China Cybersecurity Law - Recent Legal Developments and Impacts on Businesses

Barbara Li
Partner, Norton Rose Fulbright LLP Beijing Office
Head of TMT, Cybersecurity and Data Privacy for China
Vice-Chair of Cybersecurity Sub-Working Group of EU Chamber of Commerce in China

11 December 2019
Hong Kong
Outline

• Recent updates of CSL regime
• Enforcement Actions
• Several challenging questions
• Case study
• Strategies and practical solutions
# Recent updates of CSL regime

## Encryption Law of PRC

### Regulations on Protection of Children’s Personal Data

<table>
<thead>
<tr>
<th>Draft Rules</th>
<th>Guidelines, Specifications and Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulations on Multi-Level Protection of Cybersecurity</td>
<td>MPLS standards V2.0</td>
</tr>
<tr>
<td>Measures on Cybersecurity Review</td>
<td>MPS Personal Data Protection Guidelines</td>
</tr>
<tr>
<td>Measures on Data Security</td>
<td>GBT/35273 Personal Data Specifications</td>
</tr>
<tr>
<td>Measures for Security Review for Cross-Border Personal Data Transfer</td>
<td>GB standards on Personal Data Collection by Apps</td>
</tr>
</tbody>
</table>
Enforcement Actions

• Crowded space by multiple regulators (九龙治水)
• Active enforcements
• Stronger awareness by general public
• Increased liabilities
Several Challenging Questions to Answer
Q1: How to Handle CII and Data Localisation

• Critical Information Infrastructure
  – Financial, energy, telecom and information services, water, transportation, e-government
  – AND “OTHER KEY INDUSTRIES”
  – PERSONAL DATA and IMPORTANT DATA collected/generated in China
  – Stored within the territory of China
  – Export of data only allowed for business necessity and pass security assessment

*“other key industries or sectors, which can seriously harm national security or public interest, if destroyed or tampered with or if data is leaked”
Q1: How to Handle CII and Data Localisation

- Where are the boundaries?

- Regulations/standards being drafted but not completed
Q2: How to Handle Cross-Border Data Transfer?

- Data localisation for personal data and important data collected/generated by CII operators
- New draft regulations try to narrow down the scope of data subject to data localisation
- On one hand, employment data and business/operation data likely to be carved out
- On the other hand, security assessment and governmental filing requirements may expand to apply to non-CII operators
- Possibility of adopting Chinese Standard Contract Scheme for cross-border transfer of personal data
Q3: I heard MLPS standards have come into force on 2019-12-01. What is this MLPS about? What does it mean to our company?
Q3: What is MLPS regime? What does it mean to our company?

- MLPS regime not new
- Focus on IT system to be classified into 5 levels with corresponding security requirements
- Reconfirmed under CSL
Q3: What is MLPS regime? What does it mean to our company?

- MLPS standards 2.0 came into force on 1 Dec 2019
- Expanded scope for cloud, big data, IoT, industrial automation
- Not mandatory yet pending the MLPS Administrative Regulations, but strongly promoted by MPS
- Can be perceived as best practice
- Possibility to be put in a disadvantaged position in bid projects without MLPS certification
Q4: We have done GDPR compliance review. GDPR regime is so strict that we are OK under Chinese law?
Q4: We have done GDPR compliance review, so we are OK under Chinese law?

- GDPR compliant ≠ CSL compliant
- Major differences between CSL and GDPR
  - Cybersecurity + Data Privacy
  - Legal basis for data collection and handling
  - Data breach
- CSL compliance review is still necessary
Q5: Chinese cybersecurity and data regime is still evolving. So we do not have to do anything for now?
Q5: PRC regime is still evolving, so we do not have to do anything for now?

- CSL effective from 1 June 2017
- Only CII and security assessment for cross-border data transfer are less settled
- Other legal requirements are already in place and being enforced by authorities
- Necessary for compliance review, gap analysis and remedial/preventive actions
Case Study

• US-based global consumer goods manufacturing company with 3 WFOEs in China

• 1,000 employees whose personal data are to be shared with regional HR centre in Hong Kong

• Customer data to be transferred to US for user profiling and R&D
Case Study

What Data
- Employee Data
- Consumer Data

Current Data Practice
- Consent?
- Notification?
- Privacy policy?

Can transfer, but
- Must address the risks

Not CIIO
- No financial institution
- No human genetic data
- No health data

Data Cross-border Transfer
- Is it a CIIO?

Mitigations
- Update employment contract
- Revise/update consent, notice and privacy
- Review data sharing agreement
- Security assessment
- MLPS certification

Other Measures
- Data breach response
- Training
Strategies and Practical Solutions

• Data mapping / gap analysis
• Localise documents/contracts
• Training
• Close watch on regulatory and technical developments
CONTACTS

Email: barbara.li@nortonrosefulbright.com
Tel: +86 10 6535 3130
LinkedIn and WeChat: Barbara_Lawyer

Our recent client briefings

• FinTech Nation
• New Chinese Measures for Personal Data Cross-Border Transfer Security Assessments
• New Chinese Measures for Data Security Administration
• China issues new draft regulations on Cybersecurity Review for Public Comment
• China overhauls its Foreign Investment Regulatory Regime
• China issues new regulation on blockchain