

有責任依法防範、制止和懲治危害國家安全的行為和活動，法庭會嚴格公平地按照《香港國安法》及其他適用法律的條文執行司法工作，不會屈服於任何壓力而作出有罪或無罪的裁決。他強調，無論別人對香港法律制度提出怎樣的說法或評論，有一點社會大眾可以肯定的是，香港的法院及法官將繼續履行憲制責任，以無懼、無偏、無私、無欺的精神，公正有效地主持正義。這一點也是對普通法制度得以在香港延續至為重要。談及司法機構推行新措施的進度，張舉能說，簡稱為「iCMS」的電子訴訟系統已在區域法院的大部分民事法律程序以及裁判法院傳票案件順利推行，並計畫今年內推展至其他級別的法院，尤其重要的是處理大部分繁重民事訴訟的高等法院。

律政司司長林定國致辭時強調，沒有絲毫證據顯示司法機構獨立的司法權在涉及國家安全的案件中受到損害。他說，一般而言，有關國家安全的法庭聆訊全部都是公開進行。更重要的是，法庭就此作出的一切決定和判決都在司法機構的網站公佈，可供免費閱覽。大眾可輕而易舉地瞭解有關法庭程序，以及鑽研法庭所作決定和裁決的理由。林定國重申，政府定必竭盡所能，在能力範圍內採取任何措施確保法官和司法人員能夠無懼威嚇，繼續履行其司法職能。



張舉能檢閱警察儀仗隊



林定國致辭

致力保障個人資料私隱， 促進大灣區之互聯互通

鍾麗玲（大律師、香港個人資料私隱專員）

自回歸祖國以來，香港在國家的大力支持下成功落實「一國兩制」，「一國兩制」原則為香港長期的繁榮穩定及經濟體系提供制度上最佳的保障。香港作為國際金融中心和創新科技樞紐，在國家的強大後盾下，正積極推動數字經濟發展。香港個人資料私隱專員公署（以下簡稱「私隱專員公署」）作為保障個人資料私隱的獨立機構，除了負責推廣保障及尊重個人資料的文化，亦致力推動個人資料的安全流動，為國家以及香港數字經濟的高質量發展，竭盡全力。

一、私隱專員公署的角色和定位

私隱專員公署於1996年8月成立，負責監察香港法例第486章《個人資料（私隱）條例》（以下簡稱「《私

隱條例》）的實施及合規情況。私隱專員公署的工作由個人資料私隱專員（以下簡稱「私隱專員」）負責。公署設有多個部門，包括投訴部、刑事調查部、合規及查詢部、法律部、環球事務及研究部、企業傳訊部及企業支持部。除了主動及公正調查私隱風險顯著的範疇，密切監察《私隱條例》的合規情況，私隱專員公署亦緊貼科技發展，持續留意祖國和國際社會在數據安全、個人信息保護和私隱等方面的最新發展及趨勢，確保公署提供的指引和建議與時俱進，務求為市民大眾、香港特區政府、業界和持份者提供適切的支持，以應對快速發展的科技環境和日益複雜的數據使用場景。

香港以《私隱條例》作為保障個人資料私隱的法律框架。《私隱條例》於一九九六年十二月正式生效，

是亞洲區內最早全面保障個人資料私隱的法例之一。《私隱條例》於二零一二年進行了第一次修訂，引入針對使用個人資料作直接促銷的新規定。及至二零二一年，《私隱條例》進行了第二次修訂，將打擊侵犯個人資料私隱的「起底」（即「人肉搜索」）行為列為刑事罪行。該修訂亦賦予私隱專員法定權力發出停止披露通知，要求停止或限制披露涉及「起底」內容，同時賦予私隱專員權力就「起底」個案進行刑事調查和檢控，大大加強執法力度。

《私隱條例》適用於香港的公私營機構（包括政府），屬於科技中立及原則性的法例。根據《私隱條例》，「個人資料」是直接或間接與一名在世人士有關的數據，而從該數據直接或間接地確定有關的個人身份是切實可行的，及該數據的存在形式予以查詢或處理是切實可行的。「個人資料」的概念與內地《個人信息保護法》下的「個人信息」相類似。「資料當事人」是指屬於個人資料的當事人的個人；「數據用戶」則指獨自或聯同其他人或與其他人共同控制個人資料的收集、持有、處理或使用的人。任何數據用戶必須遵守《私隱條例》下的相關規定，包括涵蓋了由收集、保存、使用以至銷毀個人資料的整個生命週期的六項保障資料原則。

私隱（包括個人資料私隱）雖為基本人權之一，但非絕對的權利，亦需與其他重要權利或公眾利益取得平衡。在這方面，《私隱條例》訂明在個別情況下，個人資料的使用（或查閱）可獲豁免而不受若幹條文所管限，例子包括防止罪行或嚴重不當行為、保安及防衛、統計及研究、保障資料當事人的健康、法律程序等。

在執法方面，《私隱條例》賦權私隱專員可向違例的數據用戶發出執行通知，指令其糾正相關的違反行為以及防止類似違反行為再發生。如有關數據用戶違反執行通知的規定，即屬於犯法。此外，除「起底」罪行，違反條例的某些條文，例如有關直接促銷的規定，亦可構成刑事罪行。

二、穩中求進 - 私隱專員公署過去一年的工作

私隱專員公署一直秉持穩中求進的宗旨，在務實推進既定工作時亦推展多項新猶。在2023年，私隱專員公署進行了393次循規審查，全年共處理3,582宗投訴個案和15,914宗公眾查詢。公署亦合共處理756宗「起底」個案，向23個網上平台發出了378個停止披露通知，涉及10,682個「起底」訊息，當中遵從率超過95%。同年，私隱專員公署接獲157宗資料外泄事故通報，較2022年的105宗增加接近五成。

在全球數碼化持續急速發展的趨勢下，私隱專員公署亦與其他數據保障機構和私隱專家保持聯繫，緊貼國際資料保障社群的最新脈搏。在2023年，私隱

專員公署繼續積極參與多個國際和地區論壇，包括環球私隱議會、亞太區私隱機構、全球私隱執法機關網絡以及亞太經合組織數碼經濟督導小組數據私隱分組，就包括人工智能使用，數據擷取，數據分享等方面的私隱議題交流知識及經驗。

三、抓住國家新機遇、深化大灣區融合發展

正如香港特別行政區行政長官李家超先生在2023年施政報告中提及，在中央政府的大力支持下，香港擁有「背靠祖國、聯通世界」的獨特優勢。為積極融入國家的數字經濟發展大局，妥善發揮香港作為國際城市的地位，成為「國際數據港」，香港必須把握國家所提供的數據發展和科技創新的新機遇，全面投入國家塑造「數字灣區」的願景，在粵港澳大灣區（以下簡稱「大灣區」）數據跨境流動方面，提供穩妥的落地支撐。

事實上，隨著大灣區內各城市之間的緊密融合，香港和大灣區其他城市之間的數據跨境流動需求亦與日俱增。跨境數據流動既可促進大灣區整體的發展，亦可加速建立「數字灣區」。

在上述前提下，香港特別行政區政府創新科技及工業局（以下簡稱「創科及工業局」）與國家互聯網信息辦公室（以下簡稱「國家網信辦」）於2023年6月簽署了《促進粵港澳大灣區數據跨境流動的合作備忘錄》（以下簡稱「《合作備忘錄》」），為促進大灣區內個人信息跨境流動的發展提供堅實基礎。同年12月，國家網信辦、創科及工業局及私隱專員公署共同制定《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同》（以下簡稱「《大灣區標準合同》」）的便利措施，以促進及簡化大灣區內地城市與香港之間的個人信息跨境流動的合規安排。

《大灣區標準合同》適用於大灣區九個內地城市（即廣東省廣州市、深圳市、珠海市、佛山市、惠州市、東莞市、中山市、江門市及肇慶市）和香港兩地之間的個人信息跨境轉移，包括由大灣區內地城市至香港的個人信息跨境轉移，及由香港至大灣區內地城市的個人資料跨境轉移。

為實施《大灣區標準合同》，兩地政府訂立了《粵港澳大灣區（內地、香港）個人信息跨境流動標準合同實施指引》（以下簡稱「《大灣區標準合同實施指引》」）。個人信息處理者及接收方可以根據《大灣區標準合同實施指引》的要求，按自願原則及統一的模板訂立標準合同，從而規範合同雙方就個人信息跨境流動的責任和義務。

《大灣區標準合同》採用了「屬地」的概念，確保個人信息處理者及接收方可以按照所在地的相關法律



規定進行跨境個人信息轉移，即香港的數據用戶需要遵從香港《私隱條例》的規定，而內地的個人信息處理者則需要遵從內地《個人信息保護法》及相關法律法規。

而為了與內地的相關法律法規對接，相比起《私隱條例》的規定，《大灣區標準合同》要求個人信息處理者開展個人信息保護影響評估及就標準合同進行備案。

另一方面，作為促進大灣區內個人信息跨境流動的便利措施，《大灣區標準合同》亦豁免了部分在內地的《個人信息出境標準合同》中訂立的要求，例如：

(一)《大灣區標準合同》內並沒有訂定有關個人信息數量及敏感個人信息的限制。

(二)《大灣區標準合同》的合約方無須就接收方所在地區的個人信息保護政策和法規進行相關評估。

(三)就有關開展個人信息保護影響評估的要求，《大灣區標準合同》要求個人信息處理者重點評估的項目範圍亦大幅減少。

(四)《大灣區標準合同》內也沒有與敏感個人信息或自動化決策機制相關的特別規定。

為保障個人信息在大灣區內安全有序流動，《大灣區標準合同》並就再轉移個人信息施加限制，規定接收方不得向大灣區以外的組織或個人提供據《大灣區標準合同》所接收到的個人信息。接收方只可在符合所有特定條件的情況下，向大灣區內地或香港特別行政區同轄區內的第三方提供個人信息（如接收方註冊於（適用於組織）/位於（適用於個人）粵港澳大灣區內地城市，同轄區即指大灣區內所有內地城市；如接收方註冊於（適用於組織）/位於（適用於個人）香港，同轄區只限於香港）。

為協助香港機構理解《大灣區標準合同》的適用性及相關合約條款，私隱專員公署亦發出了「跨境數據轉移指引：《粵港澳大灣區（內地、香港）個人信

息跨境流動標準合同》」，私隱專員公署鼓勵企業及機構採用《大灣區標準合同》作出相關個人資料跨境轉移。採用《大灣區標準合同》亦有助顯示企業及機構已採取所有合理的預防措施及作出所有應作出的努力，以確保有關數據不會在接收方所屬於的司法管轄區以違反《私隱條例》規定的方式被收集、持有、處理或使用。

值得注意的是，《大灣區標準合同》便利措施並不影響私隱專員公署按《私隱條例》在職責範圍內依法保障個人資料和監督管理的工作，包括處理與保障個人資料有關的投訴、舉報，調查、處理違法個人資料處理活動等。

作為便民利企的措施，《大灣區標準合同》的出台是促進個人信息跨境安全流動和創新發展的一大步。隨著《大灣區標準合同》的推出，大灣區的數據處理將更趨一體化，不但為各方提供更為便利的商業環境，亦為大灣區內的數據經濟發展增添動力。私隱專員公署將繼續積極推動促進個人信息在大灣區內跨境流動的便利措施，為國家、大灣區和香港的互聯互通作出貢獻。

四、背靠祖國、行穩致遠

世界漸趨一體化，在善用香港的國際化優勢、全力維護個人資料私隱及數據安全的同時，有效推進國家及香港的數字經濟發展，一直是私隱專員公署的重點工作。

此外，在人工智能興起以及世界轉趨數碼化的新時代，妥善維護數據安全並保障個人資料私隱，亦是私隱專員公署重中之重的使命。私隱專員公署將繼續秉持務實開放的態度，緊貼國家的數字經濟發展，積極為大灣區的互聯互通，為祖國高質量發展和高水平對外開放，作出貢獻。

史海鉤沉 HISTORICAL STORY

守正如一： 陳守一與北大法學教育

【「北京大學法學學科建立 120 周年」影像專題】

自 1904 年「法律門」被列為京師大學堂正式學科起，現代法學教育在北京大學已走過 120 年光輝歷程。在兩個甲子的漫長歲月中，北大法學形成了厚重學術傳統，涵養了諸多名師大家。為紀念北京大學法學學科建立 120 周年，本刊特與北大法學院合作，以系列影像專題的形式，向廣大讀者介紹陳守一、芮沐、王鐵崖、沈宗靈、肖蔚雲、羅豪才等六位曾任教於北京大學的代表性法學家。

北京大學法學院供稿 吳景鍵執筆

one thing: questioning the judge's integrity or professional impartiality is quite another. Likewise, a failure to separate a court decision from the Judiciary as an institution is not helpful to the well-being of the common law system. He pointed out that judges must be able to decide cases and explain their decisions in judgments without interference or illegitimate pressure. This is of cardinal importance to judicial independence. Threats of sanction or reprisal against judges for simply discharging their judicial duties are, therefore, repugnant to the rule of law and fundamentally objectionable. He also mentioned that the Judiciary has a duty to effectively prevent, suppress and impose punishment for any act or activity endangering national security in accordance with law. The courts will administer justice strictly and fairly in accordance with the *National Security Law* as well as other applicable laws, and they will not yield to any pressure to convict or acquit, nor pay heed to harassment or threats of any kind. He emphasized that whatever may be said or written about our legal system, the community can be sure of one thing: our courts and our judges will continue to discharge their constitutional duty to administer justice fairly and efficiently, without fear or favour, self-interest or deceit. This, too, is essential to the continuation of the common law system in Hong Kong. When mentioning the progress of new measures taken by the Judiciary, Mr. Cheung said that the electronic litigation system (generally known in the abbreviated form as "iCMS") has already been smoothly implemented in most civil proceedings in the District Court as well as the summons cases in the Magistrates' Courts. Its extension to other levels of courts, most importantly the High Court level, where the bulk of our heavy civil litigation is handled, is scheduled for this year.

The Secretary for Justice, Mr Paul Lam, SC, emphasized in his speech that no evidence showed that the Judiciary's independent judicial power has been compromised in cases involving national security. He said that all court hearings relating to national security are, generally speaking, held openly. More importantly, all decisions and judgments made by the court in this respect are publicised on the Judiciary's website, which is accessible for free. People will have no difficulty

Office of the Privacy Commissioner for Personal Data, Hong Kong: Striving to Safeguard Personal Data Privacy and Promote Cross-boundary Data Flow

Ada CHUNG Lai-ling (Barrister, Privacy Commissioner for Personal Data)

Since Hong Kong's return to the Motherland, the principle of "One Country, Two Systems" has been successfully implemented with the unwavering support of the Central People's Government, guaranteeing the long-term prosperity and stability of Hong Kong as well as the robustness of its economic system. As an international financial centre and a hub of innovative technology, Hong Kong's digital economy is set to grow rapidly. The Office of the Privacy Commissioner for Personal Data, Hong Kong (hereinafter referred to as the "PCPD"), being an



Mr Andrew Cheung Kui-nung inspects a Ceremonial Guard mounted by the Hong Kong Police Force



Mr Paul Lam, SC gives an address

in following the court proceedings, and studying the reasons for the court's decisions and judgments. He reiterated that the HKSAR Government will do its best and take whatever measures within its powers to ensure that Judges and Judicial Officers will be able to perform their judicial functions without fear of intimidation. 港

independent body established to safeguard the protection of personal data privacy for citizens of Hong Kong, is dedicated to promoting the protection of and respect for personal data privacy while ensuring the safe and secure flow of personal data, thereby contributing to the qualitative development of the digital economy of the Motherland and Hong Kong.

I. About the PCPD

The PCPD was established in August 1996 to oversee the

implementation of and compliance with the *Personal Data (Privacy) Ordinance* (Chapter 486 of the Laws of Hong Kong) (hereinafter referred to as the "PDPO"). The PCPD is headed by the Privacy Commissioner for Personal Data (hereinafter referred to as the "Privacy Commissioner") and comprises different functional units, including the Complaints Division, Criminal Investigation Division, Compliance & Enquiries Division, Legal Division, Global Affairs & Research Division, Corporate Communications Division and Corporate Support Division. In addition to monitoring and supervising compliance with the PDPO, the PCPD conducts proactive investigations into areas with significant privacy risks. To assist the public, the Government of the Hong Kong Special Administrative Region (hereinafter referred to as the "HKSAR Government"), different industries and relevant stakeholders in coping with the rapidly evolving technological environment and increasingly complex data landscape, the PCPD also keeps abreast of the latest technological advancements, as well as developments in data security and personal information protection both in the Mainland and internationally, so as to ensure that its guidance and advice are up-to-date and relevant.

The PDPO is the legal framework for safeguarding personal data privacy in Hong Kong. It is one of Asia's longest-standing comprehensive data protection laws, having come into effect in December 1996. Its first major amendment was in 2012, when new regulations were introduced targeting direct marketing behaviours involving the use of personal data. In 2021, the PDPO underwent its second amendment whereby doxxing acts that infringe upon personal data privacy were criminalised. This amendment conferred new statutory powers on the Privacy Commissioner to issue cessation notices demanding the cessation or restriction of disclosure of doxxing messages. The 2021 amendments also conferred on the Privacy Commissioner powers to conduct criminal investigations and institute prosecutions for doxxing cases, further strengthening its enforcement against acts of doxxing.

The PDPO is a technology-neutral and principles-based law that applies to both the private and the public sectors, including the HKSAR Government. The PDPO defines the term "personal data" as any data relating directly or indirectly to a living individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained and in a form in which access to or processing of the data is practicable, which is similar to the notion of "personal information" under the Mainland's *Personal Information Protection Law* (hereinafter referred to as the "PIPL"). In relation to personal data, "data subject" means the individual who is the subject of the data, and "data user" refers to a person who either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data. All data users must comply with the requirements of the PDPO, which include six Data Protection Principles that cover the entire life cycle of the handling of personal data, from collection, retention, and use to destruction.

Although the right of privacy, including the right of personal data privacy, is a fundamental human right, it is not an absolute right and must be balanced against other fundamental rights or the public interest. This is reflected in the PDPO, which provides a number of exemptions in specific circumstances. These include, for example, the prevention of crimes or seriously improper conduct, security and defence, statistics and research, protection of a data subject's health, and use of personal data in legal proceedings.

As regards enforcement, the PDPO empowers the Privacy Commissioner to issue an enforcement notice to a data user, specifying remedial and/or preventive steps to be taken. Failure to comply with an enforcement notice is an offence. Besides doxxing offences, contraventions of certain provisions of the PDPO, such as the regulations targeting direct marketing, are also criminal offence.

II. A Time of Continuity and Progression—A Year in Review

In the past year, the PCPD has maintained its established efforts while pursuing new initiatives. In 2023, it conducted 393 compliance checks, and handled 3,582 complaints and 15,914 public enquiries. It also handled 756 doxxing cases and served 378 cessation notices on 23 online platforms, requesting the removal of 10,682 doxxing messages and achieving a compliance rate of over 95%. In addition, it received 157 data breach notifications, an increase of nearly 50% compared to 105 notifications in 2022.

The acceleration of global digitalisation has prompted the PCPD to maintain close contact with other data protection authorities and experts, keeping its fingers on the pulse of the international data protection community. In 2023, the PCPD continued to participate actively in a number of global and regional forums, including the Global Privacy Assembly, the Asia Pacific Privacy Authorities, the Global Privacy Enforcement Network and the APEC Digital Economy Steering Group Data Privacy Subgroup. It also continued to share with the international community its insights and experience regarding the use of artificial intelligence, data scraping and data sharing, among others.

III. Capturing New Opportunities Offered by the Motherland and Deepening Integration into the Greater Bay Area

As the Chief Executive of the HKSAR Government, Mr John KC Lee, pointed out in his 2023 Policy Address, Hong Kong has the distinctive advantage of enjoying direct access to the huge Mainland market while maintaining its strong international connectivity with the strong support of the Central Government. To fully integrate into the Motherland's national digital economy blueprint and leverage its position as an international city, Hong Kong must seize the abundant opportunities that arise from the Motherland's revitalisation and prosperity in both data development and technological innovation. Hong Kong aims to become an international data hub and contributes to the Motherland's vision of establishing a "Digital Bay Area" by fostering cross-boundary data flows within the Guangdong-Hong Kong-Macao Greater Bay Area (hereinafter referred to as the "Greater Bay Area") with full vigour.

Given the close integration of cities in the Greater Bay Area, the demand for data flows between Hong Kong and other cities within the Greater Bay Area is increasing. In addition to enabling the overall digitalisation and economic development of the Greater Bay Area, cross-boundary data flows will expedite the establishment of the "Digital Bay Area".

Against this background, the *Memorandum of Understanding on Facilitating Cross-boundary Data Flow Within the Guangdong-Hong Kong-Macao Greater Bay Area* (hereinafter referred to as the "MoU") was signed by the Innovation, Technology and Industry Bureau of the HKSAR Government (hereinafter referred to as the "ITIB") and the Cyberspace Administration of China (hereinafter

referred to as the “CAC”) in June 2023. The MoU provides a solid foundation to facilitate cross-boundary data flows within the Greater Bay Area. To further this goal and as a facilitation measure under the MoU, the CAC, the ITIB and the PCPD jointly formulated the *Standard Contract for the Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong)* (hereinafter referred to as the “GBA SC”) in December 2023. The GBA SC aims to foster the cross-boundary flows of personal information within the Greater Bay Area and streamline compliance arrangements.

The GBA SC regulates cross-boundary transfers of personal information between nine Mainland cities within the Greater Bay Area (including Guangzhou, Shenzhen, Zhuhai, Foshan, Huizhou, Dongguan, Zhongshan, Jiangmen and Zhaoqing of Guangdong Province) and Hong Kong. It covers both cross-boundary personal information transfers from these nine Mainland cities within the Greater Bay Area (hereinafter referred to as the “Mainland Cities”) to Hong Kong, and transfers from Hong Kong to the Mainland Cities.

To help implement the GBA SC, the CAC and ITIB also issued the *Implementation Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong)* (hereinafter referred to as the “Implementation Guidelines”). Personal information processors and recipients may, in accordance with the requirements set out under the Implementation Guidelines, enter into the Standard Contract voluntarily using a standardised template. The Standard Contract, which binds both contractual parties, sets out the obligations and responsibilities of both parties regarding the cross-boundary flow of personal information.

The GBA SC adopts the concept of “respective jurisdiction” to ensure that personal information processors and recipients can transfer personal information across boundaries in accordance with the relevant legal requirements of their respective jurisdictions. This means that data users in Hong Kong must observe the requirements of the PDPO, while personal information processors in the Mainland must comply with the Mainland’s PIPL, and other relevant laws and regulations.

To align with the relevant laws and regulations of the Mainland, the GBA SC imposes requirements that are additional to those under the PDPO. These include requiring personal information processors to conduct a personal information protection impact assessment on the intended transfer, and obliging the parties to follow the corresponding filing procedures of the GBA SC.

On the other hand, as a facilitation measure in promoting cross-boundary flows of personal information within the Greater Bay Area, the GBA SC has relaxed some of the requirements set out in the Mainland’s *Standard Contract for Cross-border Transfers of Personal Information*. Some examples of such relaxed requirements include:

1. The restriction concerning the amount and sensitivity of the personal information that may be transferred across borders was removed under the GBA SC;
2. The parties to the GBA SC are not required to conduct assessments of the personal information protection policies and regulations in the region where the recipient is located;
3. The scope of personal information protection impact assessment that personal information processors must conduct under the GBA SC is greatly reduced; and
4. The GBA SC does not have any specific requirement regarding sensitive personal information or automated decision-

making mechanisms.

To ensure the safe and orderly flow of personal information within the Greater Bay Area, the GBA SC also restricts the recipient from providing the personal information obtained under the GBA SC to organisations or individuals outside the Greater Bay Area. The recipient can only provide personal information to a third party in the same jurisdiction of the Mainland cities within the Greater Bay Area or the HKSAR respectively, subject to the specified conditions. In this regard, if the recipient is registered (for organisations) or located (for individuals) in a Mainland city within the Greater Bay Area, the term “same jurisdiction” means the nine Mainland cities within the Greater Bay Area; if the recipient is registered or located in Hong Kong, “same jurisdiction” means Hong Kong.

To help organisations in Hong Kong understand the applicability of the GBA SC and its contractual clauses, the PCPD has issued the *Guidance on Cross-boundary Data Transfer: Standard Contract for the Cross-boundary Flow of Personal Information Within the Guangdong–Hong Kong–Macao Greater Bay Area (Mainland, Hong Kong)*. The PCPD encourages organisations to adopt the GBA SC for cross-boundary flows of personal information within the Greater Bay Area. By adopting the GBA SC, enterprises and organisations can show that they have taken all reasonable precautions and exercised all due diligence to ensure that the relevant data will not be collected, held, processed or used in the recipient’s jurisdiction in any manner that would violate the PDPO.

Notably, the implementation of the GBA SC will not affect the operation of the PDPO or the PCPD’s role in protecting personal data privacy and supervising compliance with the PDPO in Hong Kong, including the handling of complaints and reports relating to personal data protection, conducting investigations, and dealing with activities involving the unlawful handling of personal data, etc.

The GBA SC is a convenient and facilitative measure that marks a significant milestone in promoting safe and secure cross-boundary transfers of personal information. It standardises data handling practices in the Greater Bay Area, creating a more conducive business environment and boosting the development of the digital economy in the Greater Bay Area. The PCPD will keep up with its efforts in promoting facilitation measures that foster cross-boundary flows of personal information within the Greater Bay Area and contribute to the increased connectivity between Hong Kong and the Motherland, including the Greater Bay Area.

IV. Leveraging the Country’s Support as We Forge Ahead

As the world becomes increasingly interconnected, the PCPD has always strived to leverage Hong Kong’s international position to safeguard personal data privacy and data security in promoting the development of the digital economy in the Country and Hong Kong.

In addition, as the new era witnesses the rise of artificial intelligence and global digitalisation, the PCPD has made it an important mission to ensure data security and safeguard personal data privacy. Going forward, the PCPD will continue to maintain a pragmatic and open attitude as it keeps abreast of developments in the Country’s digital economy, with a view to contributing to the integration of the Greater Bay Area and the qualitative developments of the Motherland as it continues to open up to foreign investments. ■

史海鉤沉 HISTORICAL STORY

Stay True to Original Intention: Chen Shouyi and Legal Education at Peking University

§ Images Commentating the 120th Anniversary of Law Discipline in Peking University §

Since “legal studies” was listed as an official discipline at the Imperial University of Peking in 1904, modern legal education has thrived for 120 years at Peking University. Through the glory of more than one century, it has built a profound academic tradition and nurtured many renowned masters. To commemorate its 120th anniversary, we have collaborated with the Law School of Peking University to introduce, in the form of special issues with images, six representative legal scholars who have taught at Peking University, including Chen Shouyi, Rui Mu, Wang Tieya, Shen Zongling, Xiao Weiyun, and Luo Haocai.

Contributed by Law School of Peking University
Written by Wu Jingjian