PRIVACY COMMISSIONER'S MESSAGE
私隱專員的話

香港的公司及機構在這個數碼主導經濟的年代應作好準備，採納主動的數據管理作為企業價值、道德及責任，把法律要求融入以風險為本、可驗證及可執行的企業行事方式和管控措施，以應對全球的規管改變；實行最新的業務模式、數碼化、全球化，並確保資料保障、可持續性及信任。

Companies and organisations in Hong Kong should be well poised to adopt proactive data management as corporate digital values, ethics and responsibilities in this era of data driven economy, translating legal requirements into risk-based, verifiable and enforceable corporate practices and controls, to address regulatory changes worldwide; enable updated business models, digitalisation, globalisation and ensure data protection, sustainability and trust.

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 2018-19 年度，《通用數據保障條例》生效，不單對歐盟帶來一定影響，亦對環球的私隱規管架構和形勢帶來一些改變。該條例對傳統的資料保障作出更新，亦清楚訂明歐盟以外的機構須在指明的情況下遵從規例。該條例實在開創了新趨勢，是改變的催化劑。此外，香港和世界各地發生了不少大型的資料外洩事故，顯示提升資料保安已成為機構的迫切工作。公眾對數據管治的關注亦因這些事件而大幅增加。

During the year under review (2018-19), the EU General Data Protection Regulation (GDPR) came into effect, making quite an impact not only on the EU, but the global privacy regulatory frameworks and landscapes. It was indeed a trendsetter and a catalyst for change, given its updated data protection conventionally and the explicit requirement of compliance by organisations established outside EU in specified circumstances. In addition, a number of large-scale data breach incidents took place both in Hong Kong and in international arena, indicating that enhancing data security has now become a pressing task for organisations. Public concerns about data governance were also significantly heightened as a result.

執行法律

我們去年接獲 1,878 宗投訴，較上一年增加 16%。在接獲的投訴中，71.8% 是投訴私營機構（1,348 宗），主要涉及銀行及財務公司、物業管理公司，以及交通運輸公司。政府部門及公共機構約佔 12%（225 宗），主要涉及醫院或醫療機構、警務處，以及房屋管理機構。我們接獲與資訊科技有關的投訴有明顯上升的趨勢，升幅達 102%。有關資訊科技的投訴中，關於在互聯網上披露或洩漏個人資料的投訴宗數大幅上升超過三倍，而涉及社交網絡或智能手機應用程式的投訴，亦顯著上升。

LAW ENFORCEMENT

We received 1,878 complaints last year, a 16% increase from the year before. Among the complaints received, 71.8% were on private organisations (1,348 cases), the majority of which included banking and finance institutions, property management companies and transportation companies. The government departments and public organisations accounted for about 12% (225 cases), most of which included healthcare services institutions, the Hong Kong Police Force and housing organisations. The number of complaints received relating to information technology has significantly increased by 102%. Among these IT related complaints, those relating to disclosure or leakage of personal data on the Internet has increased by more than three times, while complaints involving social networking or smartphone applications have also gone up significantly.

去年，公署接獲 113 宗資料外洩事故通報。雖然數字與上一年度相若，似乎沒有大幅飆升，但這些數字卻未足以反映事件性質的複雜和嚴重程度，或受影響人數之多，至於我們在事件中為應付專業團隊而在技術和法律上付出的實質工作之多，更加不用多說了。一如以往，我們與有關機構並肩，協助它們採取即時補救行動，以減輕對受影響人士可能造成的損失。我們亦採取措施協助機構重建顧客的信心，以減少它們因事件而被顧客離棄的情況。

Last year, my office received 113 data breach notifications. While the figure was comparable to that of the preceding year and did not seem to show any alarming trend, it did not reflect the complexity and severity of the nature of the incidents, or the large number of individuals affected, not to mention the substantive technical and legal issues advanced in defence by the professional teams. As always, we worked hand in hand with the relevant organisations and engaged them to take immediate remedial actions to contain the possible damage to the attacked individuals. We also put forward steps to re-establish their consumers' trust with a view to reducing their defection.

雖然個人資料不像其他動產（例如鈔票）或不動產般屬有形的資產，但那亦不足以免除企業沒有妥善地保護資料及沒有在達致有關目的而不再需要該資料時徹底銷毀資料的責任。《個人資料（私隱）條例》（《私隱條例》）規定機構有責任採取所有切實可行的步驟及措施，確保以適當的人士保障消費者的個人資料私隱權。顧客（資料當事人）及監管機構合理地期望企業能擁有一個完備、有效及可行、能適切企業的規模與需要、並可全面實施的私隱循規政策和計劃，以落實法例要求。這些政策和計劃是與有關企業相關的及可擴展的，以及在企業內外皆證明可行的。所要求的保安不單是以系統為本，而且是以數據為本。

The fact that personal data is less tangible than other personalty (e.g. bank notes) or realty does not absolve organisations of their failures to keep it safely and to obliterate it when it is no longer necessary for the fulfilment of the purpose for which the data is or is to be used. Our Personal Data (Privacy) Ordinance (Ordinance) provides that it is the responsibility of organisations to take all practicable steps and measures to ensure, *inter alia*, the right persons are engaged to protect the personal data privacy right of consumers. To give effect to the legal requirements, there is also an expectation of comprehensive, effective and evidenced privacy compliance policies and programmes being put in place, relevant and scalable for the businesses concerned, as well as demonstrable internally and externally. The security required is not merely system-centric but data-centric. This legitimate expectation comes from both the consumers, who are the data subjects, and the regulators.

合理期望

我們作為規管者一直向所有持份者（尤其是作為資料使用者的機構）強調，個人資料不屬於任何機構，而是屬於被收集資料的人士。因此，個人預期自己有權管控其個人資料是完全合理的。當然，純粹因為個人的資料私隱而鎖上資料是不會對公眾有利。在這個數碼主導的經濟中，大數據與資訊及通訊科技不斷發展，科學進步和社交互動帶來了巨大的利益。我們的重點是在資料保障與各方面的利益和權利之間取得平衡。

事實上，儘管資料保障法例不斷被修訂更新，但資訊及通訊科技的發展速度總是超越規管架構的組成。因此，單是符合規管要求是不足以有效地保障資料私隱及達到個人對私隱保障的期望。很多人因而認為資料保障法例應包含私隱問責性。

數據管治

良好的數據管理和管治或問責性的概念已多方面反映在很多法域的新法例中，例如歐盟的《通用數據保障條例》。雖然《私隱條例》尚未包含類似的問責原則，但香港的公司及機構在這個數碼主導經濟的年代應作好準備，採納主動的數據管理作為企業價值、道德及責任，把法律要求融入以風險為本、可證實及可執行的企業行事方式和管控措施，以應對環球的規管改變；實行最新的業務模式、數碼化、全球化，並確保資料保障、可持續性及信任。

當問責性開始佔一席位，在遵循法規之外輔以數據道德，在充滿變化的時期，成為培育資料保障的基石。數據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、透明度、沒有偏見或歧視，以及機構與個人之間的公平磋商或交易。

由於使用資訊及通訊科技會帶來私隱風險，我們合理地預期機構會實施恰當的政策及措施，以辨識、評估和減低私隱及資料保安的風險。機構透過採納道德數據管理框架，在計劃及進行數據處理活動時會考慮所有持份者的權利、利益和自由。持份者不單包括機構的客戶和顧客，亦包括受數據處理活動影響的其他人士，以及整個社會。

LEGITIMATE EXPECTATION

We as regulator have been stressing to all stakeholders, especially organisations as data users, that personal data does not belong to any organisations, but the individuals from whom the data is collected. With that in mind, it is entirely legitimate for individuals to expect that they are entitled to have control over it. Of course, it would not be in the interest of the public to have data locked up merely because of individuals' data privacy. We see the tremendous benefits brought about by scientific advancement and social interactions in this data-driven economy that keeps growing in parallel with Big Data and ICT developments. All we are talking about is to strike a balance between data protection and a variety of competing interests and rights.

Indeed, despite relentless attempts to revamp data protection laws, the ICT developments invariably outpace the formulation of regulatory framework. As a result, meeting regulatory requirements alone would not be effective enough to adequately protect data privacy, and live up to individuals' expectations of privacy protection. It is therefore widely believed that data protection laws should embody privacy accountability.

DATA STEWARDSHIP

The idea of good data stewardship and governance, or accountability has in many ways been reflected, if not incorporated, in the new laws and regulations of many jurisdictions, to say the least the EU GDPR. While similar principle of accountability is yet to be provided for in our Ordinance, companies and organisations in Hong Kong should be well poised to adopt proactive data management as corporate digital values, ethics and responsibilities in this era of data driven economy, translating legal requirements into risk-based, verifiable and enforceable corporate practices and controls, to address regulatory changes worldwide; enable updated business models, digitalisation, globalisation and ensure data protection, sustainability and trust.

Whilst resonance of accountability has started to tune up, complementing compliance with the law by adopting data ethics will form the bedrock for nurturing and flourishing data protection in times of change. Data ethical values typically centre at fairness, respect and mutual benefits. In practical terms, they involve genuine choices, meaningful consent, transparency, no bias or discrimination and fair negotiation or exchange on a level playing field between organisations and individuals.

Given the privacy risks that may arise from the use of modern ICT, organisations are reasonably expected to implement proper policies and measures to identify, assess and mitigate privacy and data security risks. By adopting an ethical data stewardship framework, an organisation is expected to take into account the rights, interests and freedoms of all stakeholders in planning and conducting its data processing activities. The stakeholders do not include only the clients and customers of the organisation, but also other individuals that may be impacted by the data processing activities, as well as society as a whole.

在報告年度內，公署發布「處理數據的正當性」研究項目的報告，題為「中國香港可採用的道德問責框架」，倡議以數據管理問責要素及價值彌合法例要求和持份者期望兩者之間的落差。同時，自 2014 年以來，我們一直倡議透過私隱管理系統進行範式轉變，在良好的企業管治和高層的承諾下，由符規轉為問責，令法律和良好措施可以更為鞏固。我們修訂了最佳行事方式指引，以具體例子、簡潔圖表及相關問卷／清單範本協助機構建立全面的私隱管理系統。

During the report year, my office released the report of the research "Legitimacy of Data Processing Project", entitled "Ethical Accountability Framework for Hong Kong, China", advocating Data Stewardship Accountability Elements and Values as the solution in bridging the gap between legal requirements and the stakeholders' expectations. Meanwhile, since 2014, we have been advocating a paradigm shift through the Privacy Management Programme (PMP) by which law and good practices could be entrenched, and compliance be transformed to accountability alongside the commitment of the top management in better corporate governance. We have revised the best practice guide with more concrete examples, charts, templates of questionnaire and checklist to assist organisations in constructing a comprehensive PMP of their own.

在 2018 年 10 月於比利時布魯塞爾舉行的第四十屆國際資料保障及私隱專員會議通過了「人工智能的道德及資料保障宣言」，公署是共同提出者之一。大會依據該宣言成立了一個新的常設工作小組，在全球進一步推廣及發展該宣言所指明的指導原則。公署作為該常設工作小組的聯合主席，會繼續與本地及海外的持份者緊密合作，培養尊重私隱的文化和環境。

At the 40th International Conference of Data Protection and Privacy Commissioners held in Brussels in October 2018, a Declaration on Ethics and Data Protection in Artificial Intelligence was passed, of which my office was one of the co-sponsors. A new permanent working group has been set up pursuant to the Declaration to further promote and develop the guiding principles as illustrated in the Declaration across the globe. Being one of the co-chairs of the permanent working group, my office will continue to work closely with stakeholders, both at home and abroad, to nourish a culture and environment that respects privacy.

對外聯繫

我們透過與海外（九個國際會議）及內地（十個區域會議及訪問）的相關機構和學者建立的工作關係，繼續與世界各地的私隱同業加強跨境聯繫及互通性。在面對無疆界的數碼資料流動，要尋求有效的資料保障，各地規管者倘不能達成一個統一框架，便應共同研究一個互通的規管框架。同樣地，國際上與互聯網有關的機構更有理由就如何在個人私隱和保安與普及的內容和服務之間取得最佳平衡達成共識。

EXTERNAL CONNECTIONS

We continued to strengthen our cross-border/boundary ties and interoperability with privacy landscape architects and designers around the world via the established work relationship with the relevant authorities and academia, not only overseas (nine international conferences) but also in the mainland of China (ten regional conferences and visits). In the pursuit of effective data protection while facing the borderless/boundary-less nature of digital data flow, regulators are widely expected to put their heads together for an interoperable regulatory framework, if not a harmonised one. Similarly, international Internet-related organisations will have all the reasons to reach a consensus on how best personal privacy and security with popular content and services could be balanced.

推廣及教育

我們在推廣及教育方面的工作一直不遺餘力地進行。我們除了為公營機構舉辦 201 場講座、研討會、會議及度新訂造課程，亦為不同界別的私營機構舉辦 153 場有關培訓；我們亦為政府部門（本港主要的資料使用者）舉辦了 70 個培訓項目。我個人則作出了 228 場演講。隨著金融科技的發展及其所帶來的影響，我們為營運者和使用者出版了有關金融科技的指引。此外，在報告年度內，我們發出或修訂了一些刊物，包括《資料外洩事故的處理及通報指引》、《私隱管理系統最佳行事方式指引》、《個人資料　由你掌握：

PROMOTION AND EDUCATION

We spared no efforts in promotion and education. In addition to 201 lectures, talks, seminars, symposiums and training courses customised for public organisations and 153 for private sectors, we organised 70 training programmes for government departments, being the major data users in Hong Kong. I personally made 228 speaking engagements. With the growing presence and impact of Fintech, we issued guidance on Fintech for the operators and users. In addition, during the reporting year, we issued or revised the publications including the Guidance on Data Breach Handling and the Giving of Breach Notifications, Privacy Management Programme: A Best Practice Guide, Children Privacy Extras: Personal Data Protection in Your Hands, as well as the

兒童號外篇》，以及處理投訴政策。我們因應內地的發展而就內地的主要個人資料規例所製作的教材，亦即將推出。在與公眾溝通方面，我們共發出 30 份新聞稿、在 171 個場合中回應傳媒查詢，以及接受了 82 次傳媒訪問。

Complaint Handling Policy. We drafted educational materials on major personal data protection regulations in the mainland of China, given its recent developments in this aspect, ready to be issued. For public consumption, we also issued 30 press releases, responded to media enquiries on 171 occasions, and attended 82 media interviews.

條例檢討

有人認為數據是這個年代的新黃金或新石油。機構在沒有完全理解所涉的風險前，已急於收集及儲存個人資料，而它們所保存的大量數據令它們成為網絡攻擊的主要目標。2018 年，環顧國際和本地，航空公司、酒店、社交媒體平台成為網絡攻擊的受害者，事件登上國際頭條。從最近的資料外洩事故、環球的資料保障規例的改革（包括歐盟的《通用數據保障條例》），以及傳媒、社會及立法會的意見（包括 2019 年 5 月 22 日立法會通過的動議）來看，全面檢討《私隱條例》是必要的。

因此，公署正進行全面檢討條例的工作，考慮的因素包括：

(a) 修例工作的合法目的；
(b) 修例工作的迫切需要；
(c) 擬議的更改與要達致的合法目的是否相稱；
(d) 除了透過修訂條例，是否還有其他實際有效的方法處理有關問題；
(e) 環球的資料私隱趨勢；
(f) 本地的情況；
(g) 所有持份者的利益；及
(h) 社會大眾的利益。

REVIEW OF THE ORDINANCE

It is said that data is the new gold or new oil of this era. Without fully appraising the risks involved, organisations are attracted to collect and amass personal data and the massive data organisations retained as a result makes them prime targets for cyber-attacks. In 2018, globally and even locally we witnessed that airlines, hotels, social media platform have fallen prey of cyber-attacks which made international headlines. The recent data breach incidents, complied with the recent global transformation of data protection regulation including the EU GDPR, and views expressed in the media, society and Legislative Council (LegCo) including the motion passed by the LegCo on 22 May 2019 seem to have made a comprehensive review of the Ordinance indispensable.

Against this background, my office was in the process of conducting a comprehensive review of the Ordinance, guided by a consideration of factors including:

(a) the legitimate purpose of the reform;
(b) the pressing need for the reform;
(c) the proportionality between the proposed change and the pursuance of the legitimate purpose;
(d) whether there are any other practical and effective means to address the problem (other than amending the Ordinance);
(e) the global data privacy landscape;
(f) the local circumstances;
(g) the interest of all stakeholders; and
(h) the interest of the community at large.

香港作為區域性的數據樞紐

在「一國兩制」的成功落實和香港獨特及無可取代的優勢得以利用下，我有信心香港能在資訊自由流通與個人資料私隱之間取得平衡，而無損經濟和資訊及通訊科技的發展，從而促進香港發展為區域性的數據樞紐，尤其作為「一帶一路」經濟體和大灣區的經濟、社會及文化發展的關鍵聯繫和主要平台。

HONG KONG AS A REGIONAL DATA HUB

With the successful implementation of "One Country, Two Systems" and capitalisation of Hong Kong's unique and irreplaceable attributes, I am confident that Hong Kong is able to strike a balance between free flow of information and personal data privacy protection without compromising economic and ICT development, so as to facilitate Hong Kong to develop as a regional data hub, as well as a key link and prime platform for economic, social and cultural development particularly in the Belt and Road economies and the Greater Bay Area.

公署會繼續公平執法，加強在教育及宣傳方面的工作，同時在規管框架之外，倡議機構引入私隱管理問責及數據道德標準，以培養保障、尊重私隱和個人資料掌控的文化。我們除了擔當執法者及教育者之外，亦協助機構（包括政府）進行涉及個人資料私隱的工作，包括智慧城市項目及就條例檢討提供建議。

My office will continue to enforce the law fairly and step up its educational and publicity efforts, and at the same time advocate the introduction of privacy management accountability and data ethical standards in organisations, complementing the regulatory framework, so as to foster a culture of protect, respect privacy and personal data control. In addition to our role as enforcer and educator, we will facilitate organisations including the Government on initiatives involving personal data privacy, including the Smart City initiatives and making recommendations on the review of the Ordinance.

面對挑戰

基本上，當個人就其個人資料與機構溝通時，他們並不預期出現令人驚訝的事。個人的期望及他們的行為資料彙編在機構的需求函數中是個常數，要與產品或服務的供應達致平衡，是需要不時作出調整。

THE CHALLENGES AHEAD

Essentially, individuals expect no surprises when they deal with organisations in relation to their personal data. Individuals' expectations, alongside their behavioural profiling, will become a constant in the organisations' demand function and the equilibrium against their supply of products or services will need to be adjusted from time to time.

在涉及感官能力、認知能力、機械人、機器學習、雲服務等技術的廣泛應用下，規管者現時所面對的其中一項挑戰，是如何在法律及道德框架下協助開放和分享個人資料，以可持續的方式從資料中獲取最大益處，而同時又能夠將相關風險和傷害減至最低，與經濟增長創造健康的協同效應，在後數據導向的經濟中找出及確立創新使用個人資料的方法。隨著時間過去，很多我們今天認為屬於私人的資訊或行為，他日不會如是，這幾乎是無可避免的。

One of the challenges that regulators have to continue to meet will be how they could help unlock and share personal data within the legal and ethical frameworks in the midst of widely applied sensory ability, cognition, robotics, machine learning and cloud services, etc., with a view to maximising the benefits of data in a sustainable way, minimising the risks and harms, creating healthy synergy with economic growth, identifying and securing the innovative use of personal data in a post-data-driven economy. It is almost inevitable that much of the information or behavior that we consider private today will not be so as time goes on.

資料保障政策、規例及措施總是落後於資訊及通訊科技的發展。當私隱保障科技繼續在能量和規模方面發展之餘，私隱侵犯技術亦會不斷發展。我們以前不會身處無處不在的監察環境，亦沒有網上社交平台或應用程式，用來達致預料不到的政治結果。不過，個人縱使並非只為追求時尚，而是講求便捷，都會較以前放棄更多的個人資料，這在新興的經濟體中尤其如此。今日不論是規管者或機構所要作出的平衡工作，看來在未來十年內未必可行。

Data protection policies, regulations and practices are invariably lagging behind ICT developments. Whilst privacy-protective technology will continue to grow in power and magnitude, so will privacy-intrusive technology. We have never had ubiquitous surveillance before. Nor have we had Internet social platforms or applications to achieve unexpected political results. That said, individuals will tend to give up more and more of their personal data than before for ease and convenience, if not for being trendy, especially in the emerging economies. The balancing exercise, whether on the part of regulators or organisations, that is working today may not been seen as workable in 10 years' time.

我期望繼續與所有本地和國際公私營機構的持份者、公署委員會成員及同事並肩迎接未來的挑戰和機遇。

I look forward to continuing to work with all stakeholders, public and private, local and inter-regional, as well as 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