

# 中國《網絡安全法》研討會：傳播與治理

## 《網絡安全法》、《數據安全法》及《個人信息保護法》對於外商投資的影響及因應策略

泰鼎法律事務所資深顧問  
蔡步青律師

2021.9.24  
香港恒生大學



- 中國大陸及臺灣執業律師
- 中華仲裁協會仲裁員
- 上海市浦東新區東方調解中心特邀律師調解員
- 基隆律師公會大陸事務委員會副主任委員
- 臺北律師公會大陸事務委員會委員

➤ 經歷：

- 北京德和衡律師事務所顧問
- 北京市中銀律師事務所顧問
- 理律法律事務所資深律師

➤ 學歷：

- 北京大學國際經濟法法學博士
- 國立台灣大學法學碩士



# 《網絡安全法》對於外商投資的影響

# 《網絡安全法》作為網絡安全的基本法

- 《網絡安全法》與《國家安全法》、《反恐怖主義法》、《刑法》、《保密法》、《治安管理處罰法》、《關於加強網絡信息保護的決定》、《關於維護互聯網安全的決定》、《電腦信息系統安全保護條例》、《互聯網信息服務管理辦法》等現行法律法規共同構成中國關於網絡安全管理的法律系統。
- 《網絡安全法》作為網絡安全的基本法，設置了最基本的網絡安全制度框架，包括：關鍵信息基礎設施保護制度、網絡安全等級保護制度、個人信息保護制度、網絡信息內容管理制度、網絡產品和服務管理制度、網絡安全事件應急回應制度等。

# 網絡安全等級保護制度

● 《網絡安全法》第21條：

● 國家實行網絡安全等級保護制度。

● 網絡運營者承擔的實施網絡安全等級保護制度相關的安全保護義務包括：

- (1) 制定內部安全管理制度和操作規程，確定網絡安全負責人，落實網絡安全保護責任；
- (2) 採取防範電腦病毒和網絡攻擊、網絡侵入等危害網絡安全行為的技術措施；
- (3) 採取監測、記錄網絡運行狀態、網絡安全事件的技術措施，並按照規定留存相關的網絡日誌不少於六個月；
- (4) 採取數據分類、重要數據備份和加密等措施；
- (5) 法律、行政法規規定的其他義務。

# 網絡產品、服務提供者的義務

● 《網絡安全法》第22條：

- 網絡產品、服務應當符合相關國家標準的強制性要求。網絡產品、服務的提供者不得設置惡意程式；發現其網絡產品、服務存在安全缺陷、漏洞等風險時，應當立即採取補救措施，按照規定及時告知用戶並向有關主管部門報告。
- 網絡產品、服務的提供者應當為其產品、服務持續提供安全維護；在規定或者當事人約定的期限內，不得終止提供安全維護。
- 網絡產品、服務具有收集使用者信息功能的，其提供者應當向用戶明示並取得同意；涉及使用者個人信息的，還應當遵守本法和有關法律、行政法規關於個人信息保護的規定。

# 網絡關鍵設備和網絡安全專用產品

- 《網絡安全法》第23條：
- 網絡關鍵設備和網絡安全專用產品應當按照相關國家標準的強制性要求，由具備資格的機構安全認證合格或者安全檢測符合要求後，方可銷售或者提供。
- 國家網信部門會同國務院有關部門制定、公佈網絡關鍵設備和網絡安全專用產品目錄，並推動安全認證和安全檢測結果互認，避免重複認證、檢測。

# 實名認證

- 《網絡安全法》第24條：
- 網絡運營者為使用者辦理網絡接入、功能變數名稱註冊服務，辦理固定電話、行動電話等入網手續，或者為使用者提供信息發佈、即時通訊等服務，在與使用者簽訂協定或者確認提供服務時，應當要求使用者提供真實身份信息。使用者不提供真實身份信息的，網絡運營者不得為其提供相關服務。
- 國家實施網絡可信身分戰略，支援研究開發安全、方便的電子身份認證技術，推動不同電子身份認證之間的互認。



# 網絡安全事件應急預案

- 《網絡安全法》第25條：
- 網絡運營者應當制定網絡安全事件應急預案，及時處置系統漏洞、電腦病毒、網絡攻擊、網絡侵入等安全風險；在發生危害網絡安全的事件時，立即啟動應急預案，採取相應的補救措施，並按照規定向有關主管部門報告。
- 《網絡安全法》第26條：
- 開展網絡安全認證、檢測、風險評估等活動，向社會發佈系統漏洞、電腦病毒、網絡攻擊、網絡侵入等網絡安全信息，應當遵守國家有關規定。

# 網絡犯罪偵查及協助

● 《網絡安全法》第27條：

● 任何個人和組織不得從事非法侵入他人網絡、干擾他人網絡正常功能、竊取網絡數據等危害網絡安全的活動；不得提供專門用於從事侵入網絡、干擾網絡正常功能及防護措施、竊取網絡數據等危害網絡安全活動的程序、工具；明知他人從事危害網絡安全的活動的，不得為其提供技術支援、廣告推廣、支付結算等幫助。

● 《網絡安全法》第28條：

● 網絡運營者應當為公安機關、國家安全機關依法維護國家安全和偵查犯罪的活動提供技術支援和協助。

# 關鍵信息基礎設施

- 《網絡安全法》第31條：
- 國家對公共通信和信息服務、能源、交通、水利、金融、公共服務、電子政務等重要行業和領域，以及其他一旦遭到破壞、喪失功能或者數據洩露，可能嚴重危害國家安全、國計民生、公共利益的關鍵信息基礎設施，在網絡安全等級保護制度的基礎上，實行重點保護。關鍵信息基礎設施的具體範圍和安全保護辦法由國務院制定。
- 國家鼓勵關鍵信息基礎設施以外的網絡運營者自願參與關鍵信息基礎設施保護體系。

# 關鍵信息基礎設施設施運營者的義務

- 關鍵信息基礎設施的建設要求（第33條）；
- 關鍵信息基礎設施運營者的安全保護義務（第34條）；
- 採購關鍵信息基礎設施產品和服務的國家安全審查要求（第35條）；
- 採購關鍵信息基礎設施產品和服務的保密要求（第36條）；
- 個人信息和重要數據的當地語系化要求（第37條）；
- 關鍵信息基礎設施的網絡安全年度檢測評估（第38條）。

# 數據本地化

● 《網絡安全法》第37條：

● 關鍵信息基礎設施的運營者在中華人民共和國境內運營中收集和產生的個人信息和重要數據應當在境內存儲。因業務需要，確需向境外提供的，應當按照國家網信部門會同國務院有關部門制定的辦法進行安全評估；法律、行政法規另有規定的，依照其規定。

# 網絡安全監測預警與應急處置制度

- 《網絡安全法》第51條：
- 國家建立網絡安全監測預警和信息通報制度。國家網信部門應當統籌協調有關部門加強網絡安全信息收集、分析和通報工作，按照規定統一發佈網絡安全監測預警信息。
- 《網絡安全法》第58條：
- 因維護國家安全 and 社會公共秩序，處置重大突發社會安全事件的需要，經國務院決定或者批准，可以在特定區域對網絡通信採取限制等臨時措施。

# 法律責任

- 《網絡安全法》第六章規定網絡運營者，根據違法行為的情形，主要的法律責任承擔形式包括責令改正、警告、罰款，責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員等進行罰款等；並且，有關機關還可以把違法行為記錄到信用檔案。對於違反第27條的人員，法律還建立了職業禁入的制度。
- 網絡運營者還應當關注違法行為所導致的民事責任和刑事責任。網絡運營者如果因違法《網絡安全法》的行為給他人造成損失的，該行為具有民事上的可訴性，網絡運營者應當承擔相應的民事責任。



# 《數據安全法》對於外商投資的影響



# 《數據安全法》的域外效力

- 《數據安全法》第2條：
- 在中華人民共和國境內開展數據處理活動及其安全監管，適用本法。
- 在中華人民共和國境外開展數據處理活動，損害中華人民共和國國家安全、公共利益或者公民、組織合法權益的，依法追究法律責任。

# 數據的意義

- 《數據安全法》第3條：
- 本法所稱數據，是指任何以電子或者其他方式對信息的記錄。
- 數據處理，包括數據的收集、存儲、使用、加工、傳輸、提供、公開等。
- 數據安全，是指通過採取必要措施，確保數據處於有效保護和合法利用的狀態，以及具備保障持續安全狀態的能力。

# 數據分類分級保護制度

● 《數據安全法》第20條：

● 國家建立數據分類分級保護制度，根據數據在經濟社會發展中的重要程度，以及一旦遭到篡改、破壞、洩露或者非法獲取、非法利用，對國家安全、公共利益或者個人、組織合法權益造成的危害程度，對數據實行分類分級保護。國家數據安全工作協調機制統籌協調有關部門制定重要數據目錄，加強對重要數據的保護。

# 數據安全風險評估、報告、信息共用 、監測預警機制

● 《數據安全法》第22條：

● 國家建立集中統一、高效權威的數據安全風險評估、報告、信息共用、監測預警機制。國家數據安全工作協調機制統籌協調有關部門加強數據安全風險信息的獲取、分析、研判、預警工作。

# 數據安全應急處置機制

● 《數據安全法》第23條：

● 國家建立數據安全應急處置機制。發生數據安全事件，有關主管部門應當依法啟動應急預案，採取相應的應急處置措施，防止危害擴大，消除安全隱患，並及時向社會發佈與公眾有關的警示信息。

# 數據安全審查制度

- 《數據安全法》第24條：
- 國家建立數據安全審查制度，對影響或者可能影響國家安全的數據處理活動進行國家安全審查。
- 依法作出的安全審查決定為最終決定。

# 數據出口管制

- 《數據安全法》第25條：
- 國家對與維護國家安全和利益、履行國際義務相關的屬於管制物項的數據依法實施出口管制。
- 《數據安全法》第26條：
- 任何國家或者地區在與數據和數據開發利用技術等有關的投資、貿易等方面對中華人民共和國採取歧視性的禁止、限制或者其他類似措施的，中華人民共和國可以根據實際情況對該國家或者地區對等採取措施。

# 數據安全保護義務/風險評估報告

● 《數據安全法》第27條：

● 開展數據處理活動應當依照法律、法規的規定，建立健全全流程數據安全管理制度，組織開展數據安全教育培訓，採取相應的技術措施和其他必要措施，保障數據安全。利用互聯網等信息網絡開展數據處理活動，應當在網絡安全等級保護制度的基礎上，履行上述數據安全保護義務。

● 重要數據的處理者應當明確數據安全負責人和管理機構，落實數據安全保護責任。

● 《數據安全法》第29條：

● 開展數據處理活動應當加強風險監測，發現數據安全缺陷、漏洞等風險時，應當立即採取補救措施；發生數據安全事件時，應當立即採取處置措施，按照規定及時告知用戶並向有關主管部門報告。



# 數據出境

- 《數據安全法》第31條：
- 關鍵信息基礎設施的運營者在中華人民共和國境內運營中收集和產生的重要數據的出境安全管理，適用《中華人民共和國網絡安全法》的規定；
- 其他數據處理者在中華人民共和國境內運營中收集和產生的重要數據的出境安全管理辦法，由國家網信部門會同國務院有關部門制定。

# 收集、使用數據

● 《數據安全法》第32條：

● 任何組織、個人收集數據，應當採取合法、正當的方式，不得竊取或者以其他非法方式獲取數據。

● 法律、行政法規對收集、使用數據的目的、範圍有規定的，應當在法律、行政法規規定的目的和範圍內收集、使用數據。

● 《數據安全法》第33條：

● 從事數據交易仲介服務的機構提供服務，應當要求數據提供方說明數據來源，審核交易雙方的身份，並留存審核、交易記錄。

● 《數據安全法》第34條：

● 法律、行政法規規定提供數據處理相關服務應當取得行政許可的，服務提供者應當依法取得許可。

# 調取數據

- 《數據安全法》第35條：
- 公安機關、國家安全機關因依法維護國家安全或者偵查犯罪的需要調取數據，應當按照國家有關規定，經過嚴格的批准手續，依法進行，有關組織、個人應當予以配合。
- 《數據安全法》第36條：
- 中華人民共和國主管機關根據有關法律和中華人民共和國締結或者參加的國際條約、協定，或者按照平等互惠原則，處理外國司法或者執法機構關於提供數據的請求。非經中華人民共和國主管機關批准，境內的組織、個人不得向外國司法或者執法機構提供存儲於中華人民共和國境內的數據。

# 違反數據安全保護義務的法律責任

● 《數據安全法》第45條：

- 開展數據處理活動的組織、個人不履行本法第二十七條、第二十九條、第三十條規定的數據安全保護義務的，由有關主管部門責令改正，給予警告，可以並處五萬元以上五十萬元以下罰款，對直接負責的主管人員和其他直接責任人員可以處一萬拒不改正或者造成大量數據洩露等嚴重後果的，處五十萬元以上二百萬元以下罰款元以上十萬元以下罰款；，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處五萬元以上二十萬元以下罰款。
- 違反國家核心數據管理制度，危害國家主權、安全和發展利益的，由有關主管部門處二百萬元以上一千萬元以下罰款，並根據情況責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照；構成犯罪的，依法追究刑事責任。

# 非法向境外提供重要數據的法律責任

● 《數據安全法》第46條：

● 違反本法第三十一條規定，向境外提供重要數據的，由有關主管部門責令改正，給予警告，可以並處十萬元以上一百萬元以下罰款，對直接負責的主管人員和其他直接責任人員可以處一萬元以上十萬元以下罰款；情節嚴重的，處一百萬元以上一千萬元以下罰款，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處十萬元以上一百萬元以下罰款。

# 從事數據交易中介服務機構的法律責任

● 《數據安全法》第47條：


● 從事數據交易中介服務的機構未履行本法第三十三條規定的義務的，由有關主管部門責令改正，沒收違法所得，處違法所得一倍以上十倍以下罰款，沒有違法所得或者違法所得不足十萬元的，處十萬元以上一百萬元以下罰款，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照；對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。

# 拒不配合數據調取及非法向外國司法 或者執法機構提供數據的法律責任

❶ 《數據安全法》第48條：

❷ 違反本法第三十五條規定，拒不配合數據調取的，由有關主管部門責令改正，給予警告，並處五萬元以上五十萬元以下罰款，對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。

❸ 違反本法第三十六條規定，未經主管機關批准向外國司法或者執法機構提供數據的，由有關主管部門給予警告，可以並處十萬元以上一百萬元以下罰款，對直接負責的主管人員和其他直接責任人員可以處一萬元以上十萬元以下罰款；造成嚴重後果的，處一百萬元以上五百萬元以下罰款，並可以責令暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照，對直接負責的主管人員和其他直接責任人員處五萬元以上五十萬元以下罰款。



《個人信息保護法》  
對於外商投資的影響



# 個人信息跨境提供的條件

● 《個保法》第38條：

● 個人信息處理者因業務等需要，確需向中華人民共和國境外提供個人信息的，應當具備下列條件之一：

➤ （一）依照本法第四十條的規定通過國家網信部門組織的安全評估；

➤ （二）按照國家網信部門的規定經專業機構進行個人信息保護認證；

➤ （三）按照國家網信部門制定的標準合同與境外接收方訂立合同，約定雙方的權利和義務；

➤ （四）法律、行政法規或者國家網信部門規定的其他條件。

➤ 中華人民共和國締結或者參加的國際條約、協定對向中華人民共和國境外提供個人信息的條件等有規定的，可以按照其規定執行。

➤ 個人信息處理者應當採取必要措施，保障境外接收方處理個人信息的活動達到本法規定的個人信息保護標準。

# 個人信息跨境提供的同意權

● 《個保法》第39條：

● 個人信息處理者向中華人民共和國境外提供個人信息的，應當向個人告知境外接收方的名稱或者姓名、聯繫方式、處理目的、處理方式、個人信息的種類以及個人向境外接收方行使本法規定權利的方式和程序等事項，並取得個人的單獨同意。

# 本地化

- 《個保法》第40條：
- 關鍵信息基礎設施運營者和處理個人信息達到國家網信部門規定數量的個人信息處理者，應當將在中華人民共和國境內收集和產生的個人信息存儲在境內。
- 確需向境外提供的，應當通過國家網信部門組織的安全評估；法律、行政法規和國家網信部門規定可以不進行安全評估的，從其規定。

# 平等互惠原則

● 《個保法》第41條：

● 中華人民共和國主管機關根據有關法律和中華人民共和國締結或者參加的國際條約、協定，或者按照平等互惠原則，處理外國司法或者執法機構關於提供存儲於境內個人信息的請求。非經中華人民共和國主管機關批准，個人信息處理者不得向外國司法或者執法機構提供存儲於中華人民共和國境內的個人信息。

# 禁止提供個人信息

● 《個保法》第42條：

● 境外的組織、個人從事侵害中華人民共和國公民的個人信息權益，或者危害中華人國家網信部門可以將其列入限制或者禁止個人信息提供清單，予以公告，並採取限制或者禁止向其提供個人信息等措施民共和國國家安全、公共利益的個人信息處理活動的，。

● 《個保法》第43條：

● 任何國家或者地區在個人信息保護方面對中華人民共和國採取歧視性的禁止、限制或者其他類似措施的，中華人民共和國可以根據實際情況對該國家或者地區對等採取措施。

# 個人信息保護措施

- 《個保法》第51條：
- 個人信息處理者應當根據個人信息的處理目的、處理方式、個人信息的種類以及對個人權益的影響、可能存在的安全風險等，採取下列措施確保個人信息處理活動符合法律、行政法規的規定，並防止未經授權的訪問以及個人信息洩露、篡改、丟失：
  - （一）制定內部管理制度和操作規程；
  - （二）對個人信息實行分類管理；
  - （三）採取相應的加密、去標識化等安全技術措施；
  - （四）合理確定個人信息處理的操作許可權，並定期對從業人員進行安全教育和培訓；
  - （五）制定並組織實施個人信息安全事件應急預案；
  - （六）法律、行政法規規定的其他措施。

# 指定個人信息保護負責人

- 《個保法》第52條：
- 處理個人信息達到國家網信部門規定數量的個人信息處理者應當指定個人信息保護負責人，負責對個人信息處理活動以及採取的保護措施等進行監督。
- 個人信息處理者應當公開個人信息保護負責人的聯繫方式，並將個人信息保護負責人的姓名、聯繫方式等報送履行個人信息保護職責的部門。

# 設立專門機構或者指定代表

● 《個保法》第53條：

● 本法第三條第二款規定的中華人民共和國境外的個人信息處理者，應當在中華人民共和國境內設立專門機構或者指定代表，負責處理個人信息保護相關事務，並將有關機構的名稱或者代表的姓名、聯繫方式等報送履行個人信息保護職責的部門。



# 合規審計

---

● 《個保法》第54條：

● 個人信息處理者應當定期對其處理個人信息遵守法律、行政法規的情況進行合規審計。

# 個人信息保護影響評估

● 《個保法》第55條：

● 有下列情形之一的，個人信息處理者應當事前進行個人信息保護影響評估，並對處理情況進行記錄：

- （一）處理敏感個人信息；
- （二）利用個人信息進行自動化決策；
- （三）委託處理個人信息、向其他個人信息處理者提供個人信息、公開個人信息；
- （四）向境外提供個人信息；
- （五）其他對個人權益有重大影響的個人信息處理活動。

# 大型個人信息處理者義務

● 《個保法》第58條：

● 提供重要互聯網平臺服務、使用者數量巨大、業務類型複雜的個人信息處理者，應當履行下列義務：

- （一）按照國家規定建立健全個人信息保護合規制度體系，成立主要由外部成員組成的獨立機構對個人信息保護情況進行監督；
- （二）遵循公開、公平、公正的原則，制定平臺規則，明確平臺內產品或者服務提供者處理個人信息的規範和保護個人信息的義務；
- （三）對嚴重違反法律、行政法規處理個人信息的平臺內的產品或者服務提供者，停止提供服務；
- （四）定期發佈個人信息保護社會責任報告，接受社會監督。

# 法律責任

- 《個保法》第66條：
- 違反本法規定處理個人信息，或者處理個人信息未履行本法規定的個人信息保護義務的，由履行個人信息保護職責的部門責令改正，給予警告，沒收違法所得，對違法處理個人信息的應用程式，責令暫停或者終止提供服務；拒不改正的，並處一百萬元以下罰款；對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款。
- 有前款規定的違法行為，情節嚴重的，由省級以上履行個人信息保護職責的部門責令改正，沒收違法所得，並處五千萬元以下或者上一年度營業額百分之五以下罰款，並可以責令暫停相關業務或者停業整頓、通報有關主管部門吊銷相關業務許可或者吊銷營業執照；對直接負責的主管人員和其他直接責任人員處十萬元以上一百萬元以下罰款，並可以決定禁止其在一定期限內擔任相關企業的董事、監事、高級管理人員和個人信息保護負責人。



# 結論與建議

# 《網絡安全法》、《數據安全法》、《個保法》 全面實施後可能面臨之問題

- 《網絡安全法》、《數據安全法》、《個保法》及《民法典》間的調和與適用。
- 《網絡安全法》、《個保法》及《民法典》間關於個人信息的認定。
- 個人信息處理者與網絡服務提供者的雙重身分與監管、法律責任問題。
- 監管機構及監管範圍不一致。《個保法》的監管部門及監管範圍，似與《網絡安全法》及《數據安全法》疊床架屋，將來監管部門如何分工，亟待相關實施條例或辦法出台明確規定之。
- 數據出境安全管理辦法及各項數據安全制度仍有待相關配套法規出台。

## 網絡運營者的企業制度建設要求(1/2)

- 與實施網絡安全等級保護制度相關的義務和制度建設，包括制定內部安全管理制度和操作規程，確定網絡安全負責人等（第21條）；
- 健全使用者信息保護制度（第22條和第40條）；
- 落實網絡實名制（第24條）；
- 網絡安全事件應急預案（第25條）；
- 關鍵信息基礎設施的安全保護義務，包括：設置專門安全管理機構和安全管理負責人，並對該負責人和關鍵崗位的人員進行安全背景審查；定期對從業人員進行網絡安全教育、技術培訓和技能考核；對重要系統和數據庫進行容災備份；制定網絡安全事件應急預案，並定期進行演練；法律、行政法規規定的其他義務（第34條）；

## 網絡運營者的企業制度建設要求(2/2)

- 採購關鍵信息基礎設施產品和服務的保密制度（第36條）
- 關鍵信息基礎設施安全性的年度評估（第36條）
- 個人信息的收集和利用規則及制度（第41條和第42條）
- 個人信息洩露事件的報告制度（第42條）
- 違法使用個人信息刪除和錯誤個人信息更正制度（第43條）
- 網絡運營者對使用者非法信息傳播的監管（第47條）
- 網絡信息安全投訴、舉報制度（第49條）
- 網絡犯罪偵查及協助
- 關鍵信息基礎設施設施運營者的義務
- 數據本地化
- 網絡安全監測預警與應急處置制度



# 《數據安全法》外商投資應注意事項

---

- 數據安全審查制度
- 數據出口管制
- 數據安全保護義務/風險評估報告
- 收集、使用數據
- 配合調取數據的義務

# 《個保法》外商投資應注意事項

- 行使同意與告知的政策
- 自動化決策
- 公開個人信息及使用公開的個人信息的特別限制
- 敏感個人信息的收集
- 個人信息跨境的限制
- 建立境外個人信息處理者的溝通路徑
- 高風險處理活動評估

## 外商因應策略（1/2）

- 外商在大陸境內、外從事收集、存儲、使用、加工、傳輸、提供、公開數據等涉及大陸地區數據之處理行為，如於社交媒體、批發零售、生產應用、或商業行為等應用場景所收集之個人數據、地理數據、生產數據等，運用於廣告行銷、市場調研、科學研究等用途，應注意《數據安全法》之適用。
- 運用自動化、智能化軟體或攝錄像所收集的數據，如個人圖像、外貌、生物特徵、行程軌跡等，均屬於數據而有《數據安全法》之適用。
- 關於數據存儲的本地化及數據出境，包括數據共享、雲端化、數據即時監控等可能產生的跨境數據傳輸問題，均應依照《數據安全法》及《網絡安全法》相關規定辦理。

## 外商因應策略（2/2）

- 關於境內存儲及境外傳輸限制的規定。除了關鍵信息基礎設施運營者依據《網絡安全法》應當將在大陸境內收集和產生的個人信息存儲在境內外，處理個人信息達到國家網信部門規定數量的個人信息處理者，同樣也受到境內存儲限制（《個保法》第40條）。
- 個人信息處理者向境外提供個人信息，應當通過安全評估，進行個人信息保護認證，及按照標準合同與境外接收方訂立合同，約定雙方的權利和義務等（《個保法》第38條），且應取得個人的單獨同意（《個保法》第39條）。
- 如個人信息處理者在大陸境外，在大陸境內設立專門機構或者指定代表，負責處理個人信息保護相關事務（《個保法》第69條），此與《個保法》的域外管轄擴展落地直接呼應，也是與歐盟GDPR等域外個人信息保護法的機制保持一致性的對等要求。



敬請指教!

泰鼎法律事務所  
蔡步青律師

Email: [roger.tsai@titanlaw.com.tw](mailto:roger.tsai@titanlaw.com.tw)

TEL: 02 2703 3366 分機12

微信: caibuqing001