數據驅動
為何隱私合規是IR的關鍵

未來數月內，包括內地在內的亞洲多地將實施新的數據保護法，該地區的IR營運須謹慎行事。

文 Victoria White及Daniela Guerreiro
MdME Lawyers

DATA DRIVEN
Why privacy compliance is key for IRs

New data privacy laws coming into effect across Asia, including in mainland China, in the coming months will require careful navigation by the region's IR operators.

By **Victoria White** and **Daniela Guerreiro**
MdME Lawyers

隨著捕獲信息的數量及敏感性的增加，數據隱私的合規性已經成為適用於絕大多數IR業務營運的關鍵要求。

With the increased volume and sensitivity of the information captured, data privacy compliance has become a critical business requirement.

數據已成為IR運營商的新儲備貨幣。獲取有關客戶大量信息的價值已成為整體業務績效的關鍵。從支付寶和微信小程序營銷，到無現金支付、數字預訂和地理定位Wifi登錄，數字活動的激增使得從新數據流中收集的數據大量增加，有助於為商業決策提供信息，並提高IR領域的整體效率。

在一個以服務為導向的行業中，通過為前線員工提供客戶個人偏好信息以提供個性化體驗，對客戶體驗和服務交付都大有裨益。同樣地，部署複雜的人工智能及數據分析工具的後端CRM管理可以協調營銷傳播戰略，取得更好的參與度及ROI結果。

因此，從庫存管理到人員配備再到營銷策略，數據已成為在整個IR業務決策的關鍵。因而數據的手機及處理範圍達到了新的水平。這些數據大部分涉及客戶、訪客和員工的個人信息，這觸發了國家對個人數據及隱私法的保護要求。

Data has become the new reserve currency for IR operators. The value of capturing extensive information about customers has become critical to overall business performance. The surge in digital activities, from Alipay and WeChat mini-program marketing, to cashless payments, digital reservations and geolocation Wifi log-ins, allows for a huge increase in data collection from new data streams that can help to inform business decisions and improve efficiencies across the IR landscape.

In a service-orientated industry, customer experience and service delivery benefit enormously from equipping front line staff with information on customers' personal preferences in order to deliver a personalized experience. Equally, back-end CRM management that deploys sophisticated AI and data analytics tools can orchestrate a marketing communications strategy with superior engagement and ROI outcomes.

Data, therefore, has become mission critical for informing decisions throughout the IR business, from inventory management to staffing and marketing strategies. Consequently, the scope of data collection and processing has reached new levels. The majority of this data concerns personal information of customers, visitors and employees, which triggers the requirements of national personal data and privacy laws.

有鑒於IR行業的性質，顧客的個人信息向來被視為尤其敏感。現在，新的高風險數據類別，包括從數字支付交易中生成的數據——及未來預期的無現金博彩交易生成的數據——以及健康碼工具，譬如新冠疫情追蹤應用程序、疫苗護照和檢測結果。隨著捕獲信息的數量及敏感性的增加，數據隱私的合規性已經成為適用於絕大多數IR業務營運的關鍵要求。

加強隱私監管和執法

與此同時，數據隱私立法也在不斷發展，在制定及執行收集和使用個人信息的數據隱私法方面，亞洲地區的監管機構變得更為積極。其中一些新規定具有域外效力，這意味著某些情況下，從海外客戶收集個人信息的運營商需要遵守客戶所在的司法管轄區的法律規定。

中國新《個人信息保護法》

迄今為止，中國還沒有專門而全面的保護個人信息的法律，而是以來大量針對特定行業的法規對某些行業的個人數據處理標準作出規定。

今年8月，中國政府通過了新的《個人信息保護法》，該法將於2021年11月1日生效。新的《個人信息保護法》將對處理中國居民個人信息的公司活動產生影響，即使這些公司位於海外、澳門或香港。因此，該法律並不僅限於位於中國大陸的實體。事實上，在中國大陸以外地區處理個人信息的境外企業，將被要求在中國境內設立代理機構或委派指定代表，處理與個人信息保護的相關事宜，並向中國當局備案。該法律還對從中國大陸向境外（包括澳門和香港）跨境轉移個人信息進行了限制。而轉移數據之前必須滿足諸如額外的安全評估、保護認證、合同或風險評估等要求。

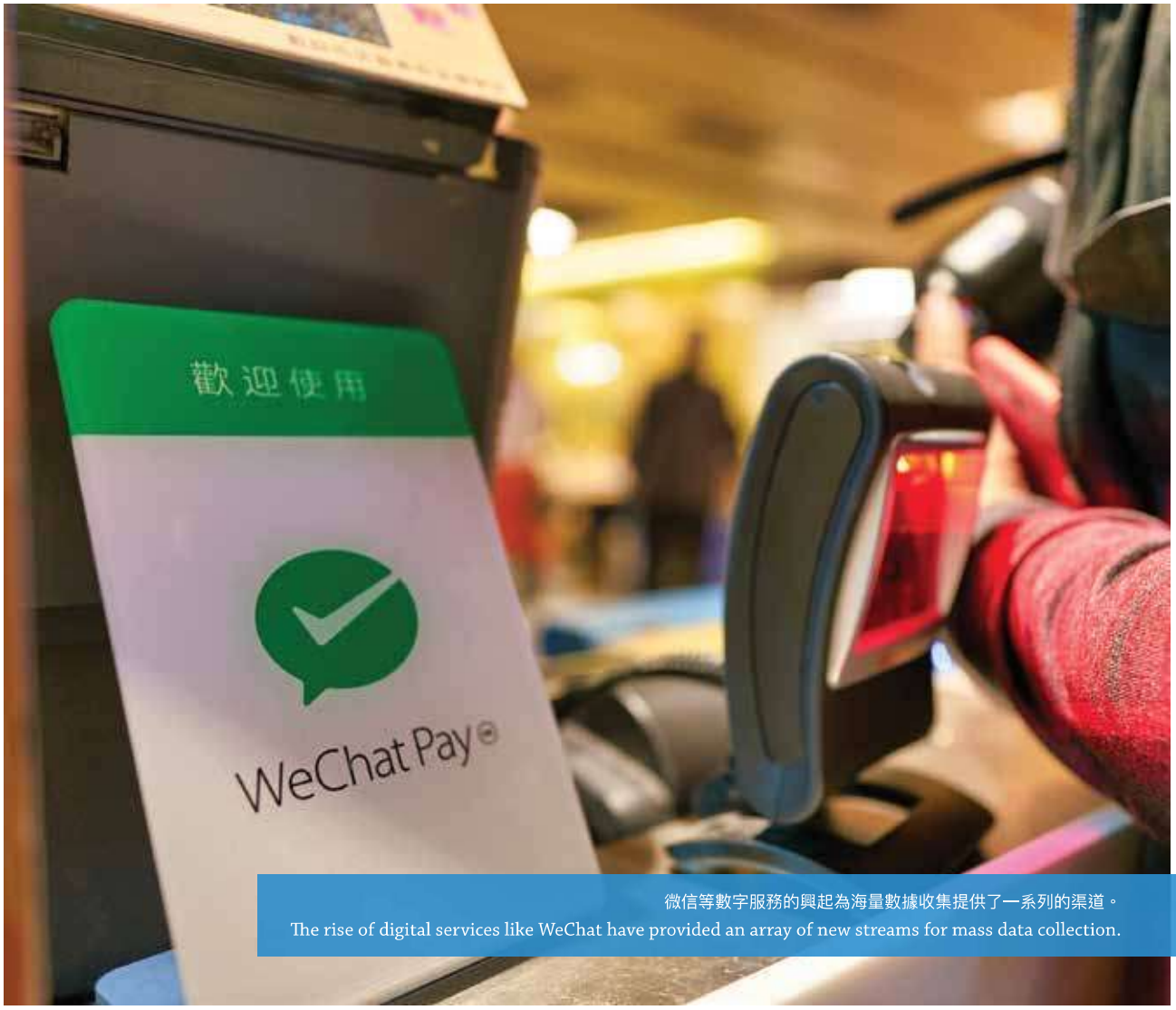
鑑於中國內地客戶是澳門IR營運商的最大市場，新的《個人信息保護法》對商業運作的影響需要在11月1日生效前仔細評估。尤其是通過市場應用程序、微信公眾號和小程序、網站收集個人信息的程序，以及隨後從境外轉移至澳門的任何程序，都要優先審查。

違反新法的處罰很高，包括對嚴重違法行為處以最高5000萬元人民幣（770萬美元）或相當於公司年營業額5%的罰款。儘管新法的執行未經檢驗，但中國當局最近對科技領域的數據隱私

Given the nature of the IR industry, patrons' personal information has always been considered especially sensitive. Now, new categories of high-risk data are subject to collection, including data generated from digital payment transactions – and prospectively cashless gaming transactions in future – as well as health code tools, such as COVID-19 tracing apps, vaccine passports and test results. With the increased volume and sensitivity of the information captured, data privacy compliance has become a critical business requirement applicable to the vast majority of IR business operations.

INCREASING PRIVACY REGULATION AND ENFORCEMENT

At the same time, the legislation of data privacy has continued to evolve, and regulators in the region have become ever-more active in enacting and enforcing new data privacy laws for the collection and use of personal information. Some of these new provisions have extra-territorial effect, meaning that operators who collect personal information from overseas customers will need to comply with the requirements of the law in the customers' home jurisdiction in certain circumstances.



微信等數字服務的興起為海量數據收集提供了一系列的渠道。
The rise of digital services like WeChat have provided an array of new streams for mass data collection.

CHINA'S NEW PERSONAL INFORMATION PROTECTION LAW

Until recently, China did not have a dedicated overarching personal information law, relying instead on a myriad of sector-specific regulations that addressed standards for personal data processing in certain industries.

In August this year, the Chinese Government passed its new law on personal data protection that will take effect on 1 November 2021. The new Personal Information Protection Law will impact the activities of companies that handle the personal information of Chinese residents – even where the companies are located overseas, or in Macau or Hong Kong. The law, therefore, is not restricted to entities located within mainland China. In fact, overseas businesses that process personal information outside of mainland China will be required to set up an agency or appoint a designated representative within China to handle matters related to personal information protection, and record it with the Chinese authorities. The law also imposes restrictions on cross-border transfers of personal information from mainland China to

overseas locations, including Macau and Hong Kong. Certain requirements, such as additional security assessments, protection certifications, contracts or risk assessments, must be fulfilled prior to overseas transfers of data to these locations.

Given that mainland Chinese customers constitute the largest market segment for Macau IR operators, the effect of the new Chinese Personal Information Protection Law on business operations will need to be closely assessed ahead of the effective date on 1 November. In particular, the procedures for collection of personal information through in-market apps, WeChat official accounts and mini-programs, websites and any subsequent overseas transfer to Macau appear a priority for review.

The penalties for infringing the new law are high, including fines of up to RMB 50 million (US$7.7 million) or 5% of the company's annual turnover for serious offences. Although enforcement of the new law is untested, the Chinese authorities have recently taken an assertive stance on data privacy violations in the technology sector. The Cyberspace Administration of China, the Chinese internet watchdog, found 84 online apps had infringed personal information through over-collection and excessive use in May 2021 and required those operators to rectify their processes within 15 days.

More recently in July 2021, Didi, the ride sharing app, was suspended from app stores in China for breaching data collection and use rules.

中國新的《個人信息保護法》將對處理中國居民個人信息的公司活動產生影響，即使這些公司位於海外、 澳門或香港。

China's new Personal Information Protection Law will impact the activities of companies that handle the personal information of Chinese residents – even where the companies are located overseas, or in Macau or Hong Kong.

The potential fines and impact on operations for businesses is evident for those which fail to comply with Chinese data privacy law requirements.

JAPAN STRENGTHENS PRIVACY LAW REQUIREMENTS

Similarly, Japan has passed amendments to its personal information law that expand the extraterritorial effect of the law to all overseas companies that handle personal information of Japanese citizens, as well as pseudonymously and anonymously processed information, in certain circumstances. The amendments to the Act on the Protection of Personal Information will come into effect on 1 April 2022 and operators with Japan-focused

侵犯採取了強硬立場。2021年5月，中國國家互聯網信息辦公室（網信辦）通報有84款在線應用程序過度收集及過度使用侵犯了個人信息，要求這些營運商在15日內糾正其流程。

近期於2021年7月，拼車應用滴滴因違反數據收集和使用規定，在中國的應用商店中被下架。對於那些未能遵守中國個人信息保護法要求的企業而言，潛在的罰款及對企業運營的影響是顯而易見的。

日本加強隱私法要求

日本也通過了《個人信息保護法》修正案，將法律的域外效力擴大到所有處理日本公民個人信息的境外公司，以及在某些情況下以假名或匿名處理信息的海外公司。該《個人信息保護法》修正案將於2022年4月1日生效。擁有日本業務團隊的營運商將需要確定是否受到影響，並需要在該日期前徹底審視流程，已符合修訂後的新法律。

澳門《個人資料保護法》執行情況

在澳門，近期發生的事件彰顯了當局對於數據隱私調查及打擊侵權行為的堅定態度。2020年，澳門個人資料保護辦公室對部分進行非法電話營銷活動和使用個人數據但並未獲得個人同意的公司，處以總計 1200 萬澳門元（150 萬美元）的罰款。

《澳門個人資料保護法》還規定了個人對其個人資料享有的多項權利，包括在某些情況下有權查閱、修正、刪除或阻止對其個人資料的處理。近年來，隨著個人權利意識的增強，對個人數據價值的認識及保護個人數據免受不當利用的必要性亦日益增強，查閱、更正及刪除資料的請求有所增加。鑑於涉及的潛在數據資料當時人的數量和來自多個地點的數據量，根據《澳門個人數據保護法》的要求，在合理時間內回應個人的數據請求需投入大量專用資源才能有效處理。

有鑒於海外個人資料保護法（例如內地新的《個人信息保護法》）對數據主體具有類似訪問、更正和刪除權，如果沒有額外的協助和人力，潛在的數據主題請求數量可能會呈指數級增長，企業或將難以應付。

澳門法律還規定，一旦收集目的完成，個人資料將被刪除。

teams will need to determine if they are affected and need to overhaul processes to comply with the updated Japanese law before the operative date.

MACAU DATA PRIVACY ENFORCEMENT

Meanwhile, in Macau recent developments have seen a determined approach by the authorities towards data privacy investigations and enforcement against infringers. In 2020, the Macau Data Protection Office levied fines totaling MOP$12 million (US$1.5 million) against companies for illegal telemarketing activities and use of personal data, and failure to secure the individuals' consent for use of their data.

The Macau Personal Data Protection Act also enshrines a number of rights for individuals over their personal data, including the right to access, rectify, erase or block the processing of their data in some cases. As individuals' consciousness of their rights has increased in recent times with a growing awareness of the value of their personal data and need for protection against exploitation, the number of data access, rectification and deletion requests has increased. In view of the potential number of data subjects involved and the volume of data from multiple contact points, the exercise of responding to individuals' data requests within a reasonable time, as required under the Macau Personal Data Protection Act, demands significant dedicated resources for it to be handled effectively.

When the potential effect of overseas data privacy laws, such as the new Chinese Personal Information Protection Law, that have similar rights of access, rectification and deletion for data

隨著捕獲的新數據流的增加，確定及記錄所收集的所有類型和類別的個人數據的保留期限，以及確保一旦保留期限到期，跨IT系統和備份服務器上的所有個人資料副本被刪除，這些是一項龐大的任務。

此外，澳門於2019年出台了針對博彩相關數據的監管規定，要求澳門的博彩監管機構對任何博彩相關數據的海外傳輸（如投注金額、籌碼的購買和贖回）須事先授權，其中可能還包括用戶的姓名、國籍等在內的個人數據。根據2019年澳門的《網絡安全法》，作為私營關鍵基礎設施營運者，IR運營商在程序、預防及應對網絡安全事故方面負有特殊責任和義務，包括向當局報告網絡安全事故及潛在的數據洩露。

應對挑戰

儘管數據隱私的合規性對IR業務的連續性至關重要，但數據收集和使用的急劇增加，通常並未與內部數據隱私團隊的發展相匹配。為了應對日益複雜的工作，新的數據技術管理工具已經出現，可以支持個人數據團隊的簡化和實施隱私的管理流程。通過實施隱私管理軟件，數據可以在結構化平台上進行編目，並可以

subjects is factored in, the volume of prospective data subject requests may rise exponentially and appear overwhelming without additional assistance and manpower.

Macau law also requires that personal data is deleted once the purpose for collection has been completed. With the infinite number of new data streams captured, it is a sizable task to determine and document the retention period for all types and categories of personal data collected, and ensure that all copies of personal data are deleted across the IT systems and on back-up servers once the retention period expires.

In addition, regulation was introduced in 2019 in Macau for gaming-specific data that requires the Macau Gaming Regulator's prior authorization for the overseas transfer of any gaming-related data (such as betting amounts, bet placements, chip purchase and redemption), which may also include patrons' personal data (name, nationality). IR operators also have a special duty to implement cyber security management systems and procedures, including to report cybersecurity incidents and potential data breaches to the authorities, under the 2019 Macau Cybersecurity Law as private critical infrastructure operators.

SOLUTIONS FOR THE CHALLENGE

The dramatic rise in the collection and use of data has not generally been matched with a proportionate expansion of the in-house data privacy team, despite the critical nature of data privacy compliance to IR business continuity. To tackle the ever-increasing complexity of the work,

在合理時間內響應個人數據請求的做法……需要大量專用資源才能有效處理。

The exercise of responding to individuals' data requests within a reasonable time ... demands significant dedicated resources for it to be handled effectively.

new privacy tech management tools have emerged that can support privacy teams to streamline and operationalize privacy management processes. By implementing privacy management software, data can be catalogued on a structured platform and a central map of all personal data stored and used across the business can be created to monitor activities, investigate potential breaches, update records and delete data after fulfilment.

For IRs, a core challenge to date has been the fragmented nature of data ownership across business teams which may hold a slew of separate databases or data sources that operate on various IT systems. A centralized privacy management platform can provide the visibility, automation and record keeping needed to comply with the various national data privacy laws and regulations that apply. Additionally, privacy tools can be incorporated which automate fulfilment of data subject access requests, data discovery and redaction processes, allowing privacy teams to focus on more strategic privacy issues and tasks.

"Privacy management platforms are critical tools for large organizations, like integrated resort operators, which have numerous data streams from different sources," according to Rob Hinson, Greater China Manager of OneTrust, the most widely-used privacy platform.

"These often involve personal data of customers across a variety of jurisdictions, which can simultaneously subject the organization to multiple national data privacy laws. In an ever-changing

regulatory landscape, having a tool to manage these obligations – while remaining up to date with the latest regulatory changes – becomes paramount."

FUTURE OF PRIVACY MANAGEMENT

The adoption of privacy management software and tools can assist with streamlining data privacy management, but selection of the modules and tools must be tailored to the business's specific data streams, processes and applicable privacy law jurisdictions. Equally, the effectiveness of privacy tech solutions relies on an understanding of privacy issues by employees – not only those in the privacy team but staff throughout the business that have contact with personal data in their roles. Employee training on new data privacy protocols and data

創建一個可顯示存儲和使用所有個人數據的中央地圖，以監控活動、調查潛在的違規行為、更新記錄並在完成後刪除數據。

對於綜合度假村而言，迄今為止的核心挑戰是跨業務團隊的數據所有權的碎片化，這些團隊可能擁有大量在各種IT系統上運行的獨立數據庫或數據源。集中式個人數據管理平台可以提供符合適用各種國家個人數據保護法律和法規所需的可視性、自動化和記錄保存。此外，工具可以自動完成數據主體訪問請求、數據查閱和編輯流程，令到數據保護團隊能夠專注於更具戰略意義的數據保護問題及任務。

使用最為廣泛的數據保護平台OneTrust的大中華區經理Rob Hinso表示：「隱私管理平台是大型組織的關鍵工具，譬如綜合度假村營運商，他們擁有來自不同來源的大量數據流。」

「這些通常涉及橫跨多個司法管轄區的客戶的個人數據，可能令該組織同時受到多個國家或地區的數據保護法的約束。在不斷變化的監管環境中，擁有管理這些義務的工具——同時與最新的監管變化保持同步——變得至關重要。」

management, triggered by the new data privacy law requirements, is also vital so that operators can demonstrate effective implementation of data protection procedures and compliance.

In fact, as customers become increasingly sensitive to personal data use and exploitation, operators can use their approach to personal data management to build a trusted reputation with customers and differentiate themselves from competitors. By providing transparent and user-centric privacy management tools that allow customers to take control and permit use only for genuinely agreed purposes, operators can demonstrate their commitment to respecting the privacy rights of users and putting the customers' preferences first. iag

個人數據保護的未來

採用個人數據管理軟件和工具有助於簡化數據隱私管理，但模塊和工具的選擇必須根據企業業務的特定數據流、流程和適用監管法規量身定制。同樣地，個人數據解決方案的有效性取決於員工對隱私問題的理解——不僅是個人數據管理團隊中的員工，還有整個企業的在其工作中會接觸到個人數據的員工。由新數據隱私法的要求所引發的新數據隱私協議和數據管理的員工培訓也是至關重要，這將令運營商能夠保證數據保護程序有效實施及合規。

事實上，隨著客戶對個人數據的使用和利用越來越敏感，運營商可以利用他們的個人數據管理方法在客戶中建立可信賴的聲譽，從而將自己與競爭對手區分開來。通過提供透明的、以用戶為中心的個人數據管理工具，允許用戶控制並允許僅用於真正同意的目的，運營商可以展示他們對用戶隱私權的尊重，及將客戶偏好放在首位的承諾。 iag