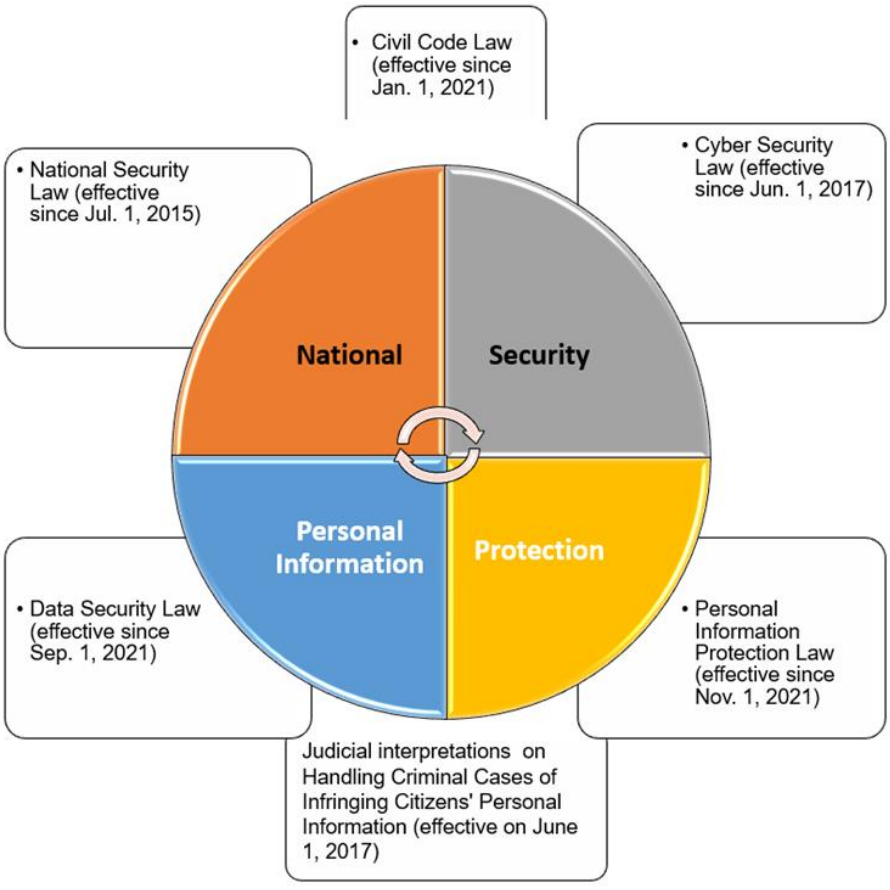
Regulatory Framework of PRC on Cross-border Data Transmission

Along with the rapid development of digital economy in China, the legislature of China has adopted a number of laws and regulations to secure national security and protect personal privacy. On July 21, 2022, Cyberspace Administration of China ("CAC") imposed a record-breaking penalty on Didi (RMB 8.026 billion, approx. USD 1.2 billion) for Didi's data breaches. It rings the alarm bell about data compliance by enterprises engaging in international business with China or operating in China.

Legal framework for data security and personal information protection in China

When reviewing the data-related laws and regulations of China which either have been adopted or are still under discussion, we may find that all these rules are focusing on national security (data security) and personal information protection. An overview chart on the legal framework for national security and personal information protection in China can be indicated as follows:



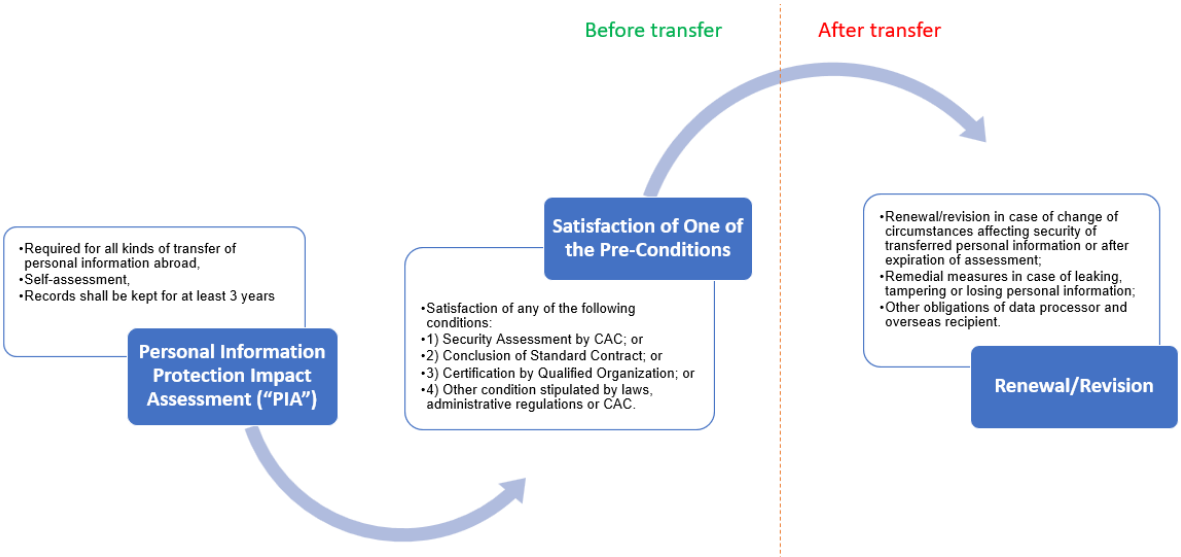
In order to implement the relevant laws and regulations above, the State Council of China as well as the administrative authorities (mainly Cyberspace Administration of China, "CAC") also adopted various implementation rules, which provide feasible instructions for the stakeholders to comply with the applicable laws and regulations and mainly include:

- Information Security Technology-Personal Information Security Specification (GB/T 35273-2020) (Effective since Oct. 1, 2020, recommended national standard);
- Regulations on Security Protection of Critical Information Infrastructures (Effective since Sep. 1. 2021);
- Measures for Data Export Security Assessment (Effective since Feb. 15, 2022);
- Cyber Security Review Measures (Effective since Sep. 1, 2022).

Overview on procedures required for transfer of personal information abroad

From the perspective of the supervision authorities, cross-border data transmission is the most critical part in the data transmission flow, especially when personal information or important data ("data that may endanger national security, economic operation, social stability, public health and safety, etc. once they are tampered with, destroyed, leaked, or illegally obtained or used.") are involved.

As required by the relevant laws and regulations (such as the Personal Information Protection Law), the transfer of personal information abroad shall be subject to the following procedures:



Further notes on the required procedures:

- PIA is required for all the data processors transferring any personal information abroad. A most common scenario is that a subsidiary of a foreign invested enterprise transfers the local employee's data to its overseas headquarter.
- A Security Assessment by CAC is only required for large-scale data processors or when important data is involved. Recently, CAC released the Measures for Data Export Security Assessment which comes into effect on September 1, 2022.
- The Conclusion of Standard Contract with the overseas data recipient is applicable to small-scale data processors and when important data is not involved. A draft version of the Standard Contract was made public by CAC for public opinion. It is expected that an official version of the Standard Contract will be released soon.
- The applicable scope of Certification by Qualified Organization is still unclear. We are waiting for further rules to be specified by CAC.

This is the first article of our Series: Cybersecurity and Data Compliance in PRC. More will follow, stay tuned!

(This post was written by Xueli Ren.)

For more information, please contact Asia Business Lab:
info@asiabusinesslab.org