines, Singapore, UK and USA.

推廣及教育

我們繼續致力於推廣及教育的工作，這是我們的主要職責之一。標準或度身訂造的講座、研討會、會議及培訓課程的舉辦次數較以往為多。這些講座通常是因應特定行業、主題及年齡而舉辦的。預計在公署的會議室擴充後，受眾人數會大幅提升。

PROMOTION AND EDUCATION

We continued to make relentless efforts on the promotion and education front, they being our other principal responsibilities. Record number of standard or customised lectures, talks, seminars, symposiums and training courses were organised and delivered. These lectures and talks were often industry-specific, topic-specific and age-specific. It is expected that the number of audience will markedly increase as the capacity of our in-house lecture room is due to be doubled.

我們於 2017 年 7 月首次出版中文書《注意！這是我的個人資料私隱》，以淺白的表達形式，闡述保障資料原則的基本概念，讓普羅大眾容易理解。

The publication of our book ever published in Chinese language in July 2017 entitled "*Watch Out! This is my personal data privacy*" (a translation) was another case in point. It sought to explain the basics of personal data privacy principles in a manner that men and women walking in the streets of Mong Kok would be able to understand.

歐盟是香港第二大的貿易夥伴，而《通用數據保障條例》下的域外應用則規定只要香港企業涉及收集和處理處於歐盟國家的人士（不只是歐盟公民）的個人資料，便須遵從《通用數據保障條例》的規定。在《通用數據保障條例》於 2018 年 5 月 25 日生效前兩個月，我們已刊發資訊冊子，深獲好評。

As the EU is Hong Kong's second largest trading partner, the new GDPR's extra-territorial effect suggests that as long as Hong Kong enterprises collect and process personal data of any individuals, not just EU citizens, who are located in an EU country, they should be prepared to comply with the requirements. Two months before the GDPR came into force on 25 May 2018, we had published an information booklet, which was well received.

對外聯繫

我們除了繼續與世界各地的私隱同業加強跨境聯繫及互通性之外，亦與內地的相關機構和學者建立工作關係，尤其是在「一帶一路」和「大灣區」的項目上推動香港作為國家的數據樞紐及有關網上數據糾紛的調解中心。

EXTERNAL CONNECTIONS

Whilst we continued to strengthen our cross-border ties and interoperability with privacy landscape architects and designers around the world, we made cross-boundary inroads and established work relationship with the relevant authorities and academia in the mainland of China, particularly in advocating the attributes of Hong Kong as the data hub and online data-related disputes resolution centre within the country for the "Belt and Road" and "Greater Bay Area" initiatives.

鼓勵和參與

我們的主要法定責任仍然是透過審查和調查公正地執行資料保障法律（不論是在接獲投訴後或主動進行）。我們在這方面不遺餘力。不過，我們的目標並非要提高檢控數字。我們是要在有人違反保障資料原則但不涉及刑事罪行時，處理投訴及不滿的根源、透過調停或調解解決糾紛、在適當時候採取有關各方均滿意的補救行動。為了對投訴人公平，

INCENTIVISING AND ENGAGING

It remains our primary statutory duty to fairly enforce the data protection law, through checks and investigations, whether upon receipt of complaints or self-initiated where appropriate. We spare no sticks in this respect. We do not, however, aim to soar up prosecution figures. We do seek to address the root of the complaints and grievances, resolve the disputes by way of conciliation or mediation, and come up with remedial actions agreeable to parties concerned in good time in cases where

如我們決定不進行調查，我們會在可行的情況下盡快向他們解釋原因。自 2016 年初，這些個案中，我們全部皆於接獲投訴後 45 日內把決定通知投訴人，完全符合法定要求。總的來說，我們在六個月內完成處理逾九成的投訴個案。

data protection principles are breached, which are not in and of themselves criminal offences. In case we decide not to carry out investigation, for fairness to the complainants, we endeavour to explain as soon as practicable to them the reasons for our decision. Since early 2016, in 100% of such cases, we have managed to inform the complainants of such decisions within 45 days after receiving their complaints, having fully met the statutory requirement. Overall, we concluded over 90% of complaint cases within 6 months.

阻嚇性的懲罰，不論多重，似乎對防止日後的違法行為成效不彰；如懲罰的阻嚇性不足，情況會更糟。資源緊絀是各地規管者所面對的共同限制。規管者應訂立策略性的緩急次序，並以結果為本的取向有效地履行其法定職責。儘管他們有懲處權力，但亦應就循規和良好的行事方式提供指引、實際協助（包括資料審計過程）及支援。正面方法亦包括具建設性的參與。

Deterrent sanctions, however heavy, do not appear to have pronounced effect on future behaviour violating the law; worse still where the sanctions are not deterrent enough. The common constraint around the world is that regulators have meagre resources. Regulators should set strategic priorities and adopt result-based approaches to discharge their statutory duties effectively. Whilst carrying a big stick, they should also provide guidelines, practical assistance (including data audit processes) and support for compliance and good practices. The carrots should also take the form of constructive engagement.

透過鼓勵性的諮詢、參與、坦誠交流及監管彈性，讓持份者參與，尤其是私營機構，讓它們「做得正確」是我們去年的首要工作。我很高興告訴大家，反應和回應都令人鼓舞。

Engaging the stakeholders, private organisations in particular, to "get it right" topped our priorities last year, through incentivising consultation, participation, frank exchange and providing support for regulatory sandboxes. I am happy to report that the response and feedback were most encouraging.

個人資料生態系統的倫理和道德

ETHICS IN PERSONAL DATA ECOSYSTEMS

個人資料（私隱）諮詢委員會及科技發展常務委員會的成員在過去一年對我們的工作作出了寶貴貢獻，我希望藉此機會向他們致以衷心的謝意。當然，我亦要感謝公署一群精明機敏、鞠躬盡瘁的同事一直以來的支持，縱使不時遇上重重考驗，仍然努力不懈、盡心盡力地將日益複雜和繁重的工作做好。

I would like to take this opportunity to register my sincere thanks to members of the Personal Data (Privacy) Advisory Committee and the Standing Committee on Technological Developments for their most invaluable contribution to our work in the past year. Credits must also go to the astute colleagues in my office for their unfailing support, exemplary efforts and commendable commitment, without which the increasingly complex and heavy work load on their plates, sometimes under trying circumstances, could not have been dealt with.

隨著環球的私隱法律框架及形勢的轉變，以及公眾對個人資料的收集、使用、保安及查閱的意識有所提高，現時是推動資料保障及尊重資料的重要時刻。公私營機構作為資料使用者、控制者或處理者，在思想及行動上均需要超越純粹循規。問責性已成為資料管治的規範，而一套全新的相關道德及管理標準正在籌劃中。我期望繼續與所有持份者、委員會成員及同事並肩迎接未來的挑戰和機遇。

This is a significant time for data protection and respect for data in the wake of the global changes in the privacy legal frameworks and landscape, as well as increased awareness and public interest in the collection, use, security and access to personal data. Being data users, controllers or processors, public and private organisations need to think and act out of the box of compliance *simpliciter*. Accountability has become the norm for data governance; and a novel set of related ethical standards and stewardship is on the drawing board. I look forward to continuing to work with all stakeholders, committee members and colleagues in embracing further challenges, and opportunities.

黃繼兒

香港個人資料私隱專員

Stephen Kai-yi WONG

Privacy Commissioner for Personal Data,
Hong Kong