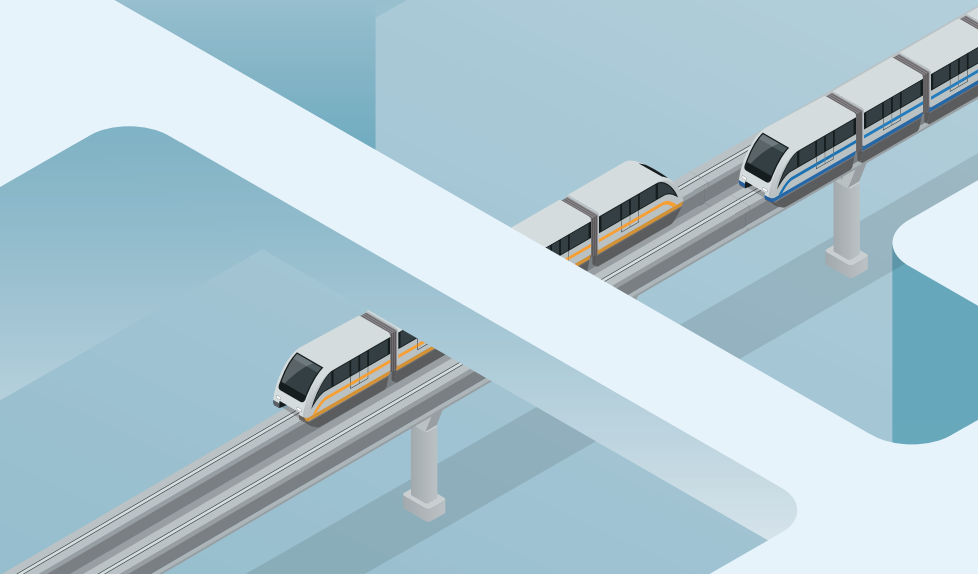




# 加強對外聯繫 STRENGTHENING EXTERNAL CONNECTIONS





## 回應跨法域區的議題

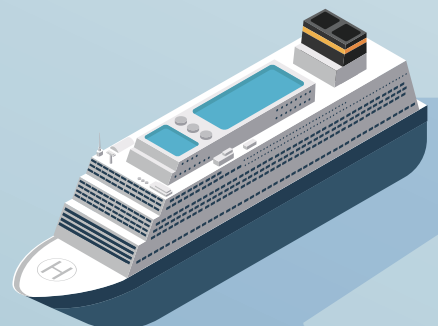
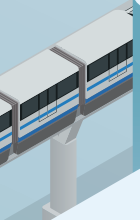
因應最新的本地及國際發展，私隱公署就有關個人資料保障的政策及議題進行研究及分析。

私隱保障跨越不同法域區，需要國際社會共同作出回應。公署與各地資料保障機構和私隱專家保持聯繫和工作關係，以緊貼全球私隱保障的發展和趨勢。

## RESPONDING TO CROSS-JURISDICTION ISSUES

PCPD conducts research and analyses policy issues relating to personal data protection in the light of the latest local and international developments.

Privacy protection has become a cross-jurisdiction issue and thus calls for an international response. PCPD liaises and works with data protection authorities and privacy experts around the world to keep abreast of global developments and trends in privacy protection.



個人資料私隱保障的狀況無論在香港本地或全球各地都在不斷變化、發展。幾乎每天都有涉及私隱的新技術、計劃、產品和服務面世；不同司法管轄區也逐步引入加強個人資料保障的法規和指引。在此背景下，私隱公署必須通過進行研究以緊貼本地和全球的發展，確保我們的法律、指引和規管政策繼續是適用和恰當的，以滿足各持份者的期望和符合國際標準。以下是公署過去一年對全球個人資料保護領域一些重要發展的觀察。

### 在2019冠狀病毒病疫情中就追蹤接觸者與私隱的平衡

自2020年初，2019冠狀病毒病成為全球的焦點。世界衛生組織在2020年3月11日宣布2019冠狀病毒病全球大流行。鑒於此是新病毒、具傳染性和潛在致命性，疫情對全球公共衛生構成了嚴重威脅。世界各國的政府都採取了不同措施來監視和追蹤已確診和疑似的患者，以控制病毒的傳播。在不同的技術方案中，追蹤接觸者的應用程式在防範病毒傳播方面被認為起了關鍵作用。

追蹤接觸者的應用程式利用手提電話的藍牙信號以記錄近距離接觸過彼此的用戶。理論上此方法能使公共衛生官員可以迅速追蹤、通知和隔離與感染者有過密切接觸的人士。一些國家如澳洲、新加坡和英國利用或計劃利用中央處理的模式去收集和處理接觸者資料。同時，另一些國家如奧地利、冰島、印尼、西班牙和瑞士則傾向採用去中心化的模式，將大部分的接觸者資料儲存在用戶的手機上。

去中心化的模式似乎更保障私隱，但有不少衛生機關批評此模式將大大限制可從數據中獲得的洞見，從而阻礙了對抗疫情的措施。

The landscape of personal data privacy protection is dynamic and constantly evolving, locally and globally. New technologies, initiatives, products and services with privacy implications are launched almost every day. Regulations and guidelines for strengthening personal data protection are also introduced or revised in different jurisdictions steadily. Against this background, PCPD must keep abreast of the local and global developments by undertaking research in order to ensure that our own law, guidelines and regulatory policy stay relevant and appropriate, meeting the expectations of stakeholders and the international standard. The following are observations by PCPD in relation to some major developments in the global data protection landscape in the reporting year.

### A BALANCING EXERCISE BETWEEN CONTACT TRACING AND PRIVACY AMIDST COVID-19 PANDEMIC

The world's attention was on COVID-19 since the beginning of 2020. The World Health Organisation characterised COVID-19 as a pandemic on 11 March 2020. Given its novel, contagious and potentially deadly nature, this pandemic posed a grave danger to global public health. Governments around the world implemented different measures to monitor and track confirmed and suspected patients in order to contain the spread of the virus. Amongst other technological solutions, contact-tracing mobile apps were thought to be crucial to containing the spread of the virus.

Contact tracing apps use the Bluetooth signals of mobile phones to keep records of individuals who came into close proximity with each other. This theoretically allows public health officials to quickly notify and quarantine people who have been in close contact with infected persons. Some countries such as Australia, Singapore and the UK used or planned to use a centralised approach for collecting and processing the contact data. Meanwhile, some other countries such as Austria, Iceland, Indonesia, Spain and Switzerland preferred a decentralised approach, under which the contact data would mostly be stored on users' mobile phones.

The decentralised approach would seem more privacy-friendly, but some health authorities criticised that it would significantly limit insights that could be gained from the data, in turn hindering the potential pandemic-fighting measures to be taken.



私隱是一項基本人權，但與生存權不同，它並非絕對的權利。包括私隱公署在內的全球大多數資料保障機構都認為，在面對公共衛生危機時，必須在個人私隱權和更大社會利益之間取得適當的平衡。誠然，如果出於保障資料當事人或其他人士的健康需要，許多資料保障法例包括香港《私隱條例》第59條都豁免了資料使用者遵從使用個人資料的限制。2019冠狀病毒病成為了許多政府如何平衡保障其人民的性命和私隱的嚴峻考驗。在這種特殊情況下，資料保障機構應靈活執法，以便利政府和衛生機關達成對公眾有益且合法的目的。

儘管如此，大多數資料保障機構之間的另一個共識是，應該避免任何被公眾視為極端的措施。所有侵犯私隱的措施對於其所追求的合法目的而言應是必要及合乎比例的，並且仍須遵守其他保障個人資料的原則（例如資料保安與資料最少化）。

為了消除公眾的疑慮及建立信任，政府、衛生機關和其他相關組織應該對建議的追蹤接觸者措施保持透明度和能夠解釋該等措施，說明會否收集個人資料、會收集哪些個人資料，如何使用、分享和轉移個人資料，採取必要的各種資料保安措施，以防止所收集和保存的個人資料在未獲授權下被披露或遺失，以及就疫情後如何處理個人資料訂立清晰政策。

Privacy is a fundamental human right. But unlike the right to life, it is not absolute. Most data protection authorities around the world, including PCPD, believed that individuals' privacy right must be balanced against larger societal interests during a public health crisis. Indeed, many data protection laws, like section 59 of the PDPO, exempt the use limitation requirement of personal data if such use is necessary for safeguarding the health of the data subjects or other individuals. COVID-19 came as an acid test of the "balance skills" of many governments in protecting the lives and privacy of their people. In these exceptional contingencies, data protection authorities should be flexible in law enforcement to facilitate governments and health authorities to pursue legitimate purposes in the interest of the public.

Nonetheless, another consensus among the majority of data protection authorities was that any measures that might seem extreme from the public's point of view should be avoided. All privacy-intrusive measures should be necessary for and proportionate to the legitimate purpose they sought to achieve, and other personal data protection principles (such as data security and data minimisation) should still be complied with.

In order to dispel doubts and build trust, governments, health authorities and other relevant organisations should be transparent about and be able to explain the proposed contact-tracing measures, spelling out whether and what personal data would be collected, how the personal data would be used, shared and transferred, adopting the kinds of data security measures necessary to prevent unauthorised disclosure or loss of the personal data collected and kept, and formulating a clear policy on handling of personal data post-pandemic.

## 個人資料保障的立法浪潮

過去一年，個人資料保障在世界各地發生了巨大的變化。歐盟通過了《通用數據保障條例》並在2018年5月25日實施，成為全球變革的主要催化劑。雖然《通用數據保障條例》並不一定適合所有地區，但其中許多資料保障原則和概念被其他司法管轄區的個人資料保護法例所採納。在美國，《加州消費者私隱保護法》於2020年1月1日生效後大大影響了有關處理個人資料的國際商業慣例。此法案的推出還推動了美國其他州分的監管行動，加速了關於在美國推出綜合私隱法例的討論。印度、印尼、巴西和泰國等一些國家亦首次推出了私隱法例或法案。其他國家如澳洲、新加坡和新西蘭也在更新其私隱法例。

在中國內地方面，儘管目前還沒有全面的個人資料保障法例，但是個人資料仍然受到各種法律和附屬法規的保障。自《網絡安全法》在2017年實施後，有許多保護個人資料的規例和指引在2019年起草、實施或修訂，例如《數據安全管理辦法》（徵求意見稿），《個人信息安全規範》（修訂本）和《兒童個人信息網絡保護規定》（已實施）。

《網絡安全法》的一項重要規定是對個人信息出境的限制，當中規定「關鍵信息基礎設施」的運營者在中國內地運營中收集和產生的個人信息和重要數據須在內地儲存。2019年發布的《個人信息出境安全評估辦法》（徵求意見稿）將個人信息的出境限制擴展至所有網絡運營者，當中包含了所有開發、擁有或使用信息網絡的企業和組織。

在香港，政府於2020年1月在立法會政制事務委員會上闡述了修訂《私隱條例》的六個初步方向。我們預期香港的資料保障水平在未來將會達到新高度。

## LEGISLATIVE TSUNAMI ON PERSONAL DATA PROTECTION

Global personal data protection landscape underwent significant changes in the past year. The passage of the GDPR in the EU, which came into effect on 25 May 2018, was a major catalyst for changes worldwide. While the GDPR might not be one-size-fits-all, many of its principles and concepts on personal data protection have been adopted or adapted into the personal data protection laws by other jurisdictions. In the US, the California Consumer Privacy Act had a major impact on international business practices towards the handling of personal data when it came into effect on 1 January 2020. Its introduction also stirred other US States into regulatory action, and accelerated the dialogue towards an omnibus privacy legislation in the US. Some countries such as India, Indonesia, Brazil and Thailand also introduced privacy laws or bills for the first time. Others like Australia, Singapore and New Zealand were updating their privacy legislation.

For the mainland of China, although it does not yet have a comprehensive piece of personal data protection legislation, personal data is nevertheless protected by a robust assortment of laws and subordinate regulations. After the implementation of the Cybersecurity Law in 2017, a plethora of related regulations and guidelines on personal data protection were drafted, implemented or revised in 2019, such as the Measures for Data Security Management (Consultation Draft), the Personal Information Security Specification (revised) and the Provisions on Cyber Protection of Children's Personal Information (implemented).

An important requirement of the Cybersecurity Law is data localisation, which requires operators of "critical information infrastructure" to store the personal data and important data collected during their operations in the mainland locally. The Measures for Security Assessment for Cross-border Transfer of Personal Information (Consultation Draft) issued in 2019 extended the data localisation requirements to all "network operators", which include all businesses and organisations that develop, own or use information networks.

In Hong Kong, the Government elaborated on its six preliminary directions for the amendment of the PDPO at the Legislative Council Panel on Constitutional Affairs meeting in January 2020. We expect that the data protection standard in Hong Kong will reach new heights in the future.





由於各司法管轄區處於不同的發展階段以及有文化差異的存在，有關個人資料保障的法律要求可能會有所不同。儘管如此，一些新的資料保障概念或要求漸漸受到關注，例如強制性資料外洩事故通報、法例的境外效力、資料的可攜權（將在下面討論）以及資料保障機構可施加行政罰款的權力。全球的私隱法例顯然正共同邁向歐盟的《通用數據保障條例》所設定的新高水平。

### 人臉識別科技

人臉識別科技的應用在世界各地越來越普遍，並且用途廣泛。

人臉識別科技應用的增加引發了對此科技的私隱問題的關注，並促使了一些國家引入法規。在美國，數個州分和城市禁止了在某些情況下使用人臉識別。在中國內地，全國信息安全標準化技術委員會正與內地的科技巨企合作起草有關人臉識別科技的國家標準。在歐盟，歐盟委員會於2020年2月發表了一份有關人工智能的白皮書，當中呼籲歐洲各國就人臉識別科技展開討論以回應社會的關注。

在香港，《私隱條例》是科技中立的，亦非禁制性。隨著人臉識別科技變得越來越普遍，社會各界應多加討論有關使用此科技的適當規例或指引，以便在科技使用者和公眾之間建立信任。

Although the legal requirements in personal data protection may vary in different jurisdictions due to their different cultures and different stages of development, some new data protection concepts or requirements were gaining traction, such as mandatory data breach notification, extra-territorial application of the laws, data portability right (to be discussed below) and the power to impose administrative fines by data protection authorities. There was clearly a perceptible convergence in global privacy regulation towards a new high-water mark set by the GDPR of the EU.

### FACIAL RECOGNITION TECHNOLOGY

Deployment of facial recognition technology is increasingly common around the world.

The increase in deployment of facial recognition technology gave rise to concerns about privacy and prompted regulation in some countries. In the US, several states and cities banned the use of facial recognition in certain situations. In the mainland of China, a national standard on the use of facial recognition technology was being drafted by the National Information Security Standardisation Technical Committee in collaboration with mainland technology companies. In the EU, the European Commission published a white paper on artificial intelligence in February 2020, in which a broad European debate on the use of facial recognition was called for in order to address the concerns of the society.

In Hong Kong, the PDPO is technology neutral and not prohibitive. As facial recognition technology becomes more common, society should have more discussion on the appropriate regulation or guidelines for its use in order to build trust among users of the technology and the general public.

## 資料可攜權日益受到關注

資料可攜權此私隱權在世界各地日益受到重視。自歐盟的《通用數據保障條例》引入資料可攜權為其中一項關鍵私隱權後，澳洲、美國加州、印度、新加坡和泰國等許多司法管轄區亦已經或計劃將此權利納入其法例中。

資料可攜權容許個人將其個人資料以機器可讀的格式從一個機構轉移到另一個機構。資料可攜權與傳統的資料查閱權類似。但是，資料查閱權的成效因為科技日新月異（尤其是電子儲存和處理大量資料的能力的提升）而受到侵蝕。例如，即使個人可以通過下載檔案查閱其個人資料，但這些檔案中的數據對他可能並無意義，加上如果有關數據並非以通用及機器可讀的格式提供，這些數據也可能無法被其他公司進一步使用。

從保障個人資料的角度來看，資料可攜權的目的是令個人對自己的個人資料有更大的控制，並幫助他們將資料轉到其他服務供應商。資料可攜權亦會通過促進數據經濟中的競爭和創新帶來更廣泛的經濟利益。

資料可攜權同時觸及資料保障、消費者保障和競爭事務的監管機構的職權範圍。此外，為了充分發揮資料可攜權的潛力和益處，還需要一套可互操作性的標準。因此，監管機構、標準制定機構和業務經營者有需要跨界別合作。有關這題目的政策討論有望帶來新的氣象，使個人獲得對其個人資料的更大控制，及使企業獲得更多有價值的數據以助創新。

## DATA PORTABILITY RIGHT GAINING TRACTION

Data portability is a privacy right that has gained increasing momentum worldwide. It was one of the key privacy rights introduced in the GDPR of the EU. A number of other jurisdictions such as Australia, California of US, India, Singapore and Thailand have since proposed to incorporate or incorporated data portability right into their legislation.

Data portability right empowers an individual to direct his or her personal data to be transferred from one organisation to another in a machine-readable format. Data portability right is analogous to the traditional data access right. However, advances in technology – particularly improvements in the capacity to store and process vast quantities of data electronically – are eroding the effectiveness of the data access right. For example, even though an individual can access his personal data via a downloadable file, that data may not be meaningful to the individual, and probably cannot be further used by another company if it is not provided in a commonly-used and machine-readable format.

From a personal data protection perspective, the goal of data portability is to increase individuals' control over their own personal data, and to facilitate moving the data to other service providers. The wider economic benefit of data portability right is the promotion of competition and innovation in the data economy.

Data portability right touches on the remits of data protection, consumer protection and competition regulators. In addition, to reap the full potential and benefits of data portability, an interoperable standard for data transfer is needed. Therefore, interdisciplinary collaboration amongst regulators, standard-setting bodies and business operators is warranted. The ongoing policy dialogue on this subject will hopefully bring in a new paradigm in which individuals will gain greater control over their personal data and businesses will obtain more valuable data for innovation.



## 環球私隱議會

環球私隱議會（前稱國際資料保障及私隱專員會議）是全球私隱專員的一個領先平台。私隱專員於2019年10月出席於阿爾巴尼亞地拉那舉行的第四十一屆會議，大會的主題為「趨向一致與連通：在數據年代提升全球數據保障標準」。

私隱專員於大會上，聯同其他成員共同推動多項個人資料保障議題，包括會議組織的未來策略發展方向、打擊在社交媒體及網上涉及暴力、仇恨言論和極端主張內容等。該等議題全獲大會通過。

私隱專員自2018年起成為人工智能的道德與數據保障常設工作小組聯席主席。他於會議上以聯席主席的身份向大會報告最新的工作情況，包括提交就去年大會人工智能的道德與數據保障決議案中的原則及方向而進行的公眾諮詢的結果。

另一方面，私隱公署加入了新的國際執法合作常設小組，並成為亞洲地區的區域推動者，以促進、鼓勵和支持在其地區或語言網絡中的小組成員，並增強其地區或語言網絡成員的聲音和對小組的貢獻。

## GLOBAL PRIVACY ASSEMBLY

Formerly known as the International Conference of Data Protection and Privacy Commissioners (ICDPPC), the Global Privacy Assembly (GPA) is the leading forum for privacy commissioners from around the world. The Privacy Commissioner attended the 41st conference in Tirana, Albania in October 2019. The theme of the conference was “Convergence and Connectivity: Raising Global Data Protection Standards in the Digital Age”.

The Privacy Commissioner, joining forces with other members, promoted a number of resolutions on various personal data protection issues, including ICDPPC’s policy strategy, and combating violent, hatred and extremist content on social media online, etc. All proposed resolutions were adopted at the conference.

The Privacy Commissioner has been a Co-chair of GPA Working Group on Ethics and Data Protection in Artificial Intelligence since 2018. He reported on the latest initiatives of the working group during the conference, including the public consultation results of the principles and directions on data ethics and data protection in artificial intelligence set out at last year’s conference.

Moreover, PCPD had joined the International Enforcement Cooperation Permanent Working Group (IEWG) and become the regional booster of the Asian region, with a view to promoting, encouraging and supporting membership of the IEWG in their geographic region or linguistic network; and amplifying the views and contributions of members of their region or linguistic network to the rest of the group.





## 亞太區私隱機構

「亞太區私隱機構」是亞太區私隱機構建立伙伴關係的主要平台，並就有關私隱的法規、最新科技發展、處理查詢及投訴交流意見。亞太區私隱機構論壇每半年舉行一次。

私隱專員分別於2019年5月及12月，在日本東京及菲律賓宿霧出席第五十一屆及第五十二屆亞太區私隱機構論壇。

私隱專員在第五十一屆亞太區私隱機構論壇，與新加坡個人資料保護委員會副專員簽訂諒解備忘錄，進一步加強兩地就個人資料保障方面的合作關係。

私隱專員在第五十二屆亞太區私隱機構論壇解釋香港社會事件所觸發與個人資料有關的議題及其他事宜，並呼籲加強區域合作，建議建立雙邊或多邊援助機制，並採用國際認可的標準或認證，以減輕跨地區執法的挑戰。

## ASIA PACIFIC PRIVACY AUTHORITIES (APPA)

The APPA is the principal forum for privacy authorities in the Asia Pacific region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. APPA Forum is held twice a year.

The Privacy Commissioner attended the 51st and 52nd APPA Forums, held in Tokyo, Japan and Cebu, the Philippines in May and December 2019 respectively.

In the 51st APPA Forum, the Privacy Commissioner and the Deputy Commissioner of Singapore's Personal Data Protection Commission furthered their warm relations by signing a Memorandum of Understanding to strengthen cooperation in personal data protection in the two jurisdictions.

In the 52nd APPA Forum, the Privacy Commissioner explained the issues relating to personal data arising from social incidents in Hong Kong, and called for strengthening inter-regional collaboration and suggested to develop a bilateral or multilateral assistance mechanism and to adopt an internationally accepted standard or certification to mitigate challenges in cross-region enforcement.





## 全球私隱執法機關網絡

全球私隱執法機關網絡促進私隱執法機構的跨境合作。私隱公署於2019年5月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，研討會的主題為「通力合作 應對數碼時代資料外洩事故新常態」，吸引了60名來自14個司法管轄區(包括澳洲、加拿大、德國、以色列、日本、摩洛哥、新西蘭、菲律賓、新加坡、英國、美國等)的代表團成員，以及消費者保障、司法和警察部隊專家的參與。公署亦有參與每月舉行的電話會議，以促進網絡成員之間的知識交流。

## GLOBAL PRIVACY ENFORCEMENT NETWORK (GPEN)

The GPEN seeks to foster cross-border cooperation among privacy enforcement authorities. In May 2019, PCPD co-hosted 3rd GPEN Enforcement Practitioners' Workshop with the Office for Personal Data Protection (GPDP), Macao. The Workshop, themed on "Collaborate to Take on the New Norm of Data Breaches in the Digital Age", attracted 60 delegates from 14 jurisdictions (including those from Australia, Canada, Germany, Israel, Japan, Morocco, New Zealand, the Philippines, Singapore, the United Kingdom, the United States, etc.), as well as experts in consumer protection, judiciary and police force. PCPD has also participated monthly teleconference for knowledge sharing among GPEN members.

## 與海外及內地資料保障機構及私隱專家的交流

## EXCHANGES WITH OVERSEAS AND MAINLAND DATA PROTECTION AUTHORITIES AND PRIVACY EXPERTS

17-19.05.2019	<p>在杭州出席新興技術與數據治理國際研討會，發表「數字化時代的隱私保護問題」演講 Presentation on "Privacy Protection in the Digital Age" at the International Symposium on Data Governance and Emerging Technologies in Hangzhou, China</p>	
23.05.2019	<p>在韓國延世大學舉辦的亞洲私隱橋樑研討會發表「數碼革命中的資料保護」演講 Presentation on "Data Protection in Digital Revolution" at the Asia Privacy Bridge Forum organised by Yonsei University, Korea</p>	
27-28.06.2019	<p>於2019世界移動通訊大會(上海)中「數據信任與安全高峰論壇」主題環節上發表「數據安全，私隱與信任：數碼生態系統的三大基石」的演講 Presentation on "Data Security, Privacy &amp; Trust: The Three Cornerstones of Digital Ecosystem" in "Data Trust &amp; Security Summit" at the Mobile World Congress Shanghai 2019</p>	
15-16.07.2019	<p>出席由國際私隱專業人員協會於新加坡舉行的2019年亞洲私隱論壇並發表論壇主題演講 Delivered an opening keynote speech for the 2019 Asia Privacy Forum organised by the IAPP in Singapore</p>	



## 接待海外及內地訪客

## RECEPTION OF OVERSEAS AND MAINLAND DELEGATIONS

在報告年度內，私隱公署曾接待以下代表團：

During the reporting year, PCPD received the following delegations:

24.05.2019	<p>接待香港城市大學司法教育與研究中心籌辦之第十四屆中國高級法官研修班課程的學員 Received a group of scholars from the 14th Advanced Programme for Chinese Senior Judges organised by the City University of Hong Kong</p>	
27.05.2019	<p>接待由律政司安排的「法律工作人員普通法訓練計劃」訪問團 Received a delegation of "Common Law Training Scheme" arranged by the Department of Justice</p>	
14.06.2019	<p>接待青海省官員訪問團 Received government officials from Qing Hai Province</p>	
16.10.2019	<p>接待來自國內的高級法官訪問團 Received a delegation of senior judges from the mainland of China</p>	
15.11.2019	<p>接待來自上海的法官訪問團 Received a delegation of judges from Shanghai</p>	