New China data privacy compliance requirements

Since China's Cybersecurity Law took effect on June 1, 2017, China has ushered in a number of new laws and regulations that set out stricter requirements, including various national standards, the *Regulation for the Cybersecurity Protection of Personal Information of Minors*, the *Judicial Interpretation on Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies*, the *Regulations on the Security and Protection of Critical Information Infrastructure*, as well as the *Data Security Law* and most recently the *Personal Information Protection Law* ("**PIPL**").

Application

The new laws and regulations set out new requirements. They apply to foreign companies operating in China as well as certain activities of foreign companies not operating in China. For example, the new PIPL will apply even if a foreign company is not operating in China if it:

- sells products or provides services to individuals in China, e.g. through CBEC or Tmall; or
- analyses the buying habits or other activities of individuals in China.

Key new requirements

1. For processing sensitive personal information (including information related to biometric recognition, religious belief, special identity, healthcare, financial account, geolocation, and a minor under the age of 14):
   - a separate consent is required;
   - the individual must be informed of the necessity of processing the sensitive personal information and its impact; and
   - consent from a parent or guardian as well as separate personal information processing policy are required in case of a minor under the age of 14.
2. Transfer of personal information outside of China needs to fulfil the following conditions:
   a) Completing one of the following actions:
      i. a security assessment by the Chinese government;
      ii. a certification of personal information protection by a professional institution;
      iii. entering into a contract prescribed by the Chinese government with the overseas recipient.
   b) Informing the individual the name and contact information of the overseas recipient, the purpose and method of the processing, the type of personal information involved, as well as the process for how the individual may exercise his/her rights.
   c) Obtaining a separate consent from the individual.
   d) Localising personal information collected or generated in China by Critical Information Infrastructure Operators (or **CIIOs**) and other companies which process personal information more than the prescribed volume. If transferring data overseas is necessary, such organisations may do so only after passing security assessment by the Chinese government in advance.

pwc

Tiang & Partners
程偉賓律師事務所

3. If the processed personal information reaches the prescribed volume, a data protection officer needs to be appointed to oversee and supervise data processing and protection. Relevant foreign companies without a presence in China need to set up special agencies or appoint representatives in China to deal with data protection matters.
4. A personal information impact assessment is necessary to process sensitive personal information, to use personal information in automated decision-making, to subcontract the data processing and to transfer personal information outside of China, etc. Records of such assessments should be kept for three years.

Penalties

Non-compliance may be subject to confiscation of income, a fine up to RMB 50 million or 5% of turnover of the previous year, business suspension and revocation of business licenses. Individuals involved may be fined up to RMB 1 million and may also be blacklisted from serving in important positions for a certain period of time. Damages and criminal prosecution are also possible.

Key takeaways

Many foreign companies have been ensuring compliance with data privacy laws in Europe, China and the US in the last few years. In many ways, the new China requirements are aligned with global legislation such as the European Union General Data Protection Regulation (or GDPR) but there are some key differences. The first step foreign business should take is to understand if and how the new China requirements apply to them and to assess how these differences apply to their operations. One key risk, for example, relates to companies' usual practice of centralising their employee files and other group wide databases outside of China. Such a practice should be reassessed.

Key takeaways are:

- All relevant companies need to:
    - be PIPL and China data privacy law compliant by November 1, 2021;
    - have China law compliant personal data protection policies; and
    - have China law compliant data privacy agreements in place with customers and employees..
- PIPL applies to certain personal information processing activity outside China (such as CBEC).
- PIPL requires certain personal information processing activity outside of China to set up a special agency or appoint a representative in China, and report their contact details.
- Transferring personal data outside of China is now subject to additional requirements for all companies (even if the volume of personal data involved is below the prescribed volume).
- Companies which process personal data over the prescribed volume need to record the responsible persons with the government.

www.pwchk.com
www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所