protiviti®
Face the Future with Confidence

Data Cross-Border Transfer

As part of our series providing insights into the Cybersecurity Law of the People's Republic of China (PRC), this fifth installment focuses on the cross-border transfer of data — or data localization — that is outlined in Article 37. This article covers the transfer and access of personal information and important data collected by critical information infrastructure (CII) operators in mainland China. However, other measures and guidelines currently under discussion (including Cross-Border Transfer Assessment Measures for Personal Information and Important Data as well as Security Assessment Guideline for Data Cross-Border Transfer) could extend network operator requirements.

On the surface, the data cross-border transfer clause seems simple as it only involves two requirements. The major one is data storage localization, which limits the transfer and access of personal information and other important information out of mainland China. But it is important to understand the impact this has on existing business models and system architecture, and the potential scope of financial costs, effort, and technical adjustments. Although the Cybersecurity Law permits data cross-border transfers, these are only allowed in compliance with industry regulations and after an official assessment on security measures and formal approval have been completed.

Overview of Data Cross-Border Transfer

Compliance Requirements of Data Cross-Border Transfer

Under the Law, personal information and other important data collected in mainland China by CII operators must be stored within the borders of mainland China. Security assessments and approval from industry regulatory bodies are required for their transfer outside mainland China, making any transfers nearly impossible for industries like banking or for specific types of data such as geolocation.

Article	Legal Requirements
Article 37	Critical information infrastructure operators (network operators) shall: • store personal information or important data within mainland China. • conduct a security assessment for approval before cross-border transfer, if necessary

According to the Security Assessment Guideline for Data Cross-Border Transfer, there are three major types of cross-border transfer:

- Active data cross-border transfer
  Example: data transfer from mainland China to the United States
- Passive data cross-border transfer
  Example: data in mainland China accessed by system administrators in Australia
- Data transfer into territories outside of mainland China's jurisdiction
  Example: data transfer to Hong Kong or the Canadian embassy

In the past, many foreign companies adopted a centralized system and data architecture, which were often located in the United States or Europe. As this is no longer in compliance with the requirements of Article 37, companies can choose to implement either decentralization or sanitization.

The decentralization method requires the local setup of a complete and separate infrastructure and system (as well as associated administration) managing the storage and processing of personal information and other important data within mainland China. The technical support, system administration, and security operations of the infrastructure and system should also be located in mainland China. This requires a separate and independent IT team and IT environment, which could incur high costs, as well as misalign with existing architecture.

The sanitization method requires the removal of any important data and details that could identify personal information, before transferring the data to the central application and infrastructure outside mainland China for storage and processing. Compared with decentralization, this may require a relatively smaller IT team and environment. However, this method may entail extensive business and IT planning in order to identify which data must be transferred to headquarters, as well as the level or method of sanitization.

Security Assessment for Data Cross-Border Transfer

According to Cross-Border Transfer Assessment Measures for Personal Information and Important Data, assessments may be conducted by industry regulatory bodies or companies themselves. When conducting self-assessment, a company must consider a number of factors, including:

- Legitimacy: the information and data to be transferred must not contravene any laws or regulatory requirements.
- Necessity: data providers should ensure that it is necessary to transfer the information and data because of business operations and legal obligations.
- Personal Information Characteristics: personal information should undergo effective deidentification and desensitization.
- Important Data Characteristics
- Amount and Frequency of Data Transferred: the amount and frequency of data transfer should be limited to what is necessary to maintain business operations.
- Security Capability of Data Provider and Receiver: the legal contract signed between data providers and receivers should be reviewed to ensure that obligations on compliance issues as well as data security and privacy protection are well-defined.
- Political and Legal Environment of Receiver's Location: assessment should take into considerations if the receiver's country has specific data security and privacy laws, especially if the laws might give local authority access to the transferred information.

If any of the following criteria are met, assessment by industry regulatory bodies is required:

- The number of personal information records exceeds a cumulative number of 0.5 million.
- The personal information or important data volume is above 1,000 GB.
- The data comes from the following fields or industries:
  - Nuclear facilities
  - Chemical and biological
  - National defense
  - Medical and health
  - Major engineering or construction program
  - Seas and oceans
  - Geolocation
- The transfer involves cybersecurity information on CII.
- The transfer involves personal information and important data from CII.
- Other fields involving national security or social interests.

Compliance Challenges

Extensive Capital and Ongoing Expenses

As noted earlier, decentralization requires the localization of infrastructure, systems, and administration in mainland China, which may lead to significant implementation costs and an increase in a company's annual IT budget. Companies must factor in costs for data center operations, security operations, IT management, maintenance of infrastructure and systems, and IT resources. These all require capital as well as ongoing operating expenses for as long as the separate infrastructure and systems are operational in mainland China.

Technical incompetence and incomprehensive design often result in security incidents or lack of compliance with the Law or other standards. These also entail potential costs ensuing from redesign, remediation, risk mitigation, recovery, as well as business interruption. Therefore, when building up the IT environment and IT team for mainland China, companies should ensure comprehensiveness of technical documentation and technical competency.

Adequate IT Competence in Mainland China

Both decentralization and sanitization methods require a certain level of infrastructure system architecture changes. It's arguable that the decentralization method requires less effort in architecture redesign, but decentralization may also require building a complete set of infrastructure and systems.

For both methods, companies have to ensure adequately skilled IT resources within mainland China that can support the running of the local IT infrastructure and systems, as well as local business needs. In particular, companies will have to engage a local cybersecurity team (including security governance and security operations) to ensure proper cybersecurity protection and comply with the Law. Some companies may face difficulties building and managing their own IT team locally, resulting in the possibility of outsourcing certain functions to experienced local service providers.

Protiviti Cybersecurity and Privacy Protection Services

IT Specialized Audit	• Often included in the overall audit co-sourcing or outsourcing program • More in-depth and technical than Information Technology General Control (ITGC) audit • Often focused on a specific part of IT operations such as Cybersecurity or Disaster Recovery
Security Risk and Compliance Assessment	• International Security Standards: ISO/IEC 2700x, NIST Cybersecurity Framework, CSA Cloud Control Matrix • Payment Card Security Standards: PCI DSS 3.x • Other Regulations/Standards: China Cybersecurity Law, HKMA, SFC, MAS, COSO SOX, ISO/IEC 27701
Data Privacy Services	• Compliance assessment against privacy regulations: Hong Kong PDPO Cap.486, China Personal Information Protection, EU GDPR, US CCPA • Managed privacy services: Privacy-as-a-service • Personal data inventory advisory
Attack and Penetration Service	• Vulnerability scan and penetration test • Source code review • Red team test • Phishing and social engineering test
Security Program and Strategy Design	• Design and revision of cybersecurity strategy and program • Design and revision of security policies, such as data and information classification • Design, revision, and implementation of security procedures
Security Architecture and Control Design	• System hardening review and enhancement • Security architecture design: on-premise, cloud platform • Security control design and review: firewall, data loss prevention, privileged access management, event log analyzer
Security Implementation Services	• Security tools design and selection • Project management and support for security tools implementation • Leverage Protiviti global partnerships with OneTrust, SailPoint, CyberArk, Palo Alto, ServiceNow, Carbon Black, Splunk, LogRhythm, etc.
Managed Security Services	• Security resource augmentation • Managed security operations • Third-party risk outsourcing
Incident Response and Forensics	• Security incident response advisory and support • Security incident investigation and root-cause analysis • Compromise assessment
Security Awareness and Capability Advisory	• Blueteam security assessment and advisory (e.g. SOC, MSSP) • Cyber incident handling and mitigation review • Security awareness assessment and support

How Protiviti Can Help

Protiviti aids businesses in ensuring that their IT services meet legal requirements and regulatory rules on both national and industry-specific levels. With a team of IT security professionals, compliance experts, auditors, and other professionals, Protiviti keeps track of evolving regulations based on industry innovations, environmental trends, and emerging risks.

Protiviti security and privacy services will evaluate your current compliance according to relevant legal requirements and regulatory rules and develop technical solutions that correspond with your current technology, procedures, and resources competency. We will close gaps in your IT technology and processes in line with your budget plan, as well as prevent disruptions to normal IT and business operations from compliance activities.

Contacts

Michael Pang
Managing Director, Technology Consulting
Mobile (HK): +852 9211 9853
Mobile (PRC): +86 131 4399 6166
michael.pang@protiviti.com

Jonathan Hsieh
Associate Director, Technology Consulting
Office: +86 21 5153 6900
Mobile: +86 138 1745 5636
jonathan.hsieh@protiviti.com